ID: 634670
Sample Name:
SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
Cookbook: default.jbs
Time: 16:44:19
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

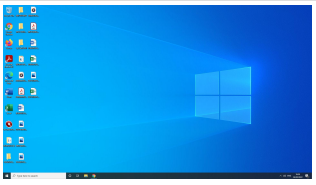
Windows Analysis Report

SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe

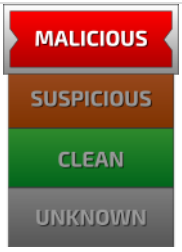
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
Analysis ID:	634670
MD5:	67a4759a7b2fcb..
SHA1:	592934bd8f6606..
SHA256:	19762fa9a397bf7.
Infos:	



Detection



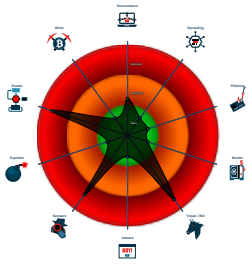
AgentTesla, GuLoader

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AgentTesla
- Yara detected GuLoader
- Found malware configuration
- Multi AV Scanner detection for subm…
- Tries to steal Mail credentials (via fi…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Sample is not signed and drops a de…
- DLL side loading technique detected
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- NDIS Filter Driver detected (likely us…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe (PID: 3120 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe" MD5: 67A4759A7B2FCB1A7E5B368FC150B974)
  - CasPol.exe (PID: 3872 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 4968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- mpam-e428c3f6.exe (PID: 1304 cmdline: "C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e428c3f6.exe" /q WD MD5: 89D4A3575EC6AEEFB442C18A41A18DDA)
  - MpSigStub.exe (PID: 1656 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe /stub 1.1.1 8500.10 /payload 1.367.502.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e428c3f6.exe /q WD MD5: 01F92DC7A766FF783AE7AF40FD0334FB)
- svchost.exe (PID: 7932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: F586835082F632DC8D9404D83BC16316)
- wevtutil.exe (PID: 5392 cmdline: C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\3FCB5F68-CD33-FF2F-34AE-798C9A7026D4.man MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 9144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- wevtutil.exe (PID: 7292 cmdline: C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\3FCB5F68-CD33-FF2F-34AE-798C9A7026D4.man "/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll" "/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll" "/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll" MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 5416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- mpengine.exe (PID: 7860 cmdline: C:\ProgramData\Microsoft\Windows Defender\Scans\\MpPayloadData\mpengine.exe MD5: C84EBFCFAFEB07D863C3ED18F6FBD40F)
  - conhost.exe (PID: 8572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- MpKslDrv.sys (PID: 4 cmdline: MD5: 97D3A85D7EF930E7035DAAC1622AD407)
- mpam-60574f34.exe (PID: 2156 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-60574f34.exe MD5: 50BCDEEB6A1DFFF15B62BEDAC2DDACA8)
  - MpSigStub.exe (PID: 9000 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe /stub 1.1.1 8500.10 /payload 4.18.2203.5 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-60574f34.exe MD5: 01F92DC7A766FF783AE7AF40FD0334FB)
- svchost.exe (PID: 6648 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: F586835082F632DC8D9404D83BC16316)
- WdNisDrv.sys (PID: 4 cmdline: MD5: B757AF9B44B0C0C75103210D9C7026FF)
- NisSrv.exe (PID: 4264 cmdline: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\NisSrv.exe MD5: B7F144CC18AE552E1C3D42051A934902)
- svchost.exe (PID: 4912 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: F586835082F632DC8D9404D83BC16316)
- svchost.exe (PID: 2928 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: F586835082F632DC8D9404D83BC16316)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "apoio.cliente@asfaltolargo.ptApoioCliente2018!mail.asfaltolargo.ptamorimoffice6@gmail.com"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1c-6Y7E6EFCnEfeUqjiCzqb4bjj7oMV7b"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.18483403549.0000000002A10000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000002.23244260810.000000001D881000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.23244260810.000000001D881000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000000.18323333088.0000000000F30000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: CasPol.exe PID: 3872	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

NDIS Filter Driver detected (likely used to intercept and sniff network traffic)

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

Persistence and Installation Behavior

Sample is not signed and drops a device driver

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

DLL side loading technique detected

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Remote Access Functionality

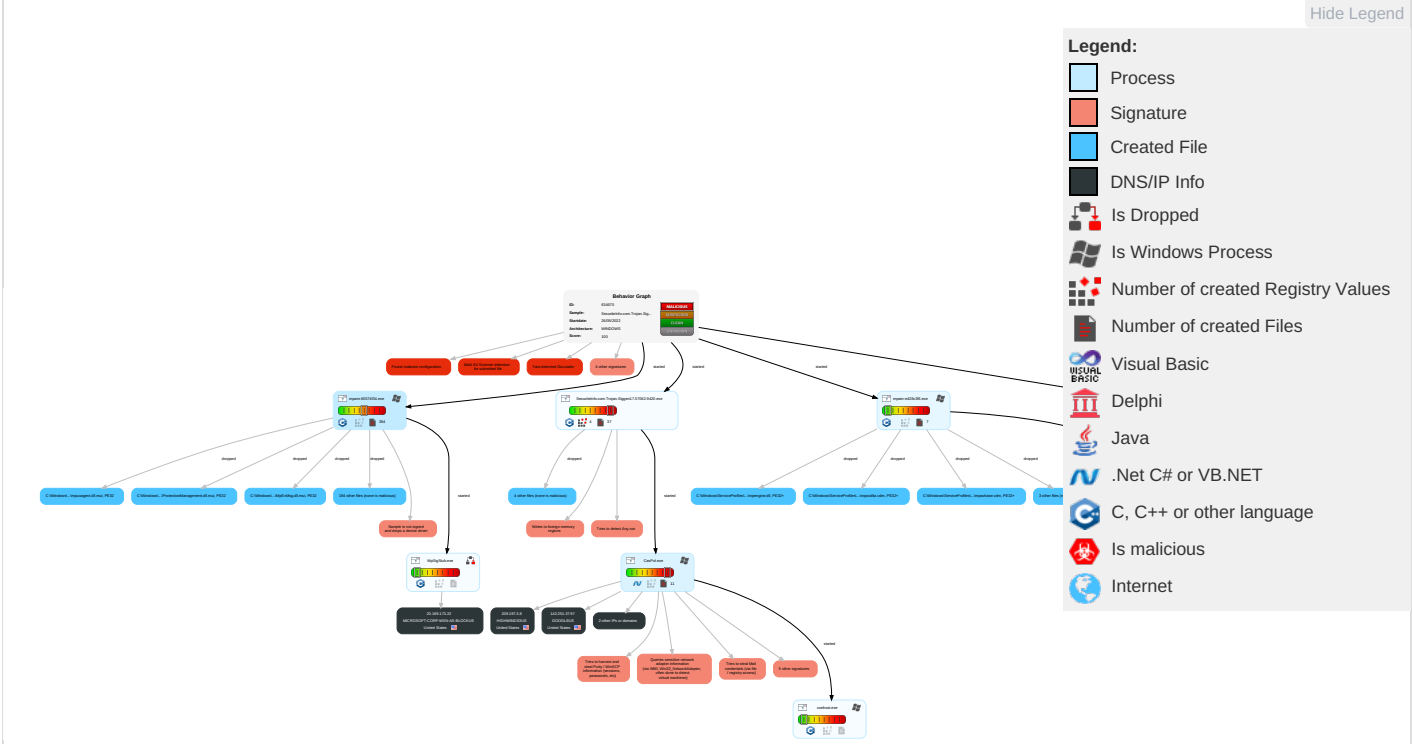
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 LSASS Driver	1 LSASS Driver	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Native API	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Network Sniffing	2 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	2 2 Windows Service	1 Access Token Manipulation	2 Obfuscated Files or Information	1 Credentials in Registry	1 Network Sniffing	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Service Execution	Logon Script (Mac)	2 2 Windows Service	1 Software Packing	NTDS	1 4 8 System Information Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 1 2 Process Injection	1 Timestomp	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 DLL Side-Loading	Cached Domain Credentials	3 7 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	2 5 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Masquerading	Proc Filesystem	2 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Modify Registry	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	2 5 1 Virtualization/Sandbox Evasion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Access Token Manipulation	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 1 2 Process Injection	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

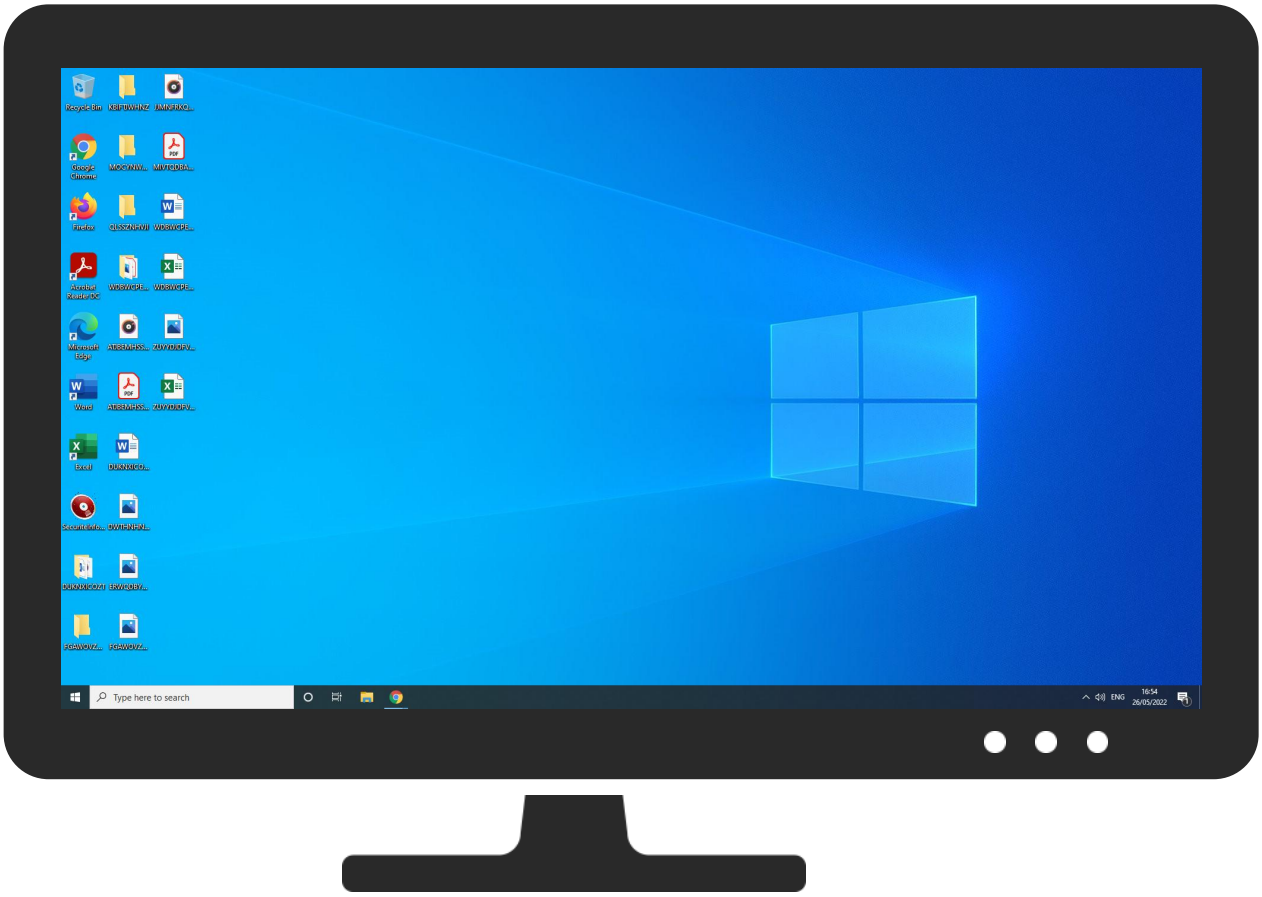
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe	31%	Virustotal		Browse
SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe	22%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsd7AB8.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsd7AB8.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	0%	Metadefender		Browse
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	Virustotal		Browse
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3.crl0	0%	Virustotal		Browse
http://www.certplus.com/CRL/class3.crl0	0%	Avira URL Cloud	safe	
http://ocsp.suscerte.gob.ve0	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	Virustotal		Browse
http://crl.dhimyotis.com/certignarootca.crl0	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	Avira URL Cloud	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	Avira URL Cloud	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://www.suscerte.gob.ve/dpc0	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://policy.camerfirma.com0	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	Avira URL Cloud	safe	
http://https://owWZDyjXwQrXMrJH.org	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	Avira URL Cloud	safe	
http://microsoft.co	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	Avira URL Cloud	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	Avira URL Cloud	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://https://owWZDyjXwQrXMrJH.or	0%	Avira URL Cloud	safe	
http://passport.net/tb	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0	0%	Avira URL Cloud	safe	
http://https://owWZDyjXwQrXMrJH.orgt-	0%	Avira URL Cloud	safe	
http://ac.economia.gob.mx/last.crl0G	0%	Avira URL Cloud	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	Avira URL Cloud	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	Avira URL Cloud	safe	
http://www.accv.es00	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://mail.asfaltolargo.pt(	0%	Avira URL Cloud	safe	
http://OGHYwH.com	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	Avira URL Cloud	safe	
http://www.acabogacia.org0	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	Avira URL Cloud	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	Avira URL Cloud	safe	
http://www.rcsc.lt/repository0	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/0	0%	Avira URL Cloud	safe	
http://www.correo.com.uy/correocert/cps.pdf0	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crt08	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	Avira URL Cloud	safe	
http://https://unitedstates4.ss.wd.microsoft.us	0%	Avira URL Cloud	safe	
http://https://unitedstates1.ss.wd.microsoft.us	0%	Avira URL Cloud	safe	
http://www.oaticerts.com/repository.	0%	Avira URL Cloud	safe	
http://www.ancert.com/cps0	0%	Avira URL Cloud	safe	
http://ocsp.accv.es0	0%	Avira URL Cloud	safe	
http://crl.mV	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	0%	Avira URL Cloud	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	Avira URL Cloud	safe	
http://mail.asfaltolargo.pt	0%	Avira URL Cloud	safe	
http://crl.defence.gov.au/pki0	0%	Avira URL Cloud	safe	
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel05	0%	Avira URL Cloud	safe	
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	0%	Avira URL Cloud	safe	
http://www.comsign.co.il/cps0	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3.crl0	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.vmware.com/0	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe, 0 0000001.00000002.18481621853.00000000004 0A000.00000004.00000001.01000000.0000000 3.sdmp	false		high
http://ocsp.suscerte.gob.ve0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601190951.000000002072C000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601324854.0000000020738000. 00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601505288.000000002083F000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518 207.00000000207A0000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.swisssign.com/0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682976608.0000000020819000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18602026 559.0000000020837000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 005.00000003.18599518207.00000000207A000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682774918.000000002073F000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18601324 854.0000000020738000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000005.00000003.1968362504 0.000000001F957000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23253192039.000000001F95A000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Azure/azure-storage-cpp)	mpam-60574f34.exe, 00000010.00000003.187 40725593.0000016C07975000.00000004.00000 020.00020000.00000000.sdmp, mpam-60574f34.exe, 00000010.00000003.18740268669.0000016C07975 000.00000004.00000020.00020000.00000000.sdmp, mpam-60574f34.exe, 00000010.00000003.1873739 2209.0000016C07BA1000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/dpc0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601190951.000000002072C000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000005.00000003.1968362504 0.000000001F957000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23253192039.000000001F95A000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.registradores.org/normativa/index.htm0	CasPol.exe, 00000005.00000003.1860060071 4.0000000020744000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://policy.camerfirma.com0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.anf.es/es/address-direccion.html	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	CasPol.exe, 00000005.00000003.1860215662 0.0000000020831000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601505288.000000002083F000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518 207.00000000207A0000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://owWZDyjXwQrXMrJH.org	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23246237802.000000001D9BE000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.23245892 965.000000001D994000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	CasPol.exe, 00000005.00000002.2325304444 3.000000001F941000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23255549826.000000002079C000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.23245892 965.000000001D994000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	CasPol.exe, 00000005.00000003.1860091957 8.0000000020866000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://microsoft.co	MpSigStub.exe, 00000013.00000003.1880858 5691.000001F8CEA95000.00000004.00000020. 00020000.00000000.sdmp, MpSigStub.exe, 0 0000013.00000002.18818438522.000001F8CEA 95000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certicamara.com/dpc/0Z	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601324854.0000000020738000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	CasPol.exe, 00000005.00000003.1860091957 8.0000000020866000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/msangcwam	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp, svchost.exe, 00000 01D.00000003.21976530622.000002C168D2900 0.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.21977267020.000 002C168D2C000.00000004.00000020.00020000 .00000000.sdmp, svchost.exe, 0000001D.00 000002.23221533613.000002C168D37000.0000 0004.00000020.00020000.00000000.sdmp, sv chost.exe, 0000001D.00000003.21976659587 .000002C168D2C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://owWZDyjXwQrXMrJH.or	CasPol.exe, 00000005.00000002.2324557723 5.000000001D986000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://passport.net/tb	svchost.exe, 0000001D.00000002.232204854 37.000002C1682B0000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltrust.info0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe, 0 0000001.00000002.18481621853.00000000004 0A000.00000004.00000001.01000000.0000000 3.sdmp	false		high
http://https://owWZDyjXwQrXMrJH.orgt-	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ac.economia.gob.mx/last.crl0G	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-0g-34-docs.googleusercontent.com/	CasPol.exe, 00000005.00000003.1845974789 4.00000000013AF000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23219964862.0000000001367000. 00000004.00000020.00020000.00000000.sdmp	false		high
http:// www.accv.es/fileadmin/Archivos/certificados/raizaccv1. crt0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.symauth.com/rpa00	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe, 0 0000001.00000002.18481621853.00000000004 0A000.00000004.00000001.01000000.0000000 3.sdmp	false		high
http://crl.oces.trust2408.com/oces.crl0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://eca.hinet.net/repository0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://certs.oaticerts.com/repository/OATICA2.crl	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es00	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com/V%-	CasPol.exe, 00000005.00000002.2321960962 8.000000000132B000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://mail.asfaltolargo.pt(	CasPol.exe, 00000005.00000002.2324589296 5.000000001D994000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_ 1.pdf0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://OGHYwH.com	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

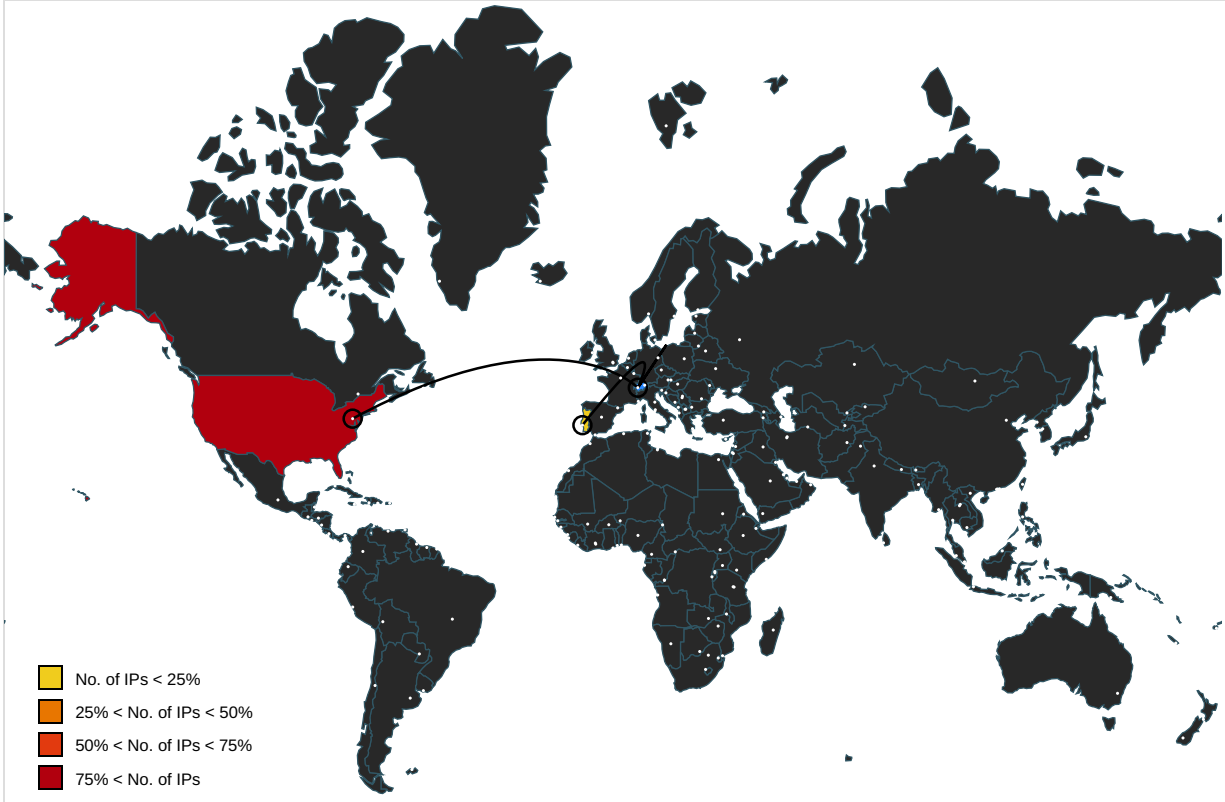
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-int0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18602026559.0000000020837000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518 207.00000000207A0000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://github.com/open-source-parsers/jsoncpp.git)	mpam-60574f34.exe, 00000010.00000003.187 40725593.0000016C07975000.00000004.00000 020.00020000.00000000.sdmp, mpam-60574f34.exe, 00000010.00000003.18740268669.0000016C07975 000.00000004.00000020.00020000.00000000.sdmp, mpam-60574f34.exe, 00000010.00000003.1873739 2209.0000016C07BA1000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.acabogacia.org0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.firmaprofesional.com/cps0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682296383.0000000020824000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.securetrust.com/SGCA.crl0	CasPol.exe, 00000005.00000003.1860119095 1.000000002072C000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rcsc.lt/repository0	CasPol.exe, 00000005.00000003.1860202655 9.0000000020837000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.19682472 622.000000002083C000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.quovadisglobal.com/cps0	CasPol.exe, 00000005.00000003.1860060071 4.0000000020744000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	CasPol.exe, 00000005.00000002.2325509276 3.0000000020728000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23253044443.000000001F941000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.23245892 965.000000001D994000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.i.lencr.org/0	CasPol.exe, 00000005.00000002.2325509276 3.0000000020728000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.23253044443.000000001F941000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.23245892 965.000000001D994000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.correo.com.uy/correocert/cps.pdf0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://signup.live.com/signup.aspx	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp, svchost.exe, 00000 01D.00000002.23221533613.000002C168D3700 0.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.chambersign.org/cps/chambersignroot.html0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://unitedstates4.ss.wd.microsoft.us	NisSrv.exe.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/check2?crx3=true&appid=%7B430FD4D0-B729-4F61-AA34-91526481799D%7	edb.log.4.dr	false		high
http://https://unitedstates1.ss.wd.microsoft.us	NisSrv.exe.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://www.anf.es/AC/RC/ocsp0c	CasPol.exe, 00000005.00000003.1968297660 8.0000000020819000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp, svchost.exe, 00000 01D.00000003.21977267020.000002C168D2C00 0.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.21976659587.000 002C168D2C000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	MpSigStub.exe, 00000013.00000003.1875256 8256.000001F8CDE3B000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.oaticerts.com/repository.	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ancert.com/cps0	CasPol.exe, 00000005.00000003.1860060071 4.0000000020744000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.accv.es0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80605	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp, svchost.exe, 00000 01D.00000003.21976530622.000002C168D2900 0.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.21977267020.000 002C168D2C000.00000004.00000020.00020000 .00000000.sdmp, svchost.exe, 0000001D.00 000003.21976659587.000002C168D2C000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://crl.mV	MpSigStub.exe, 00000013.00000003.1880858 5691.000001F8CEA95000.00000004.00000020. 00020000.00000000.sdmp, MpSigStub.exe, 0 0000013.00000003.18809059455.000001F8CEA A7000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80604	svchost.exe, 0000001D.00000002.232198181 27.000002C168241000.00000004.00000020.00 020000.00000000.sdmp, svchost.exe, 00000 01D.00000003.21977267020.000002C168D2C00 0.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.21976659587.000 002C168D2C000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	CasPol.exe, 00000005.00000003.1860215662 0.0000000020831000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.echoworx.com/ca/root2/cps.pdf0	CasPol.exe, 00000005.00000002.2325618756 5.0000000020822000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682976608.0000000020819000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518 207.00000000207A0000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	CasPol.exe, 00000005.00000003.1860060071 4.0000000020744000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-std0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18602156620.0000000020831000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18600600 714.0000000020744000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 005.00000003.18601324854.000000002073800 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518207.0000 0000207A0000.00000004.00000800.00020000. 00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.asfaltolargo.pt	CasPol.exe, 00000005.00000002.2324589296 5.000000001D994000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://g.live.com/odclientsettings/Prod/C:	edb.log.4.dr	false		high
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601324854.0000000020738000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.defence.gov.au/pki0	CasPol.exe, 00000005.00000003.1860215662 0.0000000020831000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel05	CasPol.exe, 00000005.00000003.1860100328 0.0000000020731000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18601324854.0000000020738000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pki.gva.es/cps0%	CasPol.exe, 00000005.00000003.1860202655 9.0000000020837000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.cert.fnmt.es/dpcs/0	CasPol.exe, 00000005.00000003.1859951820 7.00000000207A0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682296383.0000000020824000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-bt0	CasPol.exe, 00000005.00000003.1860091957 8.0000000020866000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.19682976608.0000000020819000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.18599518 207.00000000207A0000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 005.00000003.18601190951.000000002072C00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.comsign.co.il/cps0	CasPol.exe, 00000005.00000003.1860150528 8.000000002083F000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000003.18599518207.00000000207A0000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000005.00000002.2324426081 0.000000001D881000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.110	unknown	United States		15169	GOOGLEUS	false
94.46.30.74	unknown	Portugal		24768	ALMOUROLTECPT	false
142.251.37.97	unknown	United States		15169	GOOGLEUS	false
209.197.3.8	unknown	United States		20446	HIGHWINDS3US	false
20.189.173.22	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.11.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634670
Start date and time: 26/05/202216:44:19	2022-05-26 16:44:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@21/253@0/7
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 78.3% (good quality ratio 64%) • Quality average: 59.6% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, backgroundTaskHost.exe
- Created / dropped Files have been reduced to 100
- Execution Graph export aborted for target mpam-60574f34.exe, PID 2156 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:46:20	API Interceptor	2x Sleep call for process: svchost.exe modified
16:46:43	API Interceptor	2805x Sleep call for process: CasPol.exe modified
16:47:15	API Interceptor	1x Sleep call for process: MpSigStub.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.36462066590313524
Encrypted:	false
SSDEEP:	12:hu77eaaD0JcaaD0JwQQv7u77eaaD0JcaaD0JwQQv:hu77etgJctgJwn7u77etgJctgJwn
MD5:	72C73518694031F3E9CA1BA887CBAF3A
SHA1:	68D3E3605779412D038017B2F2AD2D0297DE82B7
SHA-256:	798EC47E6718B444DDE82A405DAB96E750F8839A0FA4B980B69D1C456C307B2F
SHA-512:	70A13B83E2FFB91EBED531A8E3694732008F15E1CC82CC0B874F9CB6D1F2B6DAC004803CDCA4D3B1D667EA7019BBA6B3DD31DE6D26DF0C466BAB162627CA F0D
Malicious:	false
Preview:	..U.....5.....).*9...y.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....5..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	1.411603014286152
Encrypted:	false
SSDEEP:	3072:PJyugY9cTJm58j7cX7g1wbyECkTGth8Y4P49+FmFYVpwDpJHuUl:ED4m
MD5:	A510A4E812F12E5ADBD43E4CC6EA307E
SHA1:	379C9BDA2D6AB38CA6C0F2DE2CEFDB7836875579
SHA-256:	44CDCD47881E77D70FE3C66435BA6379FADBF2BC0E8C04020A567ADAE9BD0C9E
SHA-512:	1B4010C8DB7234FA67C26ADBE97F5BD5083BC1085CED37939501513434DC22801AA4DA5C8A566E86F6FBF1F2B2C70F90BF69B1B1D832D2AB2062165FA08A63F E

Malicious:	false
Preview:	;g.....@..@.*...yo.*9...y.....<.....).*9...y.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....;.....a..hd..#.....`h.....h.<.....C::\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x4a9d9835, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.6946944573199703
Encrypted:	false
SSDEEP:	1536:zSB2qSB2gSjlK/vfS+NEh2ZhV88/bGLBSBLil23/3n8n/3A5v7GoCnLKxKHKr0Gt:zapaCK0DfOD8F31Xw
MD5:	BF8326B8CD8E193D830B09383486BF41
SHA1:	224E92699640C7D156AA96E5CA0CDF2FA3835620
SHA-256:	163325BF63D764E53575061F4582E7FB929F009C30381E2999F5BA541F3F89A6
SHA-512:	C0B64CFC193CBA3B875C765631F831D70AA6B6333B055557568C3985C1D67066C1AFB0BEF7B81197E90778A9D5445F07C6DB962DC3D1684CCE0482F9BE89E4AE
Malicious:	false
Preview:	J..5... .....\.....p..*9...y.....6.4.....70...z.....z..h.3.....70...z..6.4.....).*9...y.....bJ.....n....@.....l./.70...z.....6l.j70...z.....#.....6.4.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07826128739789665
Encrypted:	false
SSDEEP:	3:kul2cprRqvSagxqCvQW6uRllTOE5xtllJlbxvws:kq9MvSagxqCvQjQpOE5J
MD5:	3531E7FAF8F35B23655FD4748988C379
SHA1:	5FA66B3BCF43126A8EBB064525CF61DDBDCEB1EA
SHA-256:	0752112651925BCB68D2B674E87601BDA01262B4F64E0EB164C67B13886C707B
SHA-512:	F3CD94F36C3F93747434B3E033ACF8791F402ACC368588BC62503E70A7D5194E9347ECFFF52854C5CC1BB07FB59041C99C643313C039F9AF686AA0C174D5747
Malicious:	false
Preview:	.-x.....*9...y.....z..70...z.....70...z..70...z.....60...z.....6l.j70...z.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE3.tmp.WERInternalMetadata.xml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8020
Entropy (8bit):	3.706257493240483
Encrypted:	false
SSDEEP:	192:R9l7lZNiApxD6YkqiugmfqrAzTp11imfIEAHm:R9lnNimxD6YZTgmfsAj1TfIE9
MD5:	4F11F9210B61101E3201E072338341AA
SHA1:	47F5229ADB85964F18CC84931A8132C3ABC128C9
SHA-256:	58FAF8253A9013B2FC1EEAA23995BBE48CFC915BDD72976714EE7E4AC11B6966
SHA-512:	B737D5E5DCBA4CBEF7C0A30667F2F01275D65169F8AA65D92D66E3DA68EEC4C816A47B265938FDB7826A013A83B610D118543651983E70EB6293E2760381E52
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.9.0.0.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BDE.tmp.xml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4887
Entropy (8bit):	4.536670258763977
Encrypted:	false
SSDEEP:	96:uINfX7y8ySPf17JFKMxtb2iW/xtbdu+aTBd:uIJy8ySXHdxtWxtRCT/
MD5:	88469B220C15534AF3FA48C07BA4E6E9
SHA1:	A8C095C8CE2CDF7B338C975B8E46C45288F9C466
SHA-256:	44E18775A34CC9D803FA446EB44F299F667CA032E9FA86A99C6DB5BD198C24C8
SHA-512:	1924D2B50102CDB138F1C7C5977FFE4F61E464CC3E9DECCE1007346E4E528BE84D09E30BF7E1CF5F2229957AA2B8F2C35C261C63B7C0DD7740F439C5EC2AE7E4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="221631509" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C1C.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	60346
Entropy (8bit):	3.0516963968700885
Encrypted:	false
SSDEEP:	1536:Drszt4VjYp2rcgzEdjaeKE8vFETndMpjaq4Vf:Drszt4VjYp2rcgzEdjaeKEGFETndMpjw
MD5:	0AC1B92281A819542DDFF246DF86F6EE
SHA1:	9E771F3FDF5147D34737A82CB4BA7299D7C0DF3F
SHA-256:	AD84ED73711E44B7603DE3B8347F3E7EA51209AD33C97E29301C1E8DA2F0D638
SHA-512:	08BB1FD3D7F8A20E3907BCA50CE0E9E8156983B2A5760BE1114963A9F2180A8675D429CF239017B26CA9EBFB0C6F34017A4227EA27A37C3A9F61B9A1CFD10A34
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D45.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.700660211105054
Encrypted:	false
SSDEEP:	96:KilQHKkO4lYtYaYRaWjC7DHFYEZvftWiv510bwkBNG2auyCMgzYIUn3:flQHAd8XO7G73auyCMgz/Un3
MD5:	2CECE6A0A5C1E7DBC7EC246415D3376C
SHA1:	E92ED0DF402C995E31885FE2BE26130C7BD11D7A
SHA-256:	97E6C3B0D28FD27C3455BFFF12A735B342DF4D7E1EDE5A9B47D814D5E5AC7531
SHA-512:	56FAC0C3EE56AA86BE388625A48F0F2255854ADD2AE260D8D61A91961DD8B4B419BC7672FA1C0B014B1C71F9E7AD6BCD3DB23A4BAD136EDAFCDE749717527FCF
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .4.0.7.0.6.2.1.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .4.6.3.8.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**
SSDEEP:	1536:NATLwfiuePkACih0/8uIwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9
SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C..t.z.,x.00.1``L.....L.\..1.|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x..T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...I.....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.I...p2.(4k.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a..y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....."....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...I....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E..NF.....{o.h]}p....G..$..4...;..&.O.d....v:Ik.T..ObLq..&.j.j...B9.(..!..\.:K`.....:O..N....C..jD:.i.....1.....eCo.c..3o.....nN.D..3.7...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1122533135601187
Encrypted:	false
SSDEEP:	6:kK+/mN+SkQlPlEGYRMY9z+4KlDA3RUecl7PG1:WtkPlE99SNxAhUecl61
MD5:	BFE0683837571F3E3DDAF578E7F6FBF0
SHA1:	D621A6FEF262EF61F36AE6C475F2A678EE7FE0CA
SHA-256:	4D1A1E1D4D637CB2185508B6516A8C97D5230827CEF498260BF22B3805A81C93
SHA-512:	44CA52C64BEE574C7F0EF58236D5BFD39634992396AB5EBF0F98D6218D756974C7BB4FD76B81213EC06A619B9E5FF7AFF0DBAD7F25C85C7BABF49A7CF3178AE7
Malicious:	false
Preview:	p..... .....i.q..(..... ....3f..o.....&.....$...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.3.3.6.6.b.4.9.0.6.f.d.8.1.:.0."...

C:\Users\user\AppData\Local\Temp\Adventure_19.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	10521
Entropy (8bit):	7.888779038440803
Encrypted:	false
SSDEEP:	192:oXRZxdt62XpqRigPYtY0CfKTQlh5NKW6F5oJxfskCjGmXa6Pbpwr4WmKM:KRfdt62X+XoElh/KW6ifskEGeaIpwr4n
MD5:	8D61CCB44C962D7831FB6703B4AF623D
SHA1:	2BFDC667151057B3A42CDD22F9EB0E5AB0B0EF3C
SHA-256:	1EFFB5A4A46B05C024518546D4C8BBB45AD3496590E3E86AF533CF31C61512F4
SHA-512:	FE0C304F73713552ACA3A28D9CCD6BD2C53A45F72052892CC8F94D835A213F2F3C4D8D1656BD8160AE874A63FACC6B79BA763D4A724281E5F0DEDAC87F8637E
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..9...k....X.....&.2.Z.....k~I.....e...J...}..<..M..8....."../...O.u.....5.h...71]ZZ.....v..Yc...<.i'..m2_..>..#...K...,.qq.^<2\|D.V...j..ae.0Mu.^K..#k..3<."F V$HV.)..vmG..H.....z.\..#.....3_..Wo.g.>.o.....|...V.}.Ho.]...q#..W667Z`..)..I._E'....+\.w..K....O.o..5.....4O..~.

C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	58368
Entropy (8bit):	5.856484138583398

Encrypted:	false
SSDEEP:	768:t2y20tpnvfSd9bbM9tmRtTkwv9QMdVk1QKVnjphRJy26xG0XFC19Io:J20t1SdN0kvZ9pdW1QKVjzy26opD
MD5:	D600D4F40A2BE641991044EE0814BFA4
SHA1:	3BDEF3488C28D43D285C47F46B82B980A8F41CD8
SHA-256:	B0D12A7AADF51B02D52E9E88295E6E6606F68C1508C8D9323B6549AA20EC82AA
SHA-512:	27B125260AA56FCAD4153A3259ECFB898681C9B096A4A37EB32AC3B722599EA4BFB5BF00F0247136F11F73F280B85844B37F6236331A0EF3B90ED2EC70CEDA5 5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d...Kc..........."...0.................. .....@..... ....`...@......@.............. ...................................................................8............................................................ ..H............text........ ...................... ..`.rsrc...............................@.. @...H........W..4...N.((.....tS...}....*F.{....o....s....*F.{....o....s....*.0..........{....o.....s.......&.....*.................J.{....o.....s. ...*..((...*~.().....tV...}......s....}....*2.{....o....*2.{....o....*F.{....o....s....*2.{....o....*2.{....o....*F.{....o....,..*.*2.{....o....*2.{....o....*2.{....o....*2.{....o....*2.{....o....*:.s....%.}y...*..(....*:. ().....}....*..(*....,...}....+.r...ps+...z.....s4...}....*.0......

C:\Users\user\AppData\Local\Temp\Sites.UDP

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	data
Category:	dropped
Size (bytes):	97029
Entropy (8bit):	6.67352029006038
Encrypted:	false
SSDEEP:	1536:PQ0kJrmEiFGh45tzVKadkb4qe6BGcC44gtRujckzMc:PpkRmEiYh45tzV+NCcQQMX
MD5:	CCE79E361FEFB787AD2911F654EEAEB9
SHA1:	164FE9DCB6455C6842E01C4106E45151F7B1AFE9
SHA-256:	EFC22B0DFEC2B8D339747108AD6EFA9975FD950B73120E98B62B96EDC31BD2D0
SHA-512:	F43D00D16CBDA19B6D9E5A48EB2FFA2E3EC407B17E72892C4266A0DAB79F472F26473C241DFA923C8C92F9B8FC69E0D34DE611626F83BE6FDC460AE62E7F41 6E
Malicious:	false
Preview:	.w.s...s..f...f.f..5=...EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE..f...f.s.~..f....i..*.%n../..r@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@f!...f.c...f.u......$..."vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv...........2i.AE.. .....f....j.......(..Ilkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk.i~.....n..........!.].C+++++++++++++++++++++++++++++........o....5...y...f..........;84... ....9q.6...f.......a..t.......#...w....................................z....f.f......#z..txxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxf..............f.... ...mY111111111111111111111111111!...f.........'q*%.nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn.........f.k..*..y..e.....v....3............................. ....t.f.........8..e'.............

C:\Users\user\AppData\Local\Temp\emoji-body-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	193
Entropy (8bit):	6.41289035005742
Encrypted:	false
SSDEEP:	6:6v/lhPys693pMeNKrccoz4OtOOFImbTM0t7zlyH//jp:6v/7adpfNWcVkqfTMyUf1
MD5:	F492568998D5783731D50D7CA73AC7A3
SHA1:	E87B96367BDB02176067336A1CCE3B32EBDCB3B2
SHA-256:	7A08D7B1CC724A453A0C3EB2F36369D7FD6AC6BD965CE0B4D075D570ED369A9B
SHA-512:	2C6C726426EA6DD4C7CCC141152E24DD46BDB11D3DB45ED7BA6EAC06DE922F69E5172D5431D63B9ACF96E54B89857317CA0F87880F7B03C43AF9F7416EE95 73
Malicious:	false
Preview:	.PNG........IHDR................a....sBIT....|.d....xIDAT8.....0.E..#d.{Gp.k.q.WP....,m..$.BH....s...A<...9..L..Fp.E..7......`......6.n....]b.5...P.....r.W..#....U_....p.P.>.&.1.....IEND.B`.

C:\Users\user\AppData\Local\Temp\iso_639-3.xml

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1063988
Entropy (8bit):	4.881622518734141
Encrypted:	false
SSDEEP:	6144:z6ZdTZZl/WX4fVLcf9MvAadpxr5+ZiVHPZ6TZXjcePr:z6nTZZl/WX4fVLcqvV5+ZiX6TZXJ
MD5:	DCAD3B0F729144CE9EE9A6006D9C3E74
SHA1:	3EEF5F61BEF834B7089A87423D128990A1065E81

SHA-256:	D8AB9C2641481645A8ACF875FFA3E3CB271D2CD946691DD8E0BD48513FFF1370
SHA-512:	BB0ED1F9FBB122728776731B04C54C8FBA57BF2987D04DAD1167FC879FC8A2483093E1A8304A021D6238B408FED826E902386D7DB52B7988CE9DCC89ACB6461
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" ?>.... ....WARNING: THIS FILE IS DEPRECATED.....PLEASE USE THE JSON DATA INSTEAD.....Usually, this data can be found in /usr/share/iso-codes/json.....This file gives a list of all languages in the ISO 639-3..standard, and is used to provide translations via gettext....Copyright . 2005 Alastair McKinstry <mckinstry@computer.org>..Copyright . 2008,2012,2013 Tobias Quathamer <toddy@debian.org>.... This file is free software; you can redistribute it and/or.. modify it under the terms of the GNU Lesser General Public.. License as published by the Free Software Foundation; either.. version 2.1 of the License, or (at your option) any later version..... This file is distributed in the hope that it will be useful,.. but WITHOUT ANY WARRANTY; without even the implied warranty of.. MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU.. Lesser General Public License for more details..... You should have received a co

C:\Users\user\AppData\Local\Temp\lgpllibs.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37816
Entropy (8bit):	6.374742588554942
Encrypted:	false
SSDEEP:	384:VbijnYW+DZZMwrusWsWQfRl30fP5/A5KFUkYvntA/QcP+ACxw/3MvDG/GhUVgt:dijnQDnzruRNQfv0fP5/oABCDGehHt
MD5:	9B623087B905D8FE157BDB7EC85009A8
SHA1:	4B6DD4C0292558513A840B40A991533735D55E02
SHA-256:	7FA4C9EA4BE0088D6D311BD93FA65BAF8828DA32A2FD4BF8CE0EADE552D46246
SHA-512:	8C06714F93EB05FAD19F1A96C0DB8FF030B1CD3C03D6B17C231CDE5BCE8DD8358014D87A74306C3BABEF7C573D4AF5AE80904AFBB0329D2D83FE3758EF02019
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...>..b....." .....F...*.....P.....`A.....@g.....n..x.....t.....Te.....`.....o..X.....text...FE.....F..... ..`.rdata..p....`.....J.....@..@.data...@.....d.....@....pdata.....f.....@..@.00cfg.....l.....@..@.rsrc.....n.....@..@.reloc.....r.....@..B.....

C:\Users\user\AppData\Local\Temp\microphone-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1401
Entropy (8bit):	5.11645334711433
Encrypted:	false
SSDEEP:	24:t4Cjlza3LWdwpQiL6Rch3jV81hF3Q59UPFkyKbRAecFhBrN3AGMH:1cL8w6iJjV8jF3894kNtAecFZTMH
MD5:	BAE5EB7B918D568E955B8885EEB5DB5A
SHA1:	FC4421C6A019D0147A13B08CBB2F0720F49E17C3
SHA-256:	273F11F9F8BD84F2A32E0CC857E21050A9A9C7713F33D9A220991DC232C470BA
SHA-512:	8A6AE1E26C9451A241655242D16368D87E23036D03D61FF75F5669D5E2930446D6003D5191622F576060E529EE21DD6E28D3408D28719A4D53BD291E673037B0
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <g fill="#2e3436">. <path d="m 213.531,228.469 -1.061,1.061 14,14 1.062,-1.062 z" transform="translate(-212 -228)"/>. <path d="m 220,228 c -1.662,0 -3,1.338 -3,3 v 1.64453 l 5.2832,5.2832 C 222.72383,237.4058 223,236.73965 223,236 v -5 c 0,-1.662 -1.338,-3 -3,-3 z m -6,6 v 2.00977 c 0,2.96574 2.16538,5.4238 5,5.90039 V 244 h 2 v -2.08984 c 0.64598,-0.10861 1.24984,-0.33194 1.80859,-0.62891 l -1.11132,-1.11133 C 221.17391,240.38 220.60353,240.5 220,240.5 c -2.50669,0 -4.5,-1.99014 -4.5,-4.49023 V 234 Z m 10.5,0 v 2.00977 c 0,1.15729 -0.44099,2.19439 -1.14844,2.98632 l 1.05274,1.05274 C 225.38802,238.9836 226,237.57264 226,236.00977 V 234 Z m -7.5,1.47266 V 236 c 0,1.662 1.338,3 3,3 0.16422,0 0.3216,-0.02370.47852,-0.0488 z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-se

C:\Users\user\AppData\Local\Temp\nsd7AB8.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E

SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\printer-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	213
Entropy (8bit):	4.950492507724413
Encrypted:	false
SSDEEP:	6:tI9mc4slzcpG+xW6UmUuksJtjdU0t/ZME:t4Cp9xW6zUmjW0tOE
MD5:	A4ACDD85E11EA101F3BB4B5BEC3382F0
SHA1:	2DC81694D5D3C403BF696B1796385D2F64C40D77
SHA-256:	AD87999B06B9C8035CCAC8EF29D54C9E00055EE9E2DBDD9B7BA24CCF56C471E6
SHA-512:	6C7C1E913CBF7CD6B91721BD60705B3A87C398B5D69D1FA03D67EDF7C69E23AB410938EC5E0770584E5B6E218443E53A702BD389C2253F05C2D4F48B944D481 E
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z"/><path d="M4 9v5h8V9z"/></g></svg>

C:\Users\user\AppData\Local\Temp\svejtsers.for

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	40772
Entropy (8bit):	3.99958578967024
Encrypted:	false
SSDEEP:	768:hh1uZgY2aTsCYEHD/RZpbk9hCagM99A4jloFMSD2l:REsvEHFwOagq9AAo+SCl
MD5:	15B855905F2DE48867E35606D005ACC7
SHA1:	41A4B95539290FBE3F75449D7391F9B10710612C
SHA-256:	40F9C51DAF7AB04475F462927A471E4DA0D80D3F373327992A9464849360BA40
SHA-512:	88A65458C335446084B927EE1E97D38DC3CEF52E87494611D4F47A244AE11EA7B50ABE79813FC6635084E8E32BA99F722760B4B75741E9F7D7BC68B67A8580DA
Malicious:	false
Preview:	27593E14BF48762F251F42C3A0B162B4B932AF6F508F6C5236FD53D9593278373448EBED3E8F7995FDB755B160AC8ED7146290A48D0DAE23B6EFD36F CBE6AFD753ED6D2B3CD983BA7DFC9B4EE151DD47272BE33427DFEA4750F33928D8C7C721F80C5391864ECF3C5AA12CB96F9A14071AE993D3608E24FA 5B42AE924AC0E3266E1238BD9B228E4A11CA6E0613634F0F0FE72A38B123888727782AADA70E0B92A3C5CD216016D1CCD48A86C44A4812F8BD719D2F 09C4C40C860DA6D34EBE16FFB1176EB131F853DB2F1151441A075B4F90BB5A16EA834D0FC931C1D8D8DDD17F99974955D19FFD8D76AF3E4EA1F22066 4560A816B6F1C0EDCF0ED396877D1109F96A89AC469C883F3C9FA1E83A6FEA5F049F55E811D9C54E6DC54D98B9A791969B8218AC42C64A788F5DA9EE ECD6399ECB4C4A00A7F0ADA7836E7FCD2BE9D3407B3C2B4842D44E61CEC54A6F1121FA7074AD25B115F998C1453447D55053C9CC43CF76811579AE99 68C92BCBAA0F18D9F18BFE5BCD4FB4433244AF9A94561C69CA25F54989D680E77C18BA86CD924021075051D3C06915D4059FC8622C90B8485A0B3E4F FC555370308A14E68BABE11715B947CCF32EF583310BF8F49D615FD12C4980406AD24C6A12F84A2457F89395FF61F4BE47B9261B7C2270B0BE93BC9D 88BF45FED83D35EBA376F3B4CA09FC66FA76E903

C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	288328
Entropy (8bit):	6.5244639850667605
Encrypted:	false
SSDEEP:	6144:TWMbKY5G780mQB8fkrOX9rn8ndvcA5abagLgandSUbJ:aMbKY5AIvfkSX9rSdkfbanUbJ
MD5:	9ECB2FA510DCDF4BFB06DC80A83294BD
SHA1:	65E0CEC428D010B94D81BA784EA709EBA598A1CD
SHA-256:	865868E3BE461332134EFBBA9F1D8AAA5E29A0C8AD3F5A2AC47311F47D4CFD62
SHA-512:	6F70D42EE2A6CA1F2D85A84947B74EAD03FA4CD00AE5D897FC80832111D88B0D9EEFE81B5FFBC229AE9E1D97467713AF0D385C8C2E96D67B5E9008033C02CE 28

Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....[.....s.....s.....s.....M.....z.....z..... .....G.....Rich.....PE..d.....`......" .....j.....N.....`A.....p.....x!.....Hb.....8..... .....8.....4...@.....text..... ..`.rdata.....@..@.data...0#.....@....pdata..x!.....".....@..@.didat..`....@..... .....@....gehcont$....P.....@..@_RDATA.....`.....@..@.rsrc.....p.....@..@.reloc.....@..B..... .....

C:\Windows\Logs\waasmedic\waasmedic.20220526_155057_892.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	2.8216989048802654
Encrypted:	false
SSDEEP:	96:8k/25QZ0UC0Y0/0D0U9D0ClX0/0U9f0Clu0M0U9N0ClRy0Sv0U95v0ClBe09G:4+T8AyAZ8ycsHyqilSMy5M+xw
MD5:	4800A275A7677855810809E8C62AEE39
SHA1:	F9D641971EC8B2EA57AFA7BD1A5E05A1D203AFF1
SHA-256:	9486DD0EB9CFC87858D85D8F3D5E4EFE4C72B8BAF3799A7203EAFC83A08FAC77
SHA-512:	7FA93D18C29D675AC4ADF57A2931281895E7D9C063680821DB3A0256849F7AFD1A2314CB5A6D90174CBBD89C767EEA326ADFB7F0E9EA9CE48E8F65BF51E9A54B
Malicious:	false
Preview:	.....!.....".."..0.....bJ.....R...q..Zb..... .....@.t.z.r.e.s...d.l.l.,.-.2.6.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.6.1.....@....q.....d.q.....E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:. \.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.2.0.5.2.6._.1.5.5.0.5.7._.8.9.2...e.t.l.....P.P..".0.....8.B. .....19041.1.amd64fre.vb_release.191206-1406.....5.@.....u.5.%Nb.f.};.....WaaSMedicSvc.pdb..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\03A7312A-3D2B-4807-84DA-352D7F06B3B6MPTelemetrySubmit\client_manifest.txt

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	2.9588664479635254
Encrypted:	false
SSDEEP:	3:Q9lJWlARl9OEBlZTlJlkARl9OEBlo1ln:Q9lYaEETdXEETovn
MD5:	78832DCD6FF89BA04F6DC8EEAEA25351
SHA1:	AF126BDDE978CB20A76712C2814053FC283A2E66
SHA-256:	FD13D1B3B4DB4D12A6BE71C07FB6536F83EF00782900E919E76BE7726510DB28
SHA-512:	C649D4EF86108E109E63893568EACF1C7C68874BB046E2EF82E7E109E5FC1F2ADC5CC8E367A1D4CD0EF31BBA509C679FD1F0C61FBCFFDB0E58D4454C168D1A2D
Malicious:	false
Preview:	.....<.C.l.i.e.n.t.D.a.t.a.>.<./.C.l.i.e.n.t.D.a.t.a.>.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\03A7312A-3D2B-4807-84DA-352D7F06B3B6MPTelemetrySubmit\watson_manifest.txt

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1064
Entropy (8bit):	3.8155988132499155
Encrypted:	false
SSDEEP:	24:QaJlJzYBnjRkBDulC5Fg+u/1uW8sQ+u/1s24H:pJlJzKjaDZ56TuW8jTs24H
MD5:	2B6DE041139EB4CE6AF158056A8F1428
SHA1:	A69D321BB7B41B20936C2266AA71F7CF9704EA19
SHA-256:	EDDDA79261CD3FB39B8B6CB142666B0DAFA6CF10E590800D00722B4D51F29061
SHA-512:	17212EB331AFCA634E0CA2E85BCA30FA81C0A8FA0C7CBC927E1CCBEA9DB4A839CA62D0EFD0E950810DA73BE81F0E3E00A666BECAF25FF554D0E6A477DF2AAD3A
Malicious:	false

Preview:	.....V.e.r.s.i.o.n.=.1.3.1.0.7.2.....U.I. .L.C.I.D.=.1.0.3.3.....U.I.F.l.a.g.s.=.1.....E.v.e.n.t.L.o.g.S.o.u.r.c.e.=.M.P.S.a.m.p.l.e.S.u.b.m.i.s.s.i.o.n.....R.e.p.o.r.t.i.n.g.F.l.a.g.s.=.0. ....L.o.g.g.i.n.g.F.l.a.g.s.=.0.....G.e.n.e.r.a.l._.A.p.p.N.a.m.e.=.M.a.l.w.a.r.e. .S.i.g.n.a.t.u.r.e. .D.o.w.n.l.o.a.d.....E.v.e.n.t.T.y.p.e.=.M.p.T.e.l.e.m.e.t.r.y.....P.1.=.0.x.8.0.0.7.0. 0.0.5.....P.2.=.V.a.l.i.d.a.t.e.U.p.d.a.t.e.....P.3.=.P.l.a.t.f.o.r.m. .u.p.d.a.t.e.....P.4.=.1...1...1.8.5.0.0...1.0.,.4...1.8...2.2.0.3...5.....P.5.=.m.p.s.i.g.s.t.u.b...e.x.e.....P.6.=.4. ..1.8...2.1.0.8...7.....P.7.=.M.i.c.r.o.s.o.f.t. .W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r. .(.R.S.1.+.).....F.i.l.e.s.T.o.K.e.e.p.=.C.:.\.W.i.n.d.o.w.s.\.S.E.R.V.I.C.~.1.\.N.E.T.W.O.R.~.1. \.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.0.3.A.7.3.1.2.A.-.3.D.2.B.-.4.8.0.7.-.8.4.D.A.-.3.5.2.D.7.F.0.6.B.3.B.6.M.P.T.e.l.e.m.e.t.r.y.S.u.b.m.i.t.\.c.l.i.e.n.t._.m.a.n.i.f.e.s.t...t.x.t.|.C. :.\.W.i.n.d.o.w.s.\.S.E.R.V.I.C.~.1.\.N.E.T.W.O.R.~.1.\.A.p.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	803176
Entropy (8bit):	6.37118649960636
Encrypted:	false
SSDEEP:	24576:Ghj1QlBYDgtUUvie3n+pB3+ojRlcD1VyZTFXk:GhpQlBHtBYla1VyZpU
MD5:	01F92DC7A766FF783AE7AF40FD0334FB
SHA1:	45D7B8E98E22F939ED0083FE31204CAA9A72FA76
SHA-256:	FA42B9B84754E2E8368E8929FA045BE86DBD72678176EE75814D2A16D23E5C26
SHA-512:	BEA5F3D7FB0984C4A71720F25644CE3151FCDC95586E1E2FFE804D04567AAF30D8678608110E241C7DDF908F94882EDDD84A994573B0C808D1C064F0E135A58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..#...#..#..EV...#...Q...#...Q...#...Q...#...Q...#...#..."..EV..#..EV N..#..EV...#..Rich.#.....PE..d.....P....."....`.....@.....0.....-....`..... .....t..d..... .....D... ..h!... .....d...p..... (.....8.....0.....text...2R.....`..... ..`.rdata.....p... ...p.....@..@.data..../..... .....@....pdata...D.....P.....@..@.rsrc... ....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	54948312
Entropy (8bit):	**7.996859326410134**
Encrypted:	**true**
SSDEEP:	1572864:CPq28JE9x4iAPQwYJtW3obwsDceQ1Gl184F+:AqtJE9xP4QNIobwsD3L8H
MD5:	DD086FDB797CF2C0DFA138261C8BAEFC
SHA1:	3E12FEA6552D567AB669E6659415AC6367CAAD18
SHA-256:	743214AC6F3792CED1EB51125839B4E57D920EFFCA3EDAD6FB138A5143F45833
SHA-512:	89CE6B88CD9A93B035622D2EB0FC1DC2EA0B3139781BC360CBE0930BAAD9CE651B570819826AC3405B7B125A25433329CC89A3335AA3A947582101D2520F7CF 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d.....b....." .....JF..... .....pF.....!G...`..... ...GF.....LF..%.....rdata..p..... ...@..@.rsrc....GF.. ...HF.....@..@.....b.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ...FF..rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3043800
Entropy (8bit):	**7.999448477784981**
Encrypted:	**true**
SSDEEP:	49152:Ijk5hufQfKN1bAmdKmAMXmbljVLv68aptx2GUJ/oXsQ4lMhTWqFXJ1GXzX2qUfX0:N54fQfi1AQKeXaJVm8avx2rssliLXDUv
MD5:	8CBC2B60224A4F682E9D656FB71954C2
SHA1:	D465A4DA40D8D83035333AA796EFDF097EFEFB28
SHA-256:	9B49D04FEBBB31F010813566BE5888F9A2FA830EDE1B2DF40DCFA3339FF81D5D
SHA-512:	3123EB98B87416845F2E19F6CF95DB797030F0F93232749AE36D424419458D685DF24953FCAD227806E930EA52AE2F610CD39EDA869C346443641C858BEE3980
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....@.b....." .....J..... .....p.....m./...`.....G.....L...%.....rdata..p..... ....@..@.rsrc....G... ...H.....@..@.....@.b.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ...F...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	46652896
Entropy (8bit):	**7.997138501518718**
Encrypted:	**true**
SSDEEP:	786432:v7hIRVH8K6Un3jWNai3DRf8XPlccGjxsB0V6MKIq781z+DR:DhIH8Kx3awCDR0t1Oxs4KIqdd
MD5:	BD5DD1EA1744FD5674150946BA28BE7F
SHA1:	7639206768C0BDDA308F0BB02D9E3FCCA134FE84
SHA-256:	F3DFDC237542CF9FB175C22F1A4651E7C7FAC5A136275B06F6982E607AC210E3
SHA-512:	0810F9362A362447D62A016C40607E0A44D544095288A9D8547C7727B3EA4CF2BCD2F37E920672279B603C97F473E0BA7E251EEE06E5088AEC49AF244C66C38D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d.....b....." ....|...`.....%.....rdata..p..... ...@..@.rsrc..... .....@..@.....b.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... .....rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	modified
Size (bytes):	1449944
Entropy (8bit):	**7.997957843381355**
Encrypted:	**true**
SSDEEP:	24576:PMEeDf+20iCoe5ItGGl/CGiAy9gLLKb546tha2P2mGIy4gzZyKiINTm2YDz/oaAl:PeDf+5do8It5/CQy9gLLKbCUha2PxsZt
MD5:	96F349289C1EC4B24F699FF444EDA90E
SHA1:	7BAD86AC34890316FF2682DA0BC02402B6F27EE7
SHA-256:	8E4B7CF3510F2947D24F8430BD537C3EC1959D5BEC9446E4282DE0E31F35F143
SHA-512:	49ABBF589F5C934037E2FF1A183B7873A10E5A8707C41983302F2186D2B28B33070C57313F4BA5B9EEA948AEC8E7107FF74A044E2201F6D6BD1BEDE81E23F6CA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....@.b....." ....4...`..... ..x.....%.....rdata..p..... ....@..@.rsrc...x.... .....@..@.....@.b.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... .....rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	17066504
Entropy (8bit):	6.424166167554763
Encrypted:	false
SSDEEP:	196608:QHBT6uO6seVHZh4LGWThrMhxHyiD2YMMC5+H9u2h+cKSO/k4XK:06Csu5h4Lj92HygC5Ou2hFJ4XK
MD5:	8DF74DEA21B6EF76B6B47DE4FD6F6A0A
SHA1:	7783D1CAABF1981248EC41496A631CD1F543F9BE
SHA-256:	A583E84A264435320A726C9BF2E25AB8C2DBB7989623C66ACDBB5B316BA825C1
SHA-512:	DDEE6CAE573B7BA791E64B9B2DCEE7CA0817F4532FEBCEF999435D4D89A8CE5273D915A20A201025B6023A4FC3A729439136FCE59C93A2B82301EED80C2F607A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7..V.V.V.x$.V.V.tW.$#.V.x$..V.x$.V.x$.WV.x$...V.$#.V.....V.$# ..uP.$#...V.$#.V.Rich.V.....PE..d...7&....." .....R.....zI.....Z..... ....`A.....d.....x~.....|.....j.....p..... ...(.....8.....0.....text..... ..`.rdata....<.....<.....@..@.data.....0.....@....pdata..|.....0.....@..@.rsrc...x~..... .....@..@.reloc.....p.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	468240
Entropy (8bit):	6.360644638246213
Encrypted:	false
SSDEEP:	6144:RTr4oQz0Snpz93hSq47wRv8TDXgxBQ9hRNmxziUsDRKoZxC:dMoQISnpJQq47wRv8mBQhuxTgZxC
MD5:	DEBD8C08F597085E793324EA3DF51BA2
SHA1:	47170493FF0B022F2BE8B49B16419D378913B5B0
SHA-256:	0BFCD9FCD173D1E084A1A6A3FA4A4D10611153E59641A6CFF589DC314B6CB4F3
SHA-512:	5E3AF790ABADC069189E245B887C35912F34A0E2616AECBCEC2CAF7279DFE2CF42902D2A15D57FC717323D9C3180F902705B2BD089B4E483A8D37F025240357
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.f.g`..g`..g`..n...Q`..,...F`..,...h`..,...`..,...z`..g`...a..,...`..,...f`..,. ..f`..Richg`.....PE..d....~.u.....".....P.....@..... ....._f....`..... .....(.....#.....:.....%.....,.....p.....P... (.....@.....x...@.....text..... ..`.rdata..V{.....@..@.data...pD...P...0...P.....@....pdata...:.....@.....@..@.rsrc. ...#.....0.....@..@.reloc..,.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	439560
Entropy (8bit):	6.244826977512736
Encrypted:	false
SSDEEP:	6144:I1CDcCY8lurGvlmiOFQZCLPTjHJLh9vDK+8KohLlxIf3rkxw:ZDcnOurGvMi3ZCLTjHJ7z8Ko2k+
MD5:	2D2C922CB7EFF1BEA2B37BFCA613918F
SHA1:	3F121AF117529D7696C061283B18F9D912D413CC
SHA-256:	074EB4CB2EB0C305777A255B1F2C0B720E993C3C73C2418413DA23947680D58A
SHA-512:	315E6AE4FA67EA2E97F09A5B325FDFAF1F493E1F5AE79721E84183CD3AA636AA36489CA282ACC160B6EAC986B0716C8D874EDDFAB52F47FAEFDB47B04B02C 2A7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P.W.P.W.P.W.(.W.P.W.(.V.P.W.P.WfQ.W.(.V.P.W.(.V.P.W. (.V*P.W.(.V.P.W.(.V.P.W.({W.P.W.(.V.P.WRich.P.W.....PE..d...$!.....".....`...0.....`A.....p...p..... .....@...3.....%..... ...p.....0...(.....@.....X...8.....text...<R.....`..... ..`.rdata.....p.....p.....@..@.data....;.....0.....@... .pdata...3...@...@...0.....@..@.rsrc.....p.....@..@.reloc.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	49600
Entropy (8bit):	6.271041266014457
Encrypted:	false
SSDEEP:	768:/+iOC5WnAO01IEn2eFl0/PGWNZAUMosM289zLFxD5:44VO+o0WUpFxFzRxD5
MD5:	FCC22A6DD21EA6D5A321A83AD8981F91
SHA1:	775B2536D4851DDB891294F181BF2D009F946E6A
SHA-256:	B5DCF872FAF039C2CF4A00F7922BC96191E4A1AFE6398548442448C4357FB287
SHA-512:	61C3CCB7830EEC8F21E6A51DAE281ED6FE08BAFAAF5694509F31DB1FC72B8951DC3FC8DBE8D603C7B8BE9F9C9E9D75345F129087F64A6AA2CE2A02D57EC05 2BC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.Oz..Oz..Oz..O{..Oz..7{..Oz..7...Oz..7~..Oz..7y..Oz..7r..O z..7...Oz..7x..Oz.Rich.Oz.....PE..d....I.....".....d...4.....Pg....`A.....q..<.....`....`.....`.....%.....D....8.. p.....@0..@.....p..`.....text..... ..... ..h.rdata.....0.....$.....@..H.data.....P.....8.....@....pdata.....`.....<..... ..@..H.idata.....p.....@.....@..HPAGE...../.....0...H..... ..`INIT....~.....x..... ..bGFIDS...$.....@..B.rsrc...`.....@..B.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows

Category:	dropped
Size (bytes):	168200
Entropy (8bit):	6.164229812235971
Encrypted:	false
SSDEEP:	3072:yoEnKPnLzxxrXPoziVMUQwUfPqJOlmHt3EJ/6/:tEAnLLXgzgM3NfPqJOll4i/
MD5:	E8A73F836E3C20352681EECFF0A7146C
SHA1:	BFD81B0F250B78E2B7DB30D5E59059FF8273DD6A
SHA-256:	76B160CA85AF454C4C95884DF52160B0D2D2E8DBF75F11623EEDC6721F1ED6A9
SHA-512:	2E8D5796DF81BC6EA5A42E0DCF24514AFE920354BAF93B937D19C0482FB8241ED2730C559848F8F844C97F054DC8FB1681410929570784E189DF8DB16A1F7E2E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1W.._...._..Z..._...^.W._..^..._..[..._..\..._..W..._.....,_..]..._ .Rich.._.....PE..d.....[....."..... .....0h.....A.....P.....I...%.....p.....p b..@.....text...jM.....P..... ..h.rdata...Y...`...\...T.....@..H.data... .....@....pdata.....@..H.idata..... ..... .....@..HPAGE....B5.....8..... ..`INIT....%)...@...,... ....bGFIDS.....p.....L.....@..B.rsrc.....P.....@..B.reloc.....X.....@..B... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	443664
Entropy (8bit):	6.370764098869939
Encrypted:	false
SSDEEP:	6144:gBGvC+2CpTRJg9rIIRM75PFL6CwsJStkbwRKnyL/EkGFNOBkq0uA0QrKI69iVF/D:gBGR2CpTgiIRHZswWukyL/EkIfj69i4O
MD5:	B8948D2DC799045C0473B61CB75556A3
SHA1:	4B3D486127712D7B3C38E9724DD650C8F8896799
SHA-256:	5788A05FFAACE6D816C2F50797836E20E876F7C05BAF7A546F121763D5618667
SHA-512:	442BC95E5F43290C6EC35D4ACBA8F40A507C748D2CFBE05993D7EE4A3B18EF33C0071F6579535F8246E7E5B846AAADD3A881B7FE2249A8C1D1FA0F84B1EE09 D0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`^...0...0...0...1...0..y1...0..y5...0..y4...0..y3...0..y8...0..y...0.. y2...0.Rich..0.....PE..d....=.u....."....."....h...8.....z.....A.....P.....p...#.....%..... &..p..... ..@.....text..... ..h.rdata.....@..H.data...d....`.....H.....@....pdata...#...p...$...P.....@..H.idata...-.....0...t... .....@..HPAGE....WG.....H..... ..`INIT.....]... ...`..... ..bINIT.....L.....@...GFIDS...@.....T.....@..B.rsrc.....X.....@..B.relo c.../.....0...p.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	90384
Entropy (8bit):	6.182687893566412
Encrypted:	false
SSDEEP:	1536:A5POPUX+xxJXvwp+79ChiuTss2x1g59GfeYJ9c5vXD4PMWZzjj3:A5POP/VfIaChBk2ZYJ9GD4b73
MD5:	3D868C25CE5F5AA4087C279C1326312A
SHA1:	14143AAD35F31E3B73363572D7E2F4F56D50C8BB
SHA-256:	39992D638AF2C889591541B9676E62A2E4CA650143833C04A31B9ADBB83E584C
SHA-512:	098CC84A0EE9DBF13432B2723F7867D3FD669CF9F83FA5C6A6060B6F31DB1CF35CD1C7A02D80EC6BE6ABAA2A24BDE96019C5B37A5D9DC3976FF5FECEA377A A24
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...U...U...U...-...U...U...U...-...U...-...U...-...U...-...U...-J..U...-...U..Ri ch.U.....PE..d....>....."....."....\.....p.....G....`A.....p#..P.....<...%.....L...(...p..... .....@..... ..@..... .....text..... ..h.rdata..`".....$.....@..H.data...(.....@....pdata.....@..H.idata..... ... .@..HPAGE..... ...@...$..... ..`INIT.....p..... ....bGFIDS.....$.....@..B.rsrc.....(.....@..B.reloc.....0.....@ ..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12624
Entropy (8bit):	5.259327730394375
Encrypted:	false

SSDEEP:	192:/5mm9AfGjUa1rIL+FUVin2F/OZDfYj5YbAxqTSSS6S8SzSySovK1ZVuB:/5mm9AfGtML+Fws2Fo7m5YcxHKrVo
MD5:	B6D65A86FC1999A62DA10EA3C4CAD3E4
SHA1:	E79E97C04D8540A2005D21021F7781676E705BCD
SHA-256:	05B2BFD40FB3A344C3AE178C420A7FEA9595815CB1CC07843078112F5F551EAF
SHA-512:	7F13B4930F9BF9ABCFD64E905DA4F0111B34197A533FB0162E43C4C80F39D135ADAA09C3E7AF3E95397BEF5D1D323E75721CEE150517CB13EBED3029C781BEC6
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Drivers" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>... .. ********** ********** .. Driver files.. ********** ********** .. -->...<file destinationPath="$(runtime.drivers)" importPath="$(build.campBinaryImportPath)" name="WdFilter.sys" sourceName="WdFilter.sys" sourcePath=".\"></file>...<file destinationPath="$(runtime.drivers)" importPath="$(build.campBinaryImportPath)" name="WdBoot.sys" sourceName="WdBoot.sys" sou

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6173
Entropy (8bit):	5.373156847974759
Encrypted:	false
SSDEEP:	96:/3coK5HjFWr/96Hj+Uul2lewqo3nRtlUl3lflxSDwMKRbRhK18YaKMr4e:/mDFcujBuEgI3nzC1Z6V8f3
MD5:	5562965C32F03AE0DF8B9DEF950F8651
SHA1:	6E5AD734AB6A9F8B82B19024E21007AC2CAD2540
SHA-256:	EA64BE59286B67AE930729FA92B2B08DCE5C2EAEB70FEABE2320C47FB6DDAC6C
SHA-512:	F64D728AFE40800968D0B165019E775F62F2CCA40BFBB370F52F4BA8FCC2574F79D2C4AC41CCAE6E1CEC23082BA24B5E6C0A5531E6B336683BEEEDDA3CB81CDE
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-NisSrvEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{102aab0a-9d9c-4887-a860-55de33b96595}" message="$(string.Microsoft-Antimalware-NIS.provider.name)" messageFileName="%ProgramFiles%\Windows Defender\NisSrv.exe" name="Microsoft-Antimalware-NIS" resourceFileName="%ProgramFiles%\Windows Defender\NisSrv.exe" symbol="Microsoft_Antimalware_NIS">.....<tasks>.....<task eventGUID="{b33e041e-3a75-4f52-bf0e-c85d0963b7fb}" name="N

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3369
Entropy (8bit):	5.312049604455802
Encrypted:	false
SSDEEP:	96:/3poK58yFND08uf9zXzUzCzwat0kz9nHHzyPYjHMrje:/FbFHuf9DzUOVJ1HHePv2
MD5:	E4AD891E7B62475FCA109C0DF4DEF16E
SHA1:	B7DC3C04C67D7903E04B0EBF2AB7840AAA717EE0
SHA-256:	DF9AD93CDB61587A35FCDCE996955A64413439A474D85C86133A9E9C185D1966
SHA-512:	0849CB6F3DAA6C80B94F770E29BD389B67D31E089595B22BFAF1D6F25C6E847DA4DCBFF135F6D96E30597991FF6C8CA8EB5306C4E8D1B334016220058B2969E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpClientEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{e4b70372-261f-4c54-8fa6-a5a7914d73da}" message="$(string.Microsoft-Antimalware-Protection.provider.name)" messageFileName="%programfiles%\Windows Defender\MpClient.dll" name="Microsoft-Antimalware-Protection" resourceFileName="%programfiles%\Windows Defender\MpClient.dll" symbol="Microsoft_Antimalware_Protection">.....<tasks>.....<task eventGUID="{7db81ddd-d2be-41bd-

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14126

Entropy (8bit):	5.339552069740082
Encrypted:	false
SSDEEP:	192:/ozFIItP1HvYoPp5z7YlAZSJwfnyygPJ2HofEj:/QFlwP1PYoh5WAZSJwfsJ2YC
MD5:	0EA061B68884A0E5AD4B1F4A93B1FBF6
SHA1:	479BEC2F0FD6EC228498F12DC48B798649D5EF25
SHA-256:	1F78E8C7AE754DA422F11439E732628BE78F8BC85625CF4EBFFCF64C536679FF
SHA-512:	8ACEB6F8C3C853C2CCED573F2B047A710731628CD6E8BCFD3C9DAD1763A827ACDF107E0B7927BEDA8F6E359DE1629D0AF79550ACD956AC624FB20242EB8F2FF0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpRtpEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{8e92deef-5e17-413b-b927-59b2f06a3cfc}" message="$(string.Microsoft-Antimalware-RTP.provider.name)" messageFileName="%programfiles%\Windows Defender\MpRtp.dll" name="Microsoft-Antimalware-RTP" resourceFileName="%programfiles%\Windows Defender\MpRtp.dll" symbol="Microsoft_Antimalware_RTP">.....<maps>.....<valueMap name="DlpOperationType">.....<map message="$(string.Ope

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	33315
Entropy (8bit):	5.255657210238715
Encrypted:	false
SSDEEP:	384:/VFriW4cboWcauSi6fZeeEifUhwqh+46AJJCZvsp33icjEtRMdR2CEaXU1Hgb1R5:tFriHcblBLkJ1ycgtOHNXNxBn
MD5:	8EF4C46C00C562586B156D49E8EC6EA1
SHA1:	55C52B40219A564C01274922DB1F67F04D9C8CDC
SHA-256:	CDA3076B92F47438ADAF45388C38C6213D70070908A8F5CCA6D667F8C32E4FF0
SHA-512:	F5061C48D431E86B5E646EDFB9E4B3C69C6DC543DD04B27D6EB0211A360CBB89201FDC0B0203F22092E77FA8234F6FA2B9E0E4F83192F736CE969CAE5DFB18E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpSvcEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:ms="http://manifests.microsoft.com/win/2004/08/windows/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{751ef305-6c6e-4fed-b847-02ef79d26aef}" message="$(string.Microsoft-Antimalware-Service.provider.name)" messageFileName="%programfiles%\Windows Defender\MpSvc.dll" name="Microsoft-Antimalware-Service" resourceFileName="%programfiles%\Windows Defender\MpSvc.dll" symbol="Microsoft_Antimalware_Service">.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	149456
Entropy (8bit):	5.477366012461026
Encrypted:	false
SSDEEP:	1536:5oQofFI+1KSYfSN8bvc0/E/EvJ4rXVEc+ICO+PV5FqGc9HCOKK1HVX:SBfMrIHKK1HVX
MD5:	F02AD94BB9ED8FDABDA9AF79ACF6230A
SHA1:	A461BABC62F003991659368A7F31DBB03E9DA106
SHA-256:	0C5692DBA997F1B4ACA0BD31BCCEA4AAC49B5BC9E5743EC6D11BEC37428BE820
SHA-512:	9FBDD8350F6314E05F76728B32DCF7157A789418606BFBC6C4E009A235920272B11BF675A804F0D8AD4A62A1716895AAC7B0292E142710A149B2F666050BDA93
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Events" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<dependency discoverable="false" optional="false" resourceType="Resources">....<dependentAssembly>.....<assemblyIdentity buildType="release" language="*" name="Windows-Defender-Events.Resources" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384"></assemblyIdentity>....</dependentAssembly>...</dependency>... .. ********** ********** .. BEGIN FILES SECTION .. ********** ********** .. --

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	210184
Entropy (8bit):	5.228872488126836
Encrypted:	false
SSDEEP:	6144:RmiTVVmVVV8VVNVVVcVVVxVVVPVVlVVVRVVVtVVWV60jVLVVOVVUVZVVVVVjVVJB:Th
MD5:	69F046F01F8F661C2D060082911393A7
SHA1:	C26FC18F0F0A06D501BE414EA3C73AA67F117201
SHA-256:	17E1118EC98E9756C54A0C40B3DFAECC6B7140A59F7CE8C5AAB5E2D63DF42B96
SHA-512:	DE6893447D1EF519C38C4E0FBD9CDF2318DBFAFA368537A28273F9252767863863BA84E30B2618271A3A79833EA41FB87E293BFFAE59993DE0404F9152A2F811
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..d.....<.... ....." .....+.....`..... .....%.....T.....rdata..... .....@..@.rsrc..... ....@..@..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1340680
Entropy (8bit):	6.310755864603227
Encrypted:	false
SSDEEP:	24576:rHxbOJ2QxjiDETQvOs+fRlIVT2kQAsj8E/ivRxYJg5s/px5:rHxby2QMDE8gfRlIVZRE/iC
MD5:	B036691DE504AFC094215F1914D4D55A
SHA1:	F8FDF0D9BD1BC01A455DC7CBB6B46B2750116799
SHA-256:	0A81F395025BAC0A0618D98E876477C79712C797F4D1203D62B1C1457049AEB0
SHA-512:	FAE45823DD368E94A23B73DFCE86DC661A31A249FAE9BCDE2C27E10343B75D8298704CAFAD408E4D47C5E5A70CC967D6C991B38DCD28FEE3827E78EA93B88 535
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3.Z.w.4Rw.4Rw.4R<.5Sd.4Rw.5R6.4R<.7Sc.4R<.0S\.4R<.1S ..4R<..Ru.4R<.4Sv.4R<.=S.4R<..Rv.4R<.6Sv.4RRichw.4R.....PE..d....." .....'.....f.....p.....-.....`A.....`..... 0.....p..D....P...%...@...-..l...p.....P/..(.....@.....x/.....text..... ..`.rdata.....@..@.data.....@... .pdata..D....p.....P.....@..@.rsrc.....0.....@..@.reloc...-...@...0... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1238288
Entropy (8bit):	6.284184344287156
Encrypted:	false
SSDEEP:	24576:zPvZGm0QJGxPX4H1vYpaA1dxRvFghtLOrfoeDB:kPDPX4H1vQ71druhWoeI
MD5:	01B7F6ECBE71764DE8754230F8BD0B45
SHA1:	CDA1DDA78A75BA3AC1BD53C2BF2B5FA6FEEC1356
SHA-256:	288071E68AC9EADA23C7ACD312998584CE4E2D91B34C32C56533E51FFA27E106
SHA-512:	5BEAA7CCA576453B4F39BE49D8B4EF2B5C295AC48B68D23271DFD41B1863BB6515FCADB2F310C95CB517A18E46B3C27D62A15B40410C1F909ABBD485A9C82 54
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x.....a....a.....a...a`.....B...a.....a.....a....a..\.....a.....a...R ich.....PE..d....." .....[.....Q ....`A..... ...l.....T.....%.....!.....p.....8...(.....@ .....`.....l.....text..... ..`.rdata...l.....p.....@..@.data... ....@.....@.....@....pdata.....@..@.didat.....p..... .....@....rsrc.....@..@.reloc...!.....0.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	993000
Entropy (8bit):	6.17513414443517
Encrypted:	false
SSDEEP:	12288:uNfgsDU1uXaysw+jAo18lEp2zku5RI6+yrIFuq7ft91ILz:uy9uF9+/1mm2zkKh+yrIFJTt3In

MD5:	60EDC2A1DF1D9EEB37D0729BD76CE568
SHA1:	67D630A477723697CC2815257CCFF432200D09D9
SHA-256:	17A18346D87CD379375D8ED87D4563DCFA97503068465E0D63BFFCB348BE75C0
SHA-512:	C79524A14F50623A84EDE7E5D157F3E82B9130B2B46BCC23FC5CF59C464581DBE934E9F3E13CB510A24F9773194967D3217CC3FF70D6EB9E921B112A78EA953
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..0..0..0..1..0..1..0..60..0..1.0..1..0..0...0..1...0.T.0..0..Z0..0. .1..0Rich..0.....PE..d...l.B\....."....`.....<.....@.....G..... .....(.....8X.....F.....p..... (....x..@.....0.....P... .....text...+T.....`..... ..`.rdata.....p.....p.....@..@.data....R...@...P...@.....@....pdata..8X.....`.....@..@.didat.. .....@....rsrc.....@..@.reloc.....@..B..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365832
Entropy (8bit):	6.189208165298729
Encrypted:	false
SSDEEP:	6144:0lC7FTP+H/2NAxkjl7x8XsF9xZdGG2FwQn8ebu2yV2WTzZQ:1D+H/MhGMxYRn8Nn7Q
MD5:	3C00FF017BBCA95E4A4290CCD1FE7165
SHA1:	CA2BF0E2DC42B7D6DBF57113504B7E3D9FBA3FE0
SHA-256:	CAE6EEB6C836E462D353EC039A7086047ACF75E271C2A748EB45409F9288841B
SHA-512:	BB356AA2980D2198A3F5359810BE0EF426476DE2FD2EC94692793370155EB8BE8C7F546E42E9FD78E15461C5B848A78624042F23EAFF9C83ECB9F0B4A723176A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*..[n..n..n..%...`..%...`..%...g..g.....n..4..%...C..%...o..%...5..%.r. o..%...o..Richn.....PE..d...4^....." .....7.....f.....Qk....`A.....`.....0.....`..... ..<-...p...%...p.. ...\1..p.....0...(.. .....@.....X.....\.....text..... ..`.rdata..h..... .....@..@.data....#..... .....@....pdata..<-... ...0.....@..@.didat..X... .P.....@.....@....rsrc.....`.....P.....@..@.reloc.. ....p.....`.....@..B..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	174864
Entropy (8bit):	5.429784241744532
Encrypted:	false
SSDEEP:	3072:A+hEtFNIswK+MhL9JzFEKTeOmqE6OTuXM2:DuicbhLf66O6
MD5:	8DDC0C6F8FF7E536A99525E42029C78B
SHA1:	A1B7F5411458D684A9468AE9B3D0AD4326027C5C
SHA-256:	1718ADC90B1306FFC2914487AD5B38933A1F7909587BE51FA7F306B3C110D1B8
SHA-512:	1A7CB34071A1ED7204A2F38C754ADF5B1C25E595B594145197FE9C760F013B6A3ACAD9198DF70C4B29AD0A515E8525AE40F6131972022E771E05C0693DBEF38
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....M.....!.....Rich. .....PE..d...d].....".....`.....@..... .....m.....+...p..8....l..p..... &..(.... ..@.. .....H&.....text..... ..`.rdata...`... ...p... .....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc..8....p.....p.....@..B..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	173312
Entropy (8bit):	5.865450816648862
Encrypted:	false
SSDEEP:	1536:IpEqQLqk4J/ja4j3iMfoGx/OCbC14jMYlhsUguEIvadRadzhJqz5BTE+CpAs+Yqm:IeqQLqvJO8gUgutdQzEFasYxYp
MD5:	EB44AEBFF15B908F62F655D8574F0211
SHA1:	C53572499C443D51BEFA9E0FB7EA13C8D9B6CD70
SHA-256:	0E6CB8E7DE57D65EC64364658D71E692EB1DC17C8D1B2AE78172FF86198563A4
SHA-512:	C36D1118A0C00C492D3FC3ACA95BDD2004C2A3224F490869A418869565EE5CC86A7AE04B114DDD68C80DCFA2A33F11B07EC298F745DF5EB1954A14C5FB8C9F4
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... %.edDr6dDr6dDr6/<s7tDr6/<v7hDr6/<q7lDr6m<.6kDr6dDs6 QEr6/<w7NDr6/<r7eDr6/<{7-Dr6/<.6eDr6/<p7eDr6RichdDr6.....PE..d.....)....." ..... '.....d$....`A..... .p.....P..<.....%.....@...p.....(..`...@.....text.."..... ..`.rdata.....@..@.data.....0.....0.....@. ...pdata..<....P.. ...@.....@..@.rsrc.....p.....`.....@..@.reloc.....p.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	103680
Entropy (8bit):	5.572113522034459
Encrypted:	false
SSDEEP:	1536:JcWQg1yzvWG5hCcD9l2NRAUQIW4QuRX8jQbRPVCPvah+zwLK:JRSD9VNZd18jybCHD8u
MD5:	0B2331F6422A23555C47EC81B0B48849
SHA1:	20F0C6B612FCC4A488A41B30515EEACCDD2213C0
SHA-256:	5BFFD333CA93462920F1635640090C62A84D241C16D2F6494126501BBDF60DC4
SHA-512:	C165E6416BA9B1F35FF64632D757DF8B64F1484783914272A949B4309C35C8DEB737545C8A4028134C295E5F1F9604757F77317B1F485BE0E310BBF9929614CD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-..ui..&i..&i..&"..'c..&"..'e..&"..'a..&`.8&f..&i..&y..&"..'@..&"..'h..& "..'V..&".T&h..&"..'h..&Richi..&.....PE..d...mh<....." .....Pa.....`A.....@...H.....`..X....P.....p...%...p..... .....p.....p...(...0...@.....0.....text...2..... ..`.rdata..:Y.....`.....@..@.data.....0.....0.....@....pdata.....P.....@..... .....@..@.rsrc...X....`.....P.....@..@.reloc.....p.....`.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	389728
Entropy (8bit):	5.835662549206683
Encrypted:	false
SSDEEP:	6144:R0a+l0A2oAkdY0+U1RiyL0miTVVmVVV8VVNVVVcVVVxVVVPVVlVVVRVVVtVVWV6J:Rml0YAkdNPiyLe4
MD5:	69150F81B07EF9655BD83401D319795E
SHA1:	DB6290CCBEE4A02D371C6758B16584E2FFF6FD51
SHA-256:	8698065D54C44E78F2D347BE1B43D6843F2D0B1CDE8A85266B25A8DBBE8C0697
SHA-512:	CC870D567C0F1B0FD35C1C5A391FA25140DF30B4BCA5050A0E96AB75C7D636E28ED2E330DEC1317CD5DDB60D8C1E6536F71743C6E832CF1B7B21A5E34B5FD A73
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.'.}.I.}.I.}.I.6.M.s.I.6.J.u.I.t...m.I.6.L.O.I.6.....I.6.H.j.I.}.H.R.I. 6.@.K.I.6...|.I.6.K.|.I.Rich}.I.....PE..d.....".....a.....@.....L..@.....,.....`2.....p..... ..p.....(...`...@.....h.....text..... ..`.rdata.....@..@.data.....p.....p.....@....pdata.,..... ....@..@.rsrc.....@..@.reloc..p.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	144656
Entropy (8bit):	3.907524491292496
Encrypted:	false
SSDEEP:	768:YOmWulQnuBkG22Tumo0cTH6QKqCmuKqrWmNKq4mZKqdmjj4Kqpmpds1P8Xzg9zA2:X6BkG2usqP8Dozw0
MD5:	F7D9399A1C9481060B4FA3BBC80926E9
SHA1:	5EC3F94A482602276014B47E571539DE5B6DDDCD
SHA-256:	DC3D7A692DB783B373309841DC1E82205B75082F4848113C0412D0C9F11B2263
SHA-512:	6084230EA17297EE998DC89389070D36EC4A8D808D5185B5D86D3689BFC061E3A07249E14FE4D4F78FF63ADD2DDD047678D5B633BBA6A0D5B42AA50E82A29E 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..d...=.r..... ....." .....p.....`..... ..X.....%.....T.....rdata..... .....@..@.rsrc...X.... ....@..@..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	505096
Entropy (8bit):	6.0486451497759415
Encrypted:	false
SSDEEP:	6144:+pa2jZwVJ8o7AAROEBMB/C3BltMCCbvpmiTVVmVVV8VVNVVVcVVVxVVVPVVlVVV5:+O8o7AARH0C3BltBCbry
MD5:	A082D51D9D2FCA41BFD28972FD3748C4
SHA1:	1A55326F584A8FA9AA57EF0431DF78B4182EA321
SHA-256:	3C8255F567A8068AB079F25EED2483A04D9442F5DCD1F9B78FE9E478008A8E27
SHA-512:	BEA807354A08866A9268214235F8BEB253B2C55C772EA47B33E3B377391A21BAE215C141FC53BA8CCD846BEB74CAE1944D235EA2506F916B762F6890F218058F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~..&:.u:.u:.uq..t+.u:.u..uq..t!.uq..t5.uq..t..uq..t;.uq..tv.uq.su;.uq..t ;.uRich:.u.....PE..d...E,.a....." ....p....._.....`A.....0.....$1..x.....$$.....%.....X...p.....X.. (...`W..@.....X..p.....text..... ....`.rdata.....0.....0.....@..@.data....0...@... ...@.....@....pdata..$$.....0...`.....@..@.rsrc... .....@..@.reloc.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1795344
Entropy (8bit):	6.415045366249984
Encrypted:	false
SSDEEP:	49152:xSezVA1vvRVENPHBsEZLnLxO3o9WWbIhvOw2fKVMb1ie8:8D3qMOw5
MD5:	659AA4AE9348F71CDE798AC5248DFEA1
SHA1:	D429A68E14B32A9E87CFCA353328657E8AFCD4B3
SHA-256:	1E75629D55321E6F1301D511B2A3F79BEA0F320796ADB75E9C12543FF06AAB47
SHA-512:	6CC57AB909D604AF3EF253A706D3E6F90FFF90051C54714667505F391EB37C0844BC4FFBB1C8735347B96EBDAB776B017DBE62717BC4DA45AE959E6C3F8BE8E 3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.s>.. >.. >.. u..!).. >.. .. u..!*.. u..!... u..!.. u.. <.. u..!?.. u..!.. u.. ?.. u..!?.. Rich>.. .....PE..d....hm....." .....0... .....P.....^.....`.....`A.....P3.....(?.....u.....t....@...%...@..<...,(..p.....(. ...i..@.....(...0...P+..@.....text....-.....0..... ..`.rdata...$...@...0...@.....@..@.data....y...p...`...p.....@....pdata..t.....@..@.didat.... .....@....rsrc....u.....@..@.reloc..<....@... ... .@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	902408
Entropy (8bit):	6.3239119668596295
Encrypted:	false
SSDEEP:	12288:jMQUBF4lyh7oKj+dnEll2Utg9Lke3doMOoYxdLGrkKH:jMhFMyZbjkdl2UILBdoMO/GrkS
MD5:	D3B49C3DAF078EA17A9105FEEB614444
SHA1:	ED7F08ABBC6C94E83CE4AAF58FF4DCDF9AD287EE
SHA-256:	393514A9E16C47B568A0FD4032F8ABC852D9F418FE0FAD98643DE5044DEAD671
SHA-512:	4CF3C8288EC1CE21DA82D3C4A0362B3669091FA42F7907C6630B450F67BF8C5E7243189C74E817253115DD2DED5ABDCFB099064362C0335DC4455C1016E5B24
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...D..D..D.<...D..D..aD.<...D.<...D.<..D.<...D.<..D.<...D.<...D. <...D.Rich.D.....PE..d....jEc....." .....0...p.....0.....6.....`A.....|...l...x.....de.....%.....P...p.....(.. ....@.....8.....text.../,.....0..... ..`.rdata..J....@.....@.....@..@.data...@....0.....0.....@....pdata..de.....p.....@..@.rsrc..... .....p.....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped

Size (bytes):	803176
Entropy (8bit):	6.37118649960636
Encrypted:	false
SSDEEP:	24576:Ghj1QlBYDgtUUvie3n+pB3+ojRlcD1VyZTFXk:GhpQlBHtBYla1VyZpU
MD5:	01F92DC7A766FF783AE7AF40FD0334FB
SHA1:	45D7B8E98E22F939ED0083FE31204CAA9A72FA76
SHA-256:	FA42B9B84754E2E8368E8929FA045BE86DBD72678176EE75814D2A16D23E5C26
SHA-512:	BEA5F3D7FB0984C4A71720F25644CE3151FCDC95586E1E2FFE804D04567AAF30D8678608110E241C7DDF908F94882EDDD84A994573B0C808D1C064F0E135A58
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..#...#..#..EV...#...Q...#...Q...#...Q...#...Q...#...#..."..EV..#..EV N..#..EV...#..Rich.#.....PE..d.....P....."..... `.....@.....0.....-.... `..... .....t..d..... .....D... ..h!... .....d...p..... (.....8.....0.....text...2R..... `..... ..`.rdata.....p... ...p.....@..@.data..../..... .....@....pdata...D.....P.....@..@.rsrc... ....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3577104
Entropy (8bit):	6.391478500460786
Encrypted:	false
SSDEEP:	49152:ZQ/Ezd1FbOjfjhAEFDENsP+HxHLFbZTLlw+kR8P/ykQ4VQtU2386D1MBBWVG/wyy:Gud1Fb09AEFeZhc/02qEcA
MD5:	856E885E779B7A69EF4FF406F4FA9FEF
SHA1:	B533C1C7D913558DD7E14DD8ADE4B97CE6300DD6
SHA-256:	235CD0DA7033946EBC19E40297381BF7772A289D5AC86EB1996DB4C60473924A
SHA-512:	2465A56CCBF2F99055003C6CED51DF209C037B61967430CF32B0BCF00CB8826C508EAF076404052CCED208022E0089DB0541DF3DA748B7336C5F5C43B1074C0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..R..R.....D.....A.....X..[.,E..R..3.....c....B.P.....S.....*..u...U... .@.S.....S..RichR.....PE..d.....W....." .....(.....0.....\.....6.....6...`A....."3.d...4#3.....5.....p4..W...p6..%...p6..6.....p..... .....X.).(.....(.@.....)....`.3.....text....(.....(..... ..`.rdata.....(.....(.....@..@.data.....`3.....`3.....@....pdata...W...p4..`...04..... ....@..@.didat.....5.....5.....@....rsrc.....5.....5.....@..@.reloc...6...p6..@...06.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	156936
Entropy (8bit):	5.705583024147514
Encrypted:	false
SSDEEP:	3072:Cxrr+YZgLDlihKEQL+iQEKTe2OVHfbf/6l:CFr+YZqheK7Fzil
MD5:	29AEC41325BFAE570C85459152EBE298
SHA1:	7AD4429A20E26B757DC678D460E2F92F59B17C4D
SHA-256:	C4C99F248A2E7E8F96F9D55BCBBB12A59F65227F7065A49C9353A7FA48AEC90E
SHA-512:	56C4E5C5B22653661C5B531F877492D6344D63F8E9488CD484A7B14E35A1140F84DDBF88076626A7262DBB2E35D8240F69B69E833B07A651CF11BBA37F03C0D4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G2.H&\OH&\OH&\O.^]N[&\O.^XNE&\O.^_N@&\OA^.OF&\OH&]O .'\O.^YNb&\O.^\NI&\O.^UN.&\O.^.OI&\O.^^NI&\ORichH&\O.....PE..d....b....." ....0.....h.....P.....l....`A.....L..... ..0.....@...%...@..$...0...p.....e..(....d..@.....f.....text...2(.....0..... ..`.rdata.....@.....@.....@..@.data... .....@ ....pdata..... .....@..@.rsrc.....0..... .....@..@.reloc..$....@.....0.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	558344
Entropy (8bit):	6.077626746902674
Encrypted:	false
SSDEEP:	6144:CEunvv7sgmK8zaNcgAH2IGCXbzAoO+7MrHiTVVmVVV8VVNVVVcVVVxVVVPVVlVVC:funvv7sgf87gAH2IGCXbzAV+bz
MD5:	49A1F2027EA47DD7F52651BA3ACD59AA

SHA1:	916ED3E71AD9336F6C36243EF8B661CDBAAAB53A
SHA-256:	0A6A7A2A3E44D17AF7D9B83D503ADED7B528678F2A47433E13542B6F1BA2B4CA
SHA-512:	74A4ED5F1D8702C9CD9E288DA224B66F40445BF2F76F2BF1BD7D7B4E38F53A723065887820A4BD7ACADE5815830E3BAAB9E5ACD5567EBED25657FED5C5875D69
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K.....W...W...WD..V...WD..V...WD..V...W...W ..W...W...WD..V#. .WD.}W...WD..V...WD..Vo..WD..W...WD..V...WRich...W.....PE..d.....h....." .....V.....`.....A.....P.....`..\....0 ...%...`...%...P.....P..p.....`...(... ...@.....text...L..... ..`.rdata..... .....@..@.data....-.....0.....@....pdata.. .%...0...0...0.....@..@.rsrc...\....`.....`.....@..@.reloc.....P.....P.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	133544
Entropy (8bit):	5.848615249699151
Encrypted:	false
SSDEEP:	3072:UpmbTWzjcZlEUNAy53Rn6KTekJVT+ARjRf6lR:UpQWzjpUNX53Rnl+wFlR
MD5:	12F0FE026D6A305044A713DA22C6AE37
SHA1:	9B11F405174FA764FC9D0DFD3D53EBF91364FDE5
SHA-256:	AE2C900FB2A2B1182E6C4BFAF2D0D6A969EFACD94D78DB71677902A945E251AE
SHA-512:	5295B162EE53FCA6355E7851C907D4AECB6A8FE2CFA87BAFE9C5EA283D0942BBB485579224D04260949D6FE1E2B6DB5FE17C95A63B93F851317CD0821EEA8392
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.....N...N...N]..O...N]..O...N..ZN...N]..O&..N]..O...N...N ..N]..OR..N] .6N...N]..O...NRich...N.....PE..d...Z.{....."..... .....@.....{.....).....d....L..p..... 4..(....2..@.....H4.....text...R..... ....`.rdata...Z...0...`...0.....@..@.data.....@....pdata..... .....@..@.rsrc... .....@..@.reloc..d.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	21768
Entropy (8bit):	4.73355600681099
Encrypted:	false
SSDEEP:	192:0Wg3HWMALc2Fu462TNgRpSDBQABJ0OpF+nasu+JX01k9z3AzsNvCEVE:0Wg3HWM1MJjDBRJlpUad+JR9zusN7VE
MD5:	56C96953AC9158CBD42E69ED7F97A7F8
SHA1:	4DEED0464F3A0CA22D8CDD5BE0B050EAE1B8A124
SHA-256:	4CDB750A61129171ED6BDBFEEF0531267C5F3255F0EF64F211BEFAB40C27AF48
SHA-512:	23CDAFBEFD19136170B409DB9B2AECAFDE594F145B825F8D57F4CDD2BE2DAA308E0673EE6A75E7204E4E4BC417650C5F44F74DD4CD533B0A9ECCEDF6810AE462
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..d. ...F.Z....." ....0.....`..... .....0...%.....T.....r data.....@..@.rsrc..... ....@..@..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3116848
Entropy (8bit):	6.512761509155942
Encrypted:	false
SSDEEP:	49152:YrHb7Kijoa19g6ss1A+XeXrSTz8E06VPzTBP/QO6B70HavlazVuAr:YrXJM07V1
MD5:	F38768BA269467EA171A5AB304408D6A
SHA1:	0F5BB7DCCFF14D76A67BE1AEAF81CD7C658FEFBE
SHA-256:	87F545258C7DC408006A9EB392D91B74FED35CB21437CD0F3D653E8277AF60BB
SHA-512:	E4DCB0A5FCB63308EC11E988A3CFF068D27D498135609CB9C7639036639802A1CE2F1707C6414F16D1B9A21F6F0F5D6BE2C9BD1557E9378AD59898C3A2D2AB20

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.....\.....2.....A.....0.. .....Rich.....PE..d.....b.....".....'.....D%.....@.....0.....H50...`.....U,.,...../.H....@...f..../.0...../.03....(.p..... ...P.'.(....'.@.....x.'.P...0K,.....text.....'.....'..... ..`.rdata..tX... '..`... '.....@..@.data...0.....,.....,.....@....pdata...f...@...p...0-.....@..@. didat...../.....@....rsrc...H...../.....@..@.reloc..03..../..@.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	15169
Entropy (8bit):	5.98493580150489
Encrypted:	false
SSDEEP:	384:gBYYHOIwJu4mSFCzWFBjObOFN5YxMsrRhmKa7iKV23i/rIwg:XYHOIwJu4mwhcYzbsrRhmzey2KrA
MD5:	2249B509298F1B6048E05506974F1874
SHA1:	D34EB00A3D91C254CEEBD88BA86F9F9AAFD10F43
SHA-256:	49047C3E3F7F96E0D04C6ECCD7E58592B3E53E96944A8DF103FA31361D654F5D
SHA-512:	7374983DDA6FD3E01E998AD660FF5E6EBC4C5F7EAE1D2F3CCB1846FEEA3433A6292F678ADE8D50187E1CEF96C777A633832F38A34C32C3BC9D7AC26B0E620 C6
Malicious:	false
Preview:	@{.. GUID = 'C46BE3DC-30A9-452F-A5FD-4BF9CA87A854'.. Author="Microsoft Corporation".. CompanyName="Microsoft Corporation".. Copyright="Copyright (C) Microsoft Corporation. All rights reserved."... ModuleVersion = '1.0'.. NestedModules = @('MSFT_MpComputerStatus.cdxml',.. 'MSFT_Mp Preference.cdxml',.. 'MSFT_MpThreat.cdxml',.. 'MSFT_MpThreatCatalog.cdxml',.. 'MSFT_MpThreatDetection.cdxml',.. 'MSFT_MpScan.cdxml',.. 'MSFT_MpSignature.cdxml',.. 'MSFT_MpWDOScan.cdxml',.. 'MSFT_MpRollback.cdxml'..)... FunctionsToExport = @('Get-MpPreference',.. 'Set-MpPreference',.. 'Add-MpPreference',.. 'Remove-MpPreference',.. 'Get-MpComputerStatus',.. 'Get-MpThr

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14315
Entropy (8bit):	5.9999306217827
Encrypted:	false
SSDEEP:	384:ZYHOIwJu4mSFCRDo58rxhWwQUgIpIN6bSE1wZFPe:ZYHOIwJu4mwYi8r7WwlE6P1wZw
MD5:	CE2037B591E8EE0D5D89F80D416B5A3B
SHA1:	08E0E91567FB8C8BEECF3555DA934C6739922072
SHA-256:	A0F884FAAC5D057B3E005429FBC7BF4FA4239419847939F802CD6A588D622B43
SHA-512:	C7CB60A44751BF40FB23E8856207B2D045D7F912F5F760C9D07A2022FEDE5ACAE857BA7C9D65A2018FA3E3860687CEA9442FCC4A30783F7AFB35BABEC2AC91 B4
Malicious:	false
Preview:	@{.. GUID = 'A51E6D9E-BC14-41A7-98A8-888195641250'.. Author="Microsoft Corporation".. CompanyName="Microsoft Corporation".. Copyright="Copyright (C) Microsoft Corporation. All rights reserved."... ModuleVersion = '1.0'.. NestedModules = @('MSFT_MpPerformanceRecording.psm1')..... FormatsToProcess = @('MSFT_MpPerformanceReport.Format.ps1xml')..... CompatiblePSEditions = @('Desktop', 'Core')..... FunctionsToExport = @('New-MpPerformanceRecording',.. 'Get-MpPerformanceReport'..).. HelpInfoUri="http://go.microsoft.com/fwlink/?linkid=390762".. PowerShellVersion = '5.1'..}....# SIG # Begin signature block..# MIIeQYJKoZIhvcNAQcCoIIajCCJWYCAQExDzANBglghkgBZQMEAgEFADB5Bgor..# BgEEAYI3AgEEoGswaTA0BgorBgEEAYI3AgEeMCYC AwEAAAQQH8w7YFlLCE63JNLG..# KX7zUQIBAAIBAAIBAAIBAADAxMA0GCWCGSAFlAwQCAQUABCC5QoGq9EV41ZN5..# fnwNlxKx8aIBP8W7y/AxkQ4S rJmPcKCCC14wggTrMIID06ADAgECAhMzAAAI/yN0..# 5bNiDD7eAAAAAAj/MA0GCSqGSIb3DQEBCwUA

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15565
Entropy (8bit):	6.002588540208934
Encrypted:	false
SSDEEP:	384:on0LK0WHQV80tQEFvcjhYa85wyGvy0bW5Wb0CnV/KI:E0LK0WHY80tQvj6a8GyGvQWdnlp
MD5:	76B112FAE2CD94774D83033FC5C81B5D
SHA1:	855EA7E2F4F88F49AB61505782275E14DBA33A32
SHA-256:	C5ED226D73FCF42F1895256BB80B67734607D07A113B6214E8B36CD780AA0D91

SHA-512:	2441218BD2D91242BC733BD2E05C92E7FBDD2CFDF1D0148BC9ABC2D82E99CF4210D3B4A924E110331D55F30EBD9E3848E1256665A0DA72CF41965E31D670DE A
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="R OOT\Microsoft\Windows\Defender\MSFT_MpComputerStatus">.. <Version>1.0</Version>.. <DefaultNoun>MpComputerStatus</DefaultNoun>.... <InstanceCm dlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. .. </GetCmdletParameters>.. </InstanceCmdlets> .. </Class>.. ..</Powe rShellMetadata>..... SIG # Begin signature block -->.. MIIleQYJKoZIhvcNAQcCoIIlajCCJWYCAQExDzANBglghkgBZQMEAgEFADB5Bgor -->.. BgEEAYI3AgEEoGs waTA0BgorBgEEAYI3AgEeMCYCAwEAAAQQH8w7YFlLCE63JNLG -->.. KX7zUQIBAAIBAAIBAAIBAADAxMA0GCWCGSAFlAwQCAQUABCCCGKubREngV5EF -- >.. DodK5brTAqlkaVHav/M+SkqGWqFKKqCCC14wggTrMIID06ADAgECAhMzAAAl/yN0 -->.. 5bNiDD7eAAAAAAj/MA0GCSqGSlb3DQEBCwUAMHkxCzAJBg NVBAYTAlVTMRMwEQYD -->.. VQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdSZWRtb25kMR4wHAYDVQQKExVNaWNy -->.. b3NvZnQgQ29y

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	47935
Entropy (8bit):	5.579128775704969
Encrypted:	false
SSDEEP:	768:yF4WapeFhb1KVSMK3xFivFo1BWMmr8OGPDKQxV/U9LqoquhYHOIwJu4mwxZcYzbq:yIYrR4vFo1BWMmr8OGPDKQxV/U9Lq3/T
MD5:	2EA89BBC0492742F1485532EFAFE1C4A
SHA1:	F6954BD3FE4D06F02D54681AC049F9A15167B91A
SHA-256:	A36D3C22CB21DA1564F9946C98A52D99C64D062E8FC346B3B4205FFBBC2003C3
SHA-512:	6FEC5E7FF16DA9F06788FACE19ECFF09719E687744D126145789B27F2FFDA4BBBD463139182E86DD5ED07C5F208752C5B4E95BB08EBAA0BF982F0E595E3385A 3
Malicious:	false
Preview:	## Copyright (c) Microsoft Corporation. All rights reserved.....<#...SYNOPSIS..This cmdlet collects a performance recording of Microsoft Defender Antivirus..scans.....DE SCRIPTION..This cmdlet collects a performance recording of Microsoft Defender Antivirus..scans. These performance recordings contain Microsoft-Antimalware-Engin e..and NT kernel process events and can be analyzed after collection using the..Get-MpPerformanceReport cmdlet.....This cmdlet requires elevated administrator p rivileges.....The performance analyzer provides insight into problematic files that could..cause performance degradation of Microsoft Defender Antivirus. This tool is..pr ovided "AS IS", and is not intended to provide suggestions on exclusions...Exclusions can reduce the level of protection on your endpoints. Exclusions,..if any, should be defined with caution.....EXAMPLE..New-MpPerformanceRecording -RecordTo:.\Defender-scans.etl....#>..function New-MpPerformanceRecording {.. [CmdletBinding(D efaultPara

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text
Category:	modified
Size (bytes):	4971
Entropy (8bit):	4.542570045638256
Encrypted:	false
SSDEEP:	96:aAPEP3EPGEPJuDhDEMTRBTCq6IQEPvAwWSJNLKI+EPZMhkvyXHkJi2eEPZMUkvy/:aAcPUPpPJfMTRBTr6ILPvAwW6NRPZMh2
MD5:	990729AD92C1325C42B04BC975ECBD57
SHA1:	1CDBE901753CCE8D933DF8D50507CE16A25AA428
SHA-256:	E796454FEE4CF17EFDC25DB5FEEF00A5D7C1B335E6C4B4FE996E8AD7CAB01BC8
SHA-512:	EA0BCD6122068DA9412E5195C7AA3017C187790C790197AC5AF129F3ACF6C23780169C0165627E5C55CB3B99E6931CB18A42E61701C647FF07EAF6DA2740DAE B
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8" standalone='yes'?>..<WindowsPerformanceRecorder Version="1.0" Author="Microsoft Defender for Endpoint" Team="Microsoft Def ender for Endpoint" Comments="Microsoft Defender for Endpoint Scan performance tracing" Company="Microsoft Corporation" Copyright="Microsoft Corporation">. < Profiles>. System Providers -->.. <SystemProvider Id="SystemProvider_Scans_Light">. <Keywords>. <Keyword Value="CpuConfig" />. <Keyword Value="ProcessThread" />. <Keyword Value="ProcessCounter" />. </Keywords>. </SystemProvider>.. <SystemProvider Id="S ystemProvider_Scans_Verbose" Base="SystemProvider_Scans_Light">. <Keywords Operation="Add">. <Keyword Value="Loader" />. <Keyword Value="SampledProfile"/>. </Keywords>. <Stacks>. <Stack Value="SampledProfile"/>. </Stacks>. </Syste

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	63612
Entropy (8bit):	4.598281135137091
Encrypted:	false

SSDEEP:	768:Bw2CW0LK0WHY80tQreAqVhYMbh96Jg+GjWuW:Bw2CTVtHBdHbKuW
MD5:	8A46F440466ABA5A5D9AF56526799DE7
SHA1:	77637AE7FF8C39FD77F6B4CDCFE222A13A223CB7
SHA-256:	03E06EDFB3FE9FC11064BFB8AA8493FD354C55A6C696C9A1B50D5B14C440186C
SHA-512:	951601F925E8722E81D059AB94840CA128028003F588D17C6ACF2E992F8F12319374635AEDEF2D24D4670D5A64EE8DC96124C6A90102F69DAA520491096D8245
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<Configuration>.. <ViewDefinitions>.. <View>.. <Name>default</Name>.. <ViewSelectedBy>.. <TypeName> MpPerformanceReport.Result</TypeName>.. <TypeName>Deserialized.MpPerformanceReport.Result</TypeName>.. </ViewSelectedBy>.. <CustomCon trol>.. <CustomEntries>.. <CustomEntry>.. <CustomItem>.. <ExpressionBinding>.. <PropertyName>TopFiles</PropertyName>.. <ItemSelectionCondition>.. <ScriptBlock>($_ | gm -Name:'TopFiles' -MemberType:NoteProperty).Count -gt 0</ScriptBlock>.. </ItemSel ectionCondition>.. <CustomControl>.. <CustomEntries>.. <CustomEntry>.. <CustomItem>.. <NewLine />.. <Text>TopFiles</Text>.. <NewLine />.. <Text>========</Text>..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	116938
Entropy (8bit):	4.093756521027276
Encrypted:	false
SSDEEP:	768:5oISOD2TIWNoVejxo98O0LK0WHY80tQ9C2ByGCWdnx3LI:5lSODnWNgejx3rVt+q
MD5:	5E86E45C883373AECFBB0CF4A6D87E08
SHA1:	35A2D861F857E3D99F943176250E38CF48A5118C
SHA-256:	86F1A6AFE5DEE08BBAAEB55982829469C8728CD853428BC271ACA45F5318D05D
SHA-512:	F26BBA1BEBEE66AE63AE80FC968CF55F670999454A9177AF21D752CC8217CCFB045A5D8F44E9E8E6AC4759042A255E6C975E469B0DCAFB5BA9D8048BCC0EA 3B2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="root\Micro soft\Windows\Defender\MSFT_MpPreference" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpPreference</DefaultNoun>.. <Instance Cmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. </GetCmdletParameters>.. </InstanceCmdlets>.... <StaticCmdle ts>.. <Cmdlet>.. <CmdletMetadata Verb="Set" />.. <Method MethodName="Set">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ ReturnValue>.. <Parameters>.. <Parameter ParameterName="ExclusionPath">..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	16417
Entropy (8bit):	5.997052095509695
Encrypted:	false
SSDEEP:	384:iSD3Dnk0LK0WHQV80tQEF5IvDKLEZVhYMbo296oaXwGrGObqW27iN:iJ0LK0WHY80tQHAqVhYMbh96Jg+GjWWK
MD5:	89D599DDCA244DE89577AADBC19BCD02
SHA1:	8B4C04631C1CC6B78B81626E6826581E69F913C7
SHA-256:	EC39C0F8BC4D860728D8DB3602652CB58FADC508BCBAE34A7B8DEDC71A636CFD
SHA-512:	A18FA0D5A92330F26A8AEDA32CFF8F1B0231E37321AFD798479252ECF524235F3AE2B1F1F6340E1F976C7A5A82CCEEBB845C45F2EC7D65A9C1350AE5F2D821(1
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="R OOT\Microsoft\Windows\Defender\MSFT_MpRollback" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpRollback</DefaultNoun>.. <Stati cCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Start" />.. <Method MethodName="Start">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter P arameterName="Engine">.. <Type PSType="switch" />.. <CmdletParameterMetadata>.. <ValidateNotNull />.. <ValidateNot NullOrEmpty />.. </CmdletParameterMetadata>.. </Parameter>.. <Parameter ParameterName="Platform">.. <Type PSType="switch" />..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	16893
Entropy (8bit):	5.990176210459719
Encrypted:	false
SSDEEP:	384:7DORD5N430LK0WHQV80tQEFvyhKHNDyGS9aW5Wb0CnirVjI:t0LK0WHY80tQ/oZyGS9VWdnek

MD5:	B8B11F642C8D368A72E7EB2DAD68E3A5
SHA1:	8E3614F75FBD03A4CA656191E5070DB996977B78
SHA-256:	1FA0F28191F99613F3D5F39D6E27D851E5C7DF2CE7F3EF9CF55FCB3A8E0B639C
SHA-512:	8439C36CE7B377462B35541D40BB07EF3074D8840753188C968ECE3689AD198BBF52C9524FF1E1B6FF51A5AC54B4610C291E784008B50CAC40352129B3DE1E4F
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpScan" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpScan</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Start" />.. <Method MethodName="Start">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter ParameterName="ScanPath">.. <Type PSType="System.String" />.. <CmdletParameterMetadata>.. <ValidateNotNull />.. <ValidateNotNullOrEmpty />.. </CmdletParameterMetadata>.. </Parameter>.. <Parameter ParameterName="ScanType">.. <Type PSType="MpScan.ScanType

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	16877
Entropy (8bit):	5.991826912444448
Encrypted:	false
SSDEEP:	384:E6D5YR4/0LK0WHQV80tQEFvGhIsR3glyGzBW5Wb0CnMG8:z0LK0WHY80tQzC2ByGCWdnMp
MD5:	840180372C1BFDD5E480D695F00BEA05
SHA1:	98CDD72DEFC87CAC4753ABF4B9979144549639EE
SHA-256:	F67DDC77905A206434220AB1E59FF1CE6C452BCB391755710764FA05E75D7F98
SHA-512:	909BA31ECD1B977C17D9DC6B5C05811D2683DC70752AF7945498DC76D476E9CB79846E2E50354F12EBFCCBA4E6977F3BBEC49DE3EB37E7975E4C0A3A0CC5BBB3
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpSignature" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpSignature</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Update" />.. <Method MethodName="Update">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter ParameterName="UpdateSource">.. <Type PSType="MpSignature.UpdateSource" />.. <CmdletParameterMetadata>.. <AllowEmptyString />.. <AllowNull />.. <ValidateNotNull />.. <ValidateNotNullOrEmpty />.. <ValidateSet>.. <AllowedValue>In

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	16503
Entropy (8bit):	5.9787160175042695
Encrypted:	false
SSDEEP:	384:Tu0LK0WHQV80tQEFvKwHxByGQ4cOhW5Wb0CnSLsZO:S0LK0WHY80tQ7wHvyGv2WdnWmO
MD5:	11A592F312945D1CDE2D0AC481E9BB6D
SHA1:	10D5CDF465A528D85470C079E58E300BC85B2CF4
SHA-256:	AF755B9A91AF1494C24753F835D96F7DCB7536FA3AF85A856AED93C7C1DD9D8C
SHA-512:	4CA8DCC309325C97A2A498B461E13873AD8C03C4EFD077897740E5103F9E0D40DA5DB3091103FF560BCEC8F0523DD065C520AC01216AA57CACD68CDA475115
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreat" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreat</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Remov

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	16048
Entropy (8bit):	6.0030092065415355

Encrypted:	false
SSDEEP:	384:L0LK0WHQV80tQEF5oMfN3PMLEZlneZMMbo296oaXwGrK6EidnkPnIC:L0LK0WHY80tQeiqNTMbh96Jg+KYn+nIC
MD5:	21960A4C9E8354BA0C5FD0B008A66080
SHA1:	6E4F8F25DF48026AA1B69E8F4B1AE87C209FF5EC
SHA-256:	99595A3BCBD4C771FAADA224BC0C84CE4EFA3B85884717C731D7C693D3D50615
SHA-512:	9A877F2AB94A08777148B3B191CFBC7BEFB324AF335110A34FB4C2AA910940B5971D8E527BDD0985756016BA3D0B51F8B54DAFA7C6996F32C59421E2009E3BE6
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatCatalog" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreatCatalog</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. </Class>..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIljwYJKoZIhvcNAQcCol

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15997
Entropy (8bit):	6.0030035275776985
Encrypted:	false
SSDEEP:	384:C0LK0WHQV80tQEFvMhKHNDyGS9aW5Wb0Cni0KVJ:C0LK0WHY80tQRoZyGS9VWdnSJ
MD5:	D4EBF96E5BB8B896BDD7460EB2059552
SHA1:	1FFE3E1B208AF3418AA7910808BC6E52F6AFA9B2
SHA-256:	AE315C6AE4E5F3B4C80DCB88BAE6C5FF515AEA476B115A037DC2DC6002BE8CDA
SHA-512:	5E7A65F47A4DC1211644C367E29B6162DF34E6BD9B9713230FD0E19368352523F3703C55907957112C7C787E97C0A7AE6662902CB1B3103967E1318B850AC43F
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatDetection" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreatDetection</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. </Class>..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIleQYJKoZIhvcNAQcCoIIlajCCJW

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15776
Entropy (8bit):	6.001974939961335
Encrypted:	false
SSDEEP:	384:L30LK0WHQV80tQEFvdwHxByGQ4cOhW5Wb0CnSZn5:b0LK0WHY80tQcwHvyGv2Wdn05
MD5:	630DD6CE09085E75DF744F9424867818
SHA1:	C5DB7ED9F6C4EBAA17AF6B351D8D24CDB60371F7
SHA-256:	D4EFEDC563EC7068A215D762593B2CD4BF44E3B7559D71B06312889AF8B134B8
SHA-512:	4D4903A65481CF26E2FE39E66C970148C87861C71453CD139DBDC4A8A3ACA77F7B15E4B8B352CCB128F6CFAD64686A7987A5E45B3B91778B8552A1003D8FE188
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpWDOScan" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpWDOScan</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Start" />.. <Method MethodName="Start">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue> .. </Method>.. </Cmdlet>.. </StaticCmdlets>.. </Class> ..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIleQYJKoZIhvcNAQcCoIIlajCCJWYCAQExDzANBglghkgBZQMEAgEFADB5Bgor -->.. BgEEAYI3AgEEoGswaTA0BgorBgEEAYI3AgEeMCYCAwEAAAQQH8w7YFlLCE63JNLG -->.. KX7zUQIBAAIBAAIBAAIBADAxMA0GCWCGSAFlAwQCAQUABCBzAXdbBfjvkCEN -->.. qK7Ym3r0lwef2vQhN9zidTDdkf

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	775440

Entropy (8bit):	6.117728139036199
Encrypted:	false
SSDEEP:	12288:f73TaRE88QcXW/G1bQXB0UtvcxITEJS22K6iOOODa/uv+7:z3Wt8QcG/G1bohExIAk2f61TG7
MD5:	818FAE33592CC434E3A1271C89F8C58C
SHA1:	83755ABF3F6BC52131FA4E1CE7878138BA2153B5
SHA-256:	5D862F56EDA8E7EFC5591EE0318498320C57CDF8EAE3570ED3A7C233DABE5EFD
SHA-512:	6D33EDA0CFA8946A4C33B8DF6B2C836F72C840D6FC87487B9DDD4071E9011416B213BC6F83F80E9727CFBA6C0A204C75798AFE9C61B5EAD366E74E4F225DD5CF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'..c...c...c...(..p...c.....(..y...(..l...(.....(..b...(....(.l.b...(..b...Richc.....PE..d...7y.0....." .....N....`A.....7.....8.....`..X.....S.....%...p...l...<..p.....pR..(... ...@.....R.....t0.....text...l..... ..`.rdata...d.....p.....@..@.data.....`.....`.....@....pdata...S.....`.....@..@.didat.....P.....@.....@....rsrc...X....`.....P.....@..@.reloc...l...p...P...`.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	C source, Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	97942
Entropy (8bit):	3.5943941559672163
Encrypted:	false
SSDEEP:	768:ovQJc7QiBhFbJAbYzwyZLvQJc7QiBhFbJAbYzwyZg:/QutyqQutya
MD5:	08358ABE407C2A272148068E693744F0
SHA1:	BE7023281F1B8A5497D992FA07CE6E01C1FFC508
SHA-256:	204DA3BF376AEF0B62441ABEC6E189D7DFC70C28D77102FFD41703F4DCFA646F
SHA-512:	2FF5FECB36D361760495CF5C9C78B4E934B924DA60EC08A6A92331A43016E6616B2FEFF1BF7DAD91522FDD91C6DF1052744E35C7F99C6E173DF1D68C41C065B
Malicious:	false
Preview:	..#.p.r.a.g.m.a. .a.u.t.o.r.e.c.o.v.e.r.....#.p.r.a.g.m.a. .n.a.m.e.s.p.a.c.e.(.".\.\.\.\...\.\.r.o.o.t.\.\.M.i.c.r.o.s.o.f.t.\.\.W.i.n.d.o.w.s.\.\.D.e.f.e.n.d.e.r.".).....I.n.s.t.a.n.c.e. .o.f. . _._.W.i.n.3.2.P.r.o.v.i.d.e.r. .a.s. .$.p.r.o.v.....{..... . .N.a.m.e. .=. .".P.r.o.t.e.c.t.i.o.n.M.a.n.a.g.e.m.e.n.t.".;..... . .C.l.s.I.d. .=. .".{.A.7.C.4.5.2.E.F.-.8.E.9.F.-.4.2.E.B.-.9.F.2.B.-.2.4.5.6.1.3.C.A.0.D.C.9.}.".;..... . .I.m.p.e.r.s.o.n.a.t.i.o.n.L.e.v.e.l. .=. .1.;..... . .H.o.s.t.i.n.g.M.o.d.e.l. .=. .".L.o.c.a.l.S.e.r.v.i.c.e.H.o.s.t.".;..... . .v.e.r.s.i.o.n. .=. .1.0.7.3.7.4.1.8.2.5.;.....}.;.....I.n.s.t.a.n.c.e. .o.f. ._._.M.e.t.h.o.d.P.r.o.v.i.d.e.r.R.e.g.i.s.t.r.a.t.i.o.n.....{..... . .P.r.o.v.i.d.e.r. .=. .$.p.r.o.v.;.....}.;.....I.n.s.t.a.n.c.e. .o.f. ._._.E.v.e.n.t.P.r.o.v.i.d.e.r.R.e.g.i.s.t.r.a.t.i.o.n.....{..... . .P.r.o.v.i.d.e.r. .=. .$.p.r.o.v.;..... . .e.v.e.n.t.Q.u.e.r.y.L.i.s.t. .=. .{.".s.e.l.e.c.t. .*. .f.r.o.m. .M.S.F.T._.M.p.E.v.e.n.t.".};...

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	C source, Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	2664
Entropy (8bit):	3.464075447819169
Encrypted:	false
SSDEEP:	24:QXbclfUWvlDQzj3WvlDQzCWvlDQzwNWvlDQzYTYWvlDQzSJjWvlDQzfWvlDQzyWU:eTjDGwJ3SJnr24RFZ7a2la2Sa2mWaWP
MD5:	C4E26C53F76774E091FEE17FFFF64414
SHA1:	5CB3AD07CF6DFF3DB5BAAD55488A769A664BC093
SHA-256:	5172863C41E84024799B2034D42F10E9720FC53171A4F6C1CA2FDB2C6F71DFE9
SHA-512:	635DE182629A248B9BF3061E1A1C1D3ED904B8843187B64CEB3BF96DD4B10769D9E001EAEECED2179350F7012C82317B2C833A8501FF9C92D1A0CE94C711FEB
Malicious:	false
Preview:	..#.p.r.a.g.m.a. .n.a.m.e.s.p.a.c.e. .(. .".\.\.\.\...\.\.r.o.o.t.\.\.M.i.c.r.o.s.o.f.t.\.\.W.i.n.d.o.w.s.\.\.D.e.f.e.n.d.e.r.".).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.C.o.m.p.u.t.e.r.S.t.a.t.u.s.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.E.v.e.n.t.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.H.e.a.r.t.B.e.a.t.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.P.r.e.f.e.r.e.n.c.e.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.R.o.l.l.b.a.c.k.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.S.c.a.n.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.S.i.g.n.a.t.u.r.e.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.T.h.r.e.a.t.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.T.h.r.e.a.t.C.a.t.a.l.o.g.".,.n.o.f.a.i.l.).....#.p.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6717
Entropy (8bit):	5.162252158398129
Encrypted:	false
SSDEEP:	96:+WRspYDLPkQHFom1DW4DlHFposoSKYax9gDCk4Cp1PRsQHdBLe:DaVQHFB0AlHISKYoopoQHdxe

MD5:	CE7313760386B6ABDE405F9B9E6EA51D
SHA1:	F969931AC45991F7ECB6767A69433A7082ECCA2F
SHA-256:	73E26404B3571A9E859B3A1144F54C353172479586E0A23C3A7DDA0C1C0AE919
SHA-512:	CF990FC05FD3ED78FF35F1A1ACD5317626D46745BF7E4F8C62AA068A587ABF52F232080464F82692A2BB8C04A4FFA53599B933A4281BC7E697337720DB65BF29
Malicious:	false
Preview:	==========..1. C++ REST SDK (https://github.com/Microsoft/cpprestsdk)....C++ REST SDK ....The MIT License (MIT)....Copyright (c) Microsoft Corporation....All rights reserved.....Permission is hereby granted, free of charge, to any person ob taining a copy of..this software and associated documentation files (the "Software"), to deal in..the Software without restriction, including without limitation the rights to..use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of..the Software, and to permit persons to whom the Software is furnished to do so,..subject to the following conditions:....The above copyright notice and this permission notice shall be included in all..copies or substantial portions of the Software.....THE SOFTWA RE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR..IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANT ABILITY,..FITNESS FOR A PARTICULAR PURPO

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32520
Entropy (8bit):	5.0528261738229245
Encrypted:	false
SSDEEP:	384:1LrwfrhpOJs5f9AhVui8c+sEqEKSTGqWSa/WXDBRJENU6y50ZSxR9zus2+lhV:5riPAhfO1PqUB50Zi9zuih
MD5:	4E5123053E05141A5EB63D9A0F42CF73
SHA1:	CE858924D61F80191E88879D51CD3EE55326E68B
SHA-256:	A5C6448D3F01028AA24683BC19DCED26015C99DF387ECD5AD0268134C80F59AB
SHA-512:	301ECDA752150A1DD4352ECDDAD94086E7D73F040CF8DD5689C8D1D1C00DF7FDDCD73221769501C50F951746D0E3E33A92C50BDF0994BC6F476708F70E5731 2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..k*Fb.....!.....X.....@..... ...T.....Z...%.....rdata.. .....@..@.rsrc....T... ...V.....@..@....k*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.. ...%...O...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24328
Entropy (8bit):	6.163570071385243
Encrypted:	false
SSDEEP:	384:Nba9HtNfzRKLpPExWUN7W0WVQB8MwnWJD/oxN/pAWSa/WaDBRJu8u2vH3rPR9zuJ:Va9HtNfzRKLpcjZwQkD1Pn3l9zuA+
MD5:	21BE79263C6E56EA0544D065A041F35C
SHA1:	1433522BB2FACD1C34A4B533854EA5F6862EA5E9
SHA-256:	2AE3124C3B9AF7576B60CEB5D65B4066887095F22CC4F971CF385FC9B9C6ACB1
SHA-512:	788630212687034CF27FECAFB65D5A66C7FE71A8D25BBC05A11EE4DFBE1FF502B7C8058247BCF45D21A00CD69F14C3F0D2A109F07AB54156D86047F333DAD9 9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..I*Fb.....!.....8.....`.....@..... ..,5.....:..%.....rdata.. .....@..@.rsrc...,5... ...6.....@..@....I*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%..X0.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	60168
Entropy (8bit):	4.8899711940241986
Encrypted:	false
SSDEEP:	768:og0QI4V/O4klevfa7mvqaIzO1BiQZKfEflxZ3wp1Pz7dRmuU9zuk:QgMPP3d8zuk
MD5:	F8F15E8E63DE93C73D3A7F35DED10848
SHA1:	056ECE1B2A2254E4EF8C2D53EEA216A86BE3FACF
SHA-256:	166FA7B8F41F8BC7C5341909DEB69F0E0BF568EE91B0072CD342DBA61FC18D04

SHA-512:	0CD3D6C926B2492241061D96C19197BDD4087DD84572A933E29531D6631AB2B1A18ABBB0D7D413BA92F956CA590C6F7C2EE86CE7C9B67973BAD4C8775825D0 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L..... .....!.....@..... .....%.....8.....rdata..... .....@..@.rsrc..... .....@..@.....~D.....l...P...P.....~D.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....r src$01.....(..(....rsrc$02.... ...02.l...C[...2.#..&.;.CT..PK.~D..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	27400
Entropy (8bit):	5.6882764569289614
Encrypted:	false
SSDEEP:	384:5Yfz5kWYU1apG2R9U4HUy/HVWR69xlfWSa/WZDBRJvfwBmfWojR9zusw7g3v:iQU1apG2R9UiVWl9xok1PvPfWoF9zu8v
MD5:	6C67B7C4FE2F91C043179A43464A847A
SHA1:	43C1C050307AAC13AC9B218694C9A116EF5013AF
SHA-256:	DFC5DF9E5877D5889534C26643DEC95576FDD15F0E1BECD843B4A4C61324183C
SHA-512:	E6172F70FD9B7457D716E44FFDCB0FB98E523639AC8051D78BF24E7672ACFF3897922EF3251DA84378E7F29551BED2C1A7E628F0EC5108A5116367CE5FA3149D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..m*Fb.....!.....D.....p.....@..... ...A.....F...%.....rdata.. .....@..@.rsrc....A... ...B.....@..@....m*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%... <...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32016
Entropy (8bit):	5.700576446637723
Encrypted:	false
SSDEEP:	768:jbQPaPbPAPOPLTP6PWPkP8Pe1lOO6FD6kKOy6OQOQ4LuYz3KUrZPk//hPrPsSHZG:jblchYJP4pzH
MD5:	D75F773150E7540A1E84DBC62B9353AA
SHA1:	D5BD734FC4EA92525DF6D616B425C3F89B45500D
SHA-256:	B99BC2E8E576C46E63269638C01664C98C705E23438929D62EBBDCC6E4E86D05
SHA-512:	693EC384E3182746680B75327F3C9DF2AB450A9C6853507EC914A024E77C26E44535BDB4C68FD5FB1AED695529F7E32116E4FBEDA2A03F794927F45C667B08E8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..o*Fb.....!.....V.....@..... ...S.....X...%.....rdata.. .....@..@.rsrc....S... ...T.....@..@....o*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.. ...%..0N...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	31496
Entropy (8bit):	5.336191681213913
Encrypted:	false
SSDEEP:	768:lj1PJ4v3YFcFqFkFJFgFGFYF0Mx6F7aDd1P6adk9zu/:lj1LFcFqFkFJFgFGFYF3x6FW/P4zu/
MD5:	4D00A4FD04A744C53472F613D9FEB0EA
SHA1:	220B2A38FE0C4847A38A3FDCB6748257D3DF0053
SHA-256:	521DB53112E5535A29448CFC248BB2080EF00A2C500294F5A9252FAFA69D4F4A
SHA-512:	ECE748AB2C51C0FAE3624E7D2D13DD20BD3727FF5DD8DB7FCEDFB5D6E9DD14CB61DF72B9924EFECA7810937E0AB670923BBEA1F9CC015D090C843C3743A4 FE5F
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..q*Fb.....!.....T.....&d....@..... ...Q.....V...%.....rdata.. .....@..@.rsrc....Q... ...R.....@..@....q*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.. ...%...L...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\MpAsDesc.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	66832
Entropy (8bit):	4.750151277454491
Encrypted:	false
SSDEEP:	768:gBuDOYz0+U0TO/9VqhQGH1P2WF//dj9zg:oYcXqhQGVP2WZzg
MD5:	F9E8E0B8351F5D38E5788DC9F035C29F
SHA1:	C7B6DC52EF9F760B0ACA8D2F1BEFA290170818BB
SHA-256:	4453000A8A45725B2F210755563BBEDECD28678AFB777F991C57DF262D27D0C1
SHA-512:	FB5FC0347328DA11EEED7645C6919D7B376886E45495B026B7B21D7D96F5B8FF956DD6362CD991288579F0D676545D2C2E16DEEAC9179F9E48A1F24323B507D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L..... .....!.....@..... .....%.....8.....rdata..... .....@..@.rsrc..... .....@..@.....~D.....l...P...P.....~D.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....r src$01.....(..(....rsrc$02.... ...02.l...C[...2.#..&.;.CT..PK.~D..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32016
Entropy (8bit):	5.4341807197933445
Encrypted:	false
SSDEEP:	384:OGJOFGtxhDfmbMpouHuZ332Z3WSa/WrDBRJNXzC/R9zU5tWc:fs+hXpfOwQy1PNXzg9zCsc
MD5:	7473088906E5CF7ACE3CC384CD592519
SHA1:	0D4615B28D406026C76949C524C3C07545A6A6FF
SHA-256:	EC1936E60DE76915D7749EA11F32739924E0A79752013D8EA6183079D1E685E7
SHA-512:	6FC22591BFD16370F5C5824FFFBA87AC706A535314A6A17F6C16654E005FB1959108924605D5829976EE92F7AF2286D1DDE5FBDC43DDC06363F7EB8A4D24075
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..s*Fb.....!.....V.....@..... ...S.....X...%.....rdata.. .....@..@.rsrc....S... ...T.....@..@....s*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%...N.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32528
Entropy (8bit):	5.618562813722771
Encrypted:	false
SSDEEP:	768:uX333303MqF6WVHrS3stLXlFwozffQ6SMn6vvvU98/oEp5LWogte1eF3douJ1P67:t64H7ouvP6DozY
MD5:	C865A917635CBB299972AF487D09554B
SHA1:	20694376AF962CA358D58ACA2CA5E19F61755655
SHA-256:	682FA9604783AC9AEE4A487626ADAD7C0DDCC04B9535AD6EF16CF9B2C0237368
SHA-512:	553C10797AB351E93CDB5AF6B407416DB40EA0C5FDCD0082FF4F015925A314EE4A12F55F49B500E160E1EBF758EAC6D937B0AD7701F132219E8BD49A5CDB63 A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..t*Fb.....!.....X.....r.....@..... ...U.....Z...%.....rdata.. .....@..@.rsrc....U... ...V.....@..@....t*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%...Q.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	30992
Entropy (8bit):	5.1974491570344785
Encrypted:	false
SSDEEP:	384:FONq0HifHAHyuJv3JSFg8Ml/o001rO1gAGmDnoWSa/Wf5DBRJGMXXzC/R9zUIv:FWYuJYY/oVhOqGY51P/XXzg9zPv
MD5:	0D9C0297809D20592AC21A203703AA67
SHA1:	0B10257284385205D51FA4BF487DF17F8B89BF42
SHA-256:	F84DAAE902B2E58BF6CA5BC2940358C523FCD54B57CB76DB406962ADD2843ABE
SHA-512:	1008CE6291C3745D0BD8E796530D6D9105839F1E4E05384ED63AD563B40F903F6089FE5DC0FA257859936A0E70134CE3105066D4C48C1016357458BA0CDF7EA8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..u*Fb.....!.....R.....p.....)...@..... ...N.....T...%.....rdata.. .....@..@.rsrc....N... ...P.....@..@....u*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%...l.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32520
Entropy (8bit):	5.068955850455204
Encrypted:	false
SSDEEP:	768:6QBmfwxJvYOmnVmJYlEmnVY4mxYCOAlc5UEsUeYLSSJg94T4OM8i1PCg9zup:6VlY6yPZzup
MD5:	95158246D14FF9A7946C890FCA3834BD
SHA1:	2C4E53DA42C997FAC79BEE143619D4E726D1D3F8
SHA-256:	F07D583976FF2734427AC13B23C5DAAF0A74868E781DD6F42454E6BECBF6061C
SHA-512:	1021CFE60D6975A9DF15B42D6AD5DB37B9C191EFC7E23106720B90A34F9C724E1C51B095282333E6EDFB6C08EB43A214A4BC8DA19E035B74FF4846A2CC0C39 3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..x*Fb.....!.....X..... ....@..... ...T.....Z...%.....rdata.. .....@..@.rsrc....T... ...V.....@..@....x*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.....%...P.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	69896
Entropy (8bit):	4.2648067984070535
Encrypted:	false
SSDEEP:	768:UZH4mcWQ7uhqYxT352UL2dSsq558Vcdyuz9pUJ4cwQRMC20hvQii98+wEH4cdqj9:UUQ17uVc2RMZOhPDzu6
MD5:	7F44D2A53E6B9A90359BDB1F3270994D
SHA1:	5520DFD8B04F4DE25E65B8B6EBACEF1DF752485B
SHA-256:	6DB167C51136D8E235DAB3356DB56AF8D3764B494081008896C393460D1CE25B
SHA-512:	A0AEEFF96A523F576953167B46B15D31B81600B0A60FB3C0E4420304783D0E0D723A809C56AF9A4AD0548756FB52F2A3BBADF6A770F5AB8A3ECDC4A315E95FE 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L..... .....!.....".....@..... .....%.....8.....rdata..... .....@..@.rsrc..... .....@..@.....~D.....l...P...P.....~D.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....r src$01.....(..(....rsrc$02.... ...02.l...C[...2.#..&.;.CT..PK.~D..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	32520
Entropy (8bit):	5.037611764672926
Encrypted:	false
SSDEEP:	768:+7Db5bipJjCwb+kbsHtlb4H5YmSiMgrNDFWBGWn+YC29HdzMZ8lF1PAfWoF9zua:wT1biDPAf9Xzua
MD5:	F2E82FF440828F4792C84D1B8AE31637
SHA1:	032026761DA3FE46FEDCE79362BB1483109DFA0B
SHA-256:	14888EB1C9824102E013DDF8E53F2BF3A4EB3E541F29574EE8106EDDC4E7A12B
SHA-512:	602C233394C5FD080A10CD6ADFEA987C0D7860433EB8A1CB3BBDD7C5003B5B3CA17ED44CCD32894C7B38946C4C1DAE5EDE75016FFB121D4627E7329EA73A0 22C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..v*Fb.....!.....X.....{....@..... ...U.....Z...%.....rdata.. .....@..@.rsrc....U... ...V.....@..@....v*Fb.....l...4...4.....rdata.....rdata$voltmd...4...l....rdata$zzzdbg.... .....rsrc$01.. ...%...P...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.8011887903612696
Encrypted:	false
SSDEEP:	6:3HWSjKNde/Ott+dmvVnEuLrORVCqwvFFaFlLulkNCB+SrxxLxeNCWHyLIo:L2kO+WnEeMOUlLAjB/1N/0o
MD5:	60A2FC65D3CC1D3DE9ECD2C5319738FC
SHA1:	873D18E03523BBE80D1410AA475ED6CC2DAF0D9D
SHA-256:	6C6F52B13235148AF305BD614779EA885C00B64D0BB7CC764E3C67198CC524A2
SHA-512:	36E8930108DA1B953DC07809A9E670F923A4F07EAC9AD2A229844E556595CE7383F35001E43AA6877FF42D9BD42C55BB2BF0ED05E058D4E8CFF65E6B2B7A7BF D
Malicious:	false
Preview:	{.. "name": "com.microsoft.defender.browser_extension.native_message_host",.. "description": "Native host for Microsoft Defender Browser Extension",.. "path": "mpextms.exe",.. "type": "stdio",.. "allowed_origins": [.. "chrome-extension://echcggldkblhodogklpincgchnpgcdco/",.. "chrome-extension://lcmcgbabdcbngcbcfabdncm oppkajglo/"..]..}

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpAsDesc.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	64776
Entropy (8bit):	4.539762320385182
Encrypted:	false
SSDEEP:	768:fqqhXzlbrS2tVdqSpbwHjiKMQf4EEEddeat1Pv9/9zuHO:fJhXz1Lf04qjiKMQf4t8eabPLzuHO
MD5:	6EB48597411B21EA974EA7FB32BFC8B0
SHA1:	BED2E05BF31F26E4785316ABAC2950D1F45F5246
SHA-256:	DF15FB1B3D6AF1AB638B441E43A31F77CE15C65D55AA0F7275FE5737E32692F8
SHA-512:	7219DF21268F2E9C24F48B1F14D7C399B6E70243BF99B2DFBE01F502EF2F07D11904B3B6B44E05E468963B32E37ADA35D335E4BF18EFE010939807846AB4A0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L..... .....!.....@..... .....%.....8.....rdata..... .....@..@.rsrc..... .....@..@.....~D.....l...P...P.....~D.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....r src$01.....(..(....rsrc$02.... ...02.l...C[...2.#..&.;.CT..PK.~D..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpEvMsg.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54536
Entropy (8bit):	4.721448918628152
Encrypted:	false

SSDEEP:	768:3NMyciFk6/zRyodW7/obSxnj0v21PT4ed9zuzI:3NMyciFk6/zRy+bSxjyOPd/zuzI
MD5:	A0CC7D88E3250773D9A65306C89754CE
SHA1:	D0796FD9F81B3AA14DA467E0B33D3AC16031DC27
SHA-256:	C0C5A64EB1EE3A4B07AFE4F1339008D11F731E68587F5DE53589DCF4FC531F4A
SHA-512:	D294A08D1315AE9695F60BBEA0AB67AD8C5A48C1D2206AAD6ED9F699C640300C80650A13C8245B0B6806E8A6B09DC70DF88E5A28FE14AAE76E1D6102EDC3C 9A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L..... .....!.....I.....@..... .....%.....8.....rdata..... .....@..@.rsrc..... .....@..@.....q.....I...P...P.....q.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ....;.F...`..w.8.-.S..1.d.q....q..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	30480
Entropy (8bit):	5.302340783561848
Encrypted:	false
SSDEEP:	768:oY45SCVYNbEg20U2pC5DqH9PVrMB1P0EXzg9zII:oY45SCVYNbf20U2pC5DqH9PVrM3PRDoA
MD5:	3DE9335C531194088181B57CB1E9A327
SHA1:	5E95D46B1CC07D2A911E10F2EA98236E2BDCE41C
SHA-256:	14FE5259D9E30793CEBA234606986081165B5C28EBBFEEDF30DD6DAC90CA04B5
SHA-512:	284D6D4AB7013E89235187B13E6CB1410D0F81C2D4A1A327771ECA7873FDFB586A78EFF97D4161559219239C46E696BE8C390D67DDBD60D6AE67550995C7C68
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..z*Fb.....!.....P.....p.....@..... ...M.....R...%.....rdata... .....@..@.rsrc....M... ...N.....@..@....z*Fb.....I...4...4.....rdata.....rdata$voltmd...4...I....rdata$zzzdbg.... .....rsrc$01... ..%...H...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	33032
Entropy (8bit):	5.062234437378297
Encrypted:	false
SSDEEP:	384:EZ3aB5CKtgWhPbjY2YQYTZYRgaM3cNqng73m3cX3u3cjgTyTKT3TsjxTPTBTnTbn:/CNP9K17Xc502zr7MDg1PjK3l9zuADF
MD5:	365E7E85D1239892F39420F89DEE847D
SHA1:	DBA5C2BABB98EE17BCE73D8F71EE49BE16865CFE
SHA-256:	43A375E16C1B311BA47824A95841AF41D4E64BD233156ED8AA9905E0801B8326
SHA-512:	B92A0FD071C3BF1850C906FA43EB9998B25524E614076304D8E8C1A5FDADE775764577531C4F356CB52E4401939178D85742C0161795D2A0C28F2C0C14EC1C3E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L. ..}*Fb.....!.....Z.....d.....@..... ...V.....\...%.....rdata.. .....@..@.rsrc....V... ...X.....@..@....}*Fb.....I...4...4.....rdata.....rdata$voltmd...4...I....rdata$zzzdbg.... .....rsrc$01.....%...Q.. .rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpAsDesc.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	65288
Entropy (8bit):	4.288309702869772
Encrypted:	false
SSDEEP:	768:5XbQqbSuL8rmOXbO5OKi9O06k1P9QP9zuGHF:5rQqeuL8bs0P4zuI
MD5:	EA63A57BBC6871C805C4CF8E7CE21115
SHA1:	E9ACB22FBAEE96C229638F90441AF46ABAE9CCFE
SHA-256:	595AC536B9D8020F60B4E9F8D30D132AFCFB22A984B5867ABBA4FC748888C0CE

SHA-512:	651567895C8B222E34EF1BC41650A9678FAF09BEAA7023710EF2714A94D3B1054C042A5FA227ABFFC64FEFB93A3E5110C0D0F0E8DB53AC22DF4E4CA54B96E1D7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L.....!.....'....@..d.....%.....8.....rdata.....@..@.rsrc..... .....@..@.....~D.....l...P...P.....~D.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....rsrc$01.....(..(....rsrc$02.... ...02.l...C[...2.#..&.;.CT..PK.~D.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpEvMsg.dll.mui

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55560
Entropy (8bit):	4.517868844714394
Encrypted:	false
SSDEEP:	384:M7jcx80WKqt9o5uDwepIRXVCQECoz0NKERDH9rLdGtqWFwLWlDBRJxosRmuTcR9U:MMxnkCk1PxtRmuU9zux
MD5:	8CEBC84C305B92C55B9E2027D667B882
SHA1:	3E8B82DD11D610DF7440E917492420B94B061114
SHA-256:	A32D306D66B9ACE067639D208611A35DCA0E744BF64386355005BC2766094A1D
SHA-512:	EB21E59DC776A0E9958421D2BEB24E04BD843ABEF990454A9BF34E5F11D27A9C11B7B951E973B9F2EC2ADD013613252D43379D1471731550A14D3642AC84914
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t=.M.S.M.S.M.S..m..L.S..mQ.L.S.RichM.S.....PE..L.....!.....S.....@.....%.....8.....rdata.....@..@.rsrc..... .....@..@.....q.....l...P...P.....q.....$.....8....rdata..8.....rdata$voltmd...P.....rdata$zzzdbg.... .....rsrc$01.....8....rsrc$02.... ...;.F...`..w.8.-.S..1.d.q.....q.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.401310327702789
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
File size:	609224
MD5:	67a4759a7b2fcb1a7e5b368fc150b974
SHA1:	592934bd8f6606f80a890008008a621f7abda152
SHA256:	19762fa9a397bf711cb2aa16f78915d4beaf49e9b67ffccfa3e3b01e35c7289a
SHA512:	e7540621211cc64faee06b3cf17c69fe45fdb9a39e69e8404c284d44a518a624a812eca1e9f49dd0aead9d717f9bc52cc6c7f4c32535f42baa472884b84ba133
SSDEEP:	12288:5bspFozv47H44s5Q4IDT9jXbgO1xzSs9IKTQWfsmuYUE:5bsLnY4s5k0k9IKTQWkmuZE
TLSH:	9DD4F155BAC8ECABC01691B81475AF626A93FE2518748E03173E7E2FF732153243B91D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	38e6d3b1b3a2cc71

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FD2384DEDDAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FD2384DEDAAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax

Instruction
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6b000	0x27620	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x35000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6b000	0x27620	0x27800	False	0.363744808149	data	4.74589509923	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6b2f8	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x7bb20	0x94a8	data	English	United States
RT_ICON	0x84fc8	0x5488	data	English	United States
RT_ICON	0x8a450	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 6356992, next used block 0	English	United States
RT_ICON	0x8e678	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x90c20	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x91cc8	0x100	data	English	United States
RT_DIALOG	0x91dc8	0x11c	data	English	United States
RT_DIALOG	0x91ee8	0xc4	data	English	United States
RT_DIALOG	0x91fb0	0x60	data	English	United States
RT_GROUP_ICON	0x92010	0x5a	data	English	United States
RT_VERSION	0x92070	0x270	data	English	United States
RT_MANIFEST	0x922e0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Insweepi
FileVersion	27.29.17
CompanyName	CHRYSALIDAH
LegalTrademarks	Vrdi24
Comments	reconnoiterlbni
ProductName	petiolispill
FileDescription	Pratalkoholis
Translation	0x0409 0x04b0

Possible Origin

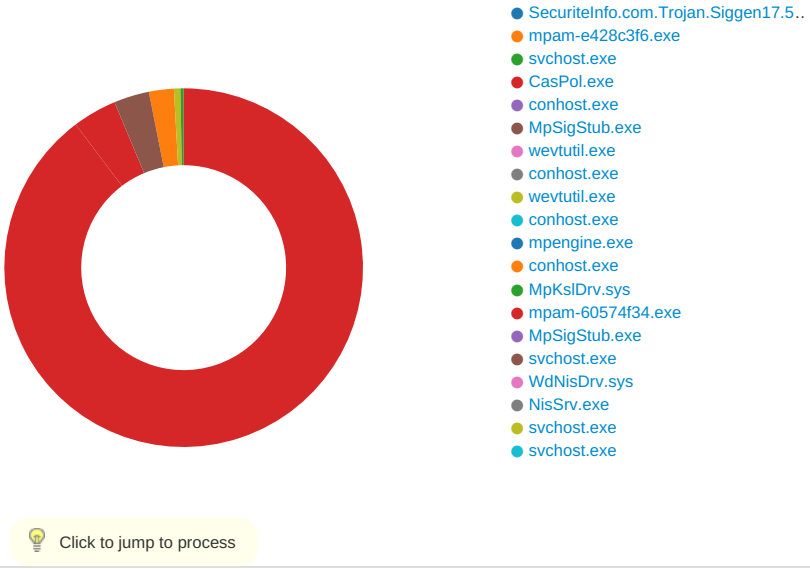
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe PID: 3120, Parent PID: 7904

General

Target ID:	1
Start time:	16:46:10
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe"
Imagebase:	0x400000
File size:	609224 bytes
MD5 hash:	67A4759A7B2FCB1A7E5B368FC150B974
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.18483403549.0000000002A10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: mpam-e428c3f6.exe PID: **1304**, Parent PID: **4880**

General

Target ID:	3
Start time:	16:46:14
Start date:	26/05/2022
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-e428c3f6.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e428c3f6.exe" /q WD
Imagebase:	0x7ff74e710000
File size:	112821704 bytes
MD5 hash:	89D4A3575EC6AEEFB442C18A41A18DDA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF74E71B773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74E71B1E3	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	success or wait	1	7FF74E7137CA	NtSetInformationFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 37 fd 6b 56 ab 56 ab 56 fd 78 24 e2 56 ab 56 fd 74 57 fd 24 23 e3 56 fd 78 24 fd fd 56 fd 78 24 c9 56 fd 78 24 fd 57 56 fd 78 24 14 fd fd 56 fd 24 23 ea 56 8c fd fd fd fd 56 fd 24 23 fd fd 75 50 fd 24 23 16 fd fd 56 fd 24 23 ea 56 fd 52 69 63 68 fd 56 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7VVVx$VVtW$#Vx VxVxWVxV$#VV$#uP$#V$#VRichV	success or wait	521	7FF74E71B2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	0	5624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 42 cf fd 23 fd fd fd 23 fd fd fd 23 fd fd 45 56 fd fd fd 23 fd fd 19 51 fd fd fd 23 fd fd 19 51 fd fd fd 23 fd fd 19 51 fd fd 18 23 fd fd 19 51 fd fd fd 23 fd fd fd 23 fd fd fd 22 fd fd 45 56 fd 67 23 fd fd 45 56 4e fd fd 23 fd fd 45 56 fd fd fd 23 fd fd 52 69 63 68 fd 23 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 a6 0e 50 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$B###EV#Q#Q#Q#Q ##"EV#EVN#EV#Rich#PEdP"	success or wait	26	7FF74E71B2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd fd 62 00 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 4a 46 03 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 70 46 03 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEdb" JFpF	success or wait	1677	7FF74E71B2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	0	3624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd 40 fd 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 4a 2e 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 70 2e 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEd@b" J.p.	success or wait	94	7FF74E71B2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	0	7248	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd fd 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 fd fd 02 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 fd fd 02 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEdb"	success or wait	1425	7FF74E71B2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd 40 fd 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 fd 15 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 20 16 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEd@b"	success or wait	45	7FF74E71B2C6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	unknown	262144	success or wait	66	7FF74E71B365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	unknown	262144	success or wait	4	7FF74E71B365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	unknown	262144	success or wait	210	7FF74E71B365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	unknown	262144	success or wait	12	7FF74E71B365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	unknown	262144	success or wait	178	7FF74E71B365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	unknown	262144	success or wait	6	7FF74E71B365	ReadFile

Analysis Process: svchost.exe PID: **7932**, Parent PID: **932**

General

Target ID:	4
Start time:	16:46:20
Start date:	26/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff655680000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **3872**, Parent PID: **3120**

General

Target ID:	5
Start time:	16:46:26
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen17.57062.9420.exe"
Imagebase:	0xb50000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.23244260810.000000001D881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.23244260810.000000001D881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.18323333088.0000000000F30000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F44CAE	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D313263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D313263	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D313263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D313263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C279B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C279B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D31099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2662DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D31D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D31D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D31D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D2662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2662DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D31099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D2662DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6C279B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	9	6C279B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\4f83a345-9a34-4194-a391-86900553d0e9	unknown	4096	success or wait	2	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C279B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6C279B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6C279B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D31099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D31099B	unknown

Analysis Process: conhost.exe PID: **4968**, Parent PID: **3872**

General

Target ID:	6
Start time:	16:46:26
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8620000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MpSigStub.exe PID: **1656**, Parent PID: **1304**

General

Target ID:	7
Start time:	16:46:32
Start date:	26/05/2022
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe /stub 1.1.18500.10 /payload 1.367.502.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e428c3f6.exe /q WD

Imagebase:	0x7ff6f4470000
File size:	803176 bytes
MD5 hash:	01F92DC7A766FF783AE7AF40FD0334FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\MpSigStub.log	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file | open reparse point	success or wait	1	7FF6F44DA6A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	0	2	fd fd		success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	2	164	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	166	68	53 00 74 00 61 00 72 00 74 00 20 00 74 00 69 00 6d 00 65 00 3a 00 20 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 20 00 31 00 35 00 3a 00 34 00 36 00 3a 00 33 00 32 00 5a 00 0d 00 0a 00	Start time: 2022-05-26 15:46:32Z	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	234	60	50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3a 00 20 00 36 00 37 00 38 00 2e 00 31 00 64 00 38 00 37 00 31 00 31 00 37 00 63 00 35 00 66 00 32 00 39 00 63 00 39 00 33 00 0d 00 0a 00	Process: 678.1d87117c5f29c93	success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	294	262	43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 3a 00 20 00 2f 00 73 00 74 00 75 00 62 00 20 00 31 00 2e 00 31 00 2e 00 31 00 38 00 35 00 30 00 30 00 2e 00 31 00 30 00 20 00 2f 00 70 00 61 00 79 00 6c 00 6f 00 61 00 64 00 20 00 31 00 2e 00 33 00 36 00 37 00 2e 00 35 00 30 00 32 00 2e 00 30 00 20 00 2f 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 45 00 52 00 56 00 49 00 43 00 7e 00 31 00 5c 00 4e 00 45 00 54 00 57 00 4f 00 52 00 7e 00 31 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 54 00 65 00 6d 00 70 00 5c 00 6d 00 70 00 61 00 6d 00 2d 00 65 00 34 00 32 00 38 00 63 00 33 00 66 00 36 00 2e 00 65 00 78 00 65 00 20 00 2f 00 71 00 20 00 57	Command: /stub 1.1.18500.10 /payload 1.367.502.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e428c3f6.exe /q W	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	556	38	41 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 3a 00 20 00 6e 00 6f 00 0d 00 0a 00	Administrator: no	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	594	46	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3a 00 20 00 31 00 2e 00 31 00 2e 00 31 00 38 00 35 00 30 00 30 00 2e 00 31 00 30 00 0d 00 0a 00	Version: 1.1.18500.10	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	640	172	0d 00 0a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 20 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 53 00 65 00 61 00 72 00 63 00 68 00 20 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 0d 00 0a 00 0d 00 0a 00	================================ ProductSearch ================================	success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	812	1722	20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 20 00 28 00 52 00 53 00 31 00 2b 00 29 00 3a 00 20 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 53 00 74 00 61 00 74 00 75 00 73 00 3a 00 20 00 41 00 63 00 74 00 69 00 76 00 65 00 20	Microsoft Windows Defender (RS1+): Status: Active	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	2534	172	0d 00 0a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 20 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 44 00 69 00 73 00 63 00 6f 00 76 00 65 00 72 00 79 00 20 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 0d 00 0a 00 0d 00 0a 00	============================== PackageDiscovery =========== =================== =	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	2706	1806	20 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 20 00 66 00 69 00 6c 00 65 00 73 00 20 00 64 00 69 00 73 00 63 00 6f 00 76 00 65 00 72 00 65 00 64 00 3a 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 3a 00 20 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 45 00 52 00 56 00 49 00 43 00 7e 00 31 00 5c 00 4e 00 45 00 54 00 57 00 4f 00 52 00 7e 00 31 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 54 00 65 00 6d 00 70 00 5c 00 32 00 43 00 33 00 39 00 45 00 32 00 42 00 32 00 2d 00 39 00 36 00 34 00 30 00 2d 00 34 00 35 00 31 00 36 00 2d 00 42 00 30 00 36 00 38 00 2d 00 38	Package files discovered: Directory: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8	success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	4512	336	20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 41 00 4d 00 20 00 46 00 45 00 3a 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 45 00 6e 00 67 00 69 00 6e 00 65 00 3a 00 20 00 31 00 2e 00 31 00 2e 00 31 00 39 00 32 00 30 00 30 00 2e 00 36 00 0d 00 0a 00 20 00 20 00 41 00 53 00 20 00 62 00 61 00 73 00 65 00 20 00 56 00 44 00 4d 00 3a 00 20 00 31 00 2e 00 33 00 36 00 37 00 2e 00 30 00 2e 00 30 00 20 00 20 00 0d 00 0a 00 20 00 20 00 41 00 56 00 20 00 62 00 61 00 73 00 65 00 20 00 56 00 44 00 4d 00 3a 00 20 00 31 00 2e 00 33 00 36 00 37 00 2e 00 30 00 2e 00 30 00 20 00 20 00 0d 00 0a 00 20 00 41 00 53 00 20 00 64 00 65 00 6c 00 74 00 61 00 20 00 56 00 44 00 4d 00 3a 00 20 00 31	AM FE: Engine: 1.1.19200.6 AS base VDM: 1.367.0.0 AV base VDM: 1.367.0.0 AS delta VDM: 1	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	4848	172	0d 00 0a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 20 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 0d 00 0a 00 0d 00 0a 00	==================================== Update ==================================== =	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	5020	100	20 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 20 00 6e 00 61 00 6d 00 65 00 3a 00 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 20 00 28 00 52 00 53 00 31 00 2b 00 29 00 0d 00 0a 00	Product name: Microsoft Windows Defender (RS1+)	success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	5120	1630	20 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 20 00 66 00 69 00 6c 00 65 00 73 00 3a 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 3a 00 20 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 45 00 52 00 56 00 49 00 43 00 7e 00 31 00 5c 00 4e 00 45 00 54 00 57 00 4f 00 52 00 7e 00 31 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 54 00 65 00 6d 00 70 00 5c 00 32 00 43 00 33 00 39 00 45 00 32 00 42 00 32 00 2d 00 39 00 36 00 34 00 30 00 2d 00 34 00 35 00 31 00 36 00 2d 00 42 00 30 00 36 00 38 00 2d 00 38 00 30 00 34 00 34 00 42 00 34 00 39 00 45 00 33 00 46 00 39 00 35 00 0d 00 0a 00 20 00 20 00 6d 00 70 00 61 00 73 00 62 00 61 00 73	Package files: Directory: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95 mpasbas	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	6750	470	53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 4c 00 6f 00 63 00 61 00 74 00 69 00 6f 00 6e 00 20 00 63 00 68 00 61 00 6e 00 67 00 65 00 64 00 20 00 66 00 72 00 6f 00 6d 00 20 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 44 00 61 00 74 00 61 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 44 00 65 00 66 00 69 00 6e 00 69 00 74 00 69 00 6f 00 6e 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 73 00 5c 00 7b 00 37 00 36 00 31 00 33 00 45 00 45 00 42 00 35 00 2d 00 38 00 34 00 33 00 34 00 2d 00 34 00 42 00 46 00 37 00 2d 00 38 00 36 00 34 00 36 00 2d 00 41 00 41 00 41 00 39 00 33 00 34 00 32 00 34 00 35 00 42 00 42	SignatureLocation changed from C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB	success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	7220	220	53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 20 00 75 00 70 00 64 00 61 00 74 00 65 00 64 00 20 00 66 00 72 00 6f 00 6d 00 20 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 45 00 52 00 56 00 49 00 43 00 7e 00 31 00 5c 00 4e 00 45 00 54 00 57 00 4f 00 52 00 7e 00 31 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 54 00 65 00 6d 00 70 00 5c 00 32 00 43 00 33 00 39 00 45 00 32 00 42 00 32 00 2d 00 39 00 36 00 34 00 30 00 2d 00 34 00 35 00 31 00 36 00 2d 00 42 00 30 00 36 00 38 00 2d 00 38 00 30 00 34 00 34 00 42 00 34 00 39 00 45 00 33 00 46 00 39 00 35 00 0d 00 0a 00	Signatures updated from C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	7440	172	0d 00 0a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 20 00 56 00 61 00 6c 00 69 00 64 00 61 00 74 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 20 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 0d 00 0a 00 0d 00 0a 00	================================ ValidateUpdate =================================	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	7612	182	4d 00 70 00 53 00 69 00 67 00 53 00 74 00 75 00 62 00 20 00 73 00 75 00 63 00 63 00 65 00 73 00 73 00 66 00 75 00 6c 00 6c 00 79 00 20 00 75 00 70 00 64 00 61 00 74 00 65 00 64 00 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 20 00 28 00 52 00 53 00 31 00 2b 00 29 00 20 00 75 00 73 00 69 00 6e 00 67 00 20 00 74 00 68 00 65 00 20 00 41 00 4d 00 20 00 46 00 45 00 20 00 70 00 61 00 63 00 6b 00 61 00 67 00 65 00 2e 00 0d 00 0a 00	MpSigStub successfully updated Microsoft Windows Defender (RS1+) using the AM FE package.	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	7794	4	0d 00 0a 00		success or wait	1	7FF6F44DA78A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	7798	504	20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 3a 00 20 00 20 00 20 00 20 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 64 00 20 00 74 00 6f 00 3a 00 0d 00 0a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 45 00 6e 00 67 00 69 00 6e 00 65 00 3a 00 20 00 31 00 2e 00 31 00 2e 00 31 00 38 00 35 00 30 00 30 00 2e 00 31 00 30 00 20 00 20 00 31 00 2e 00 31 00 2e 00 31 00 39 00 32 00 30 00 30 00 2e 00 36 00 0d 00 0a 00 20 00 20 00 41 00 53 00 20 00 62 00 61 00 73 00 65 00 20 00 56 00 44 00 4d 00 3a 00 20 00 31 00 2e 00 33 00 34 00 39 00 2e 00 30 00 2e 00 30 00 20 00 20 00 20 00 20 00 20 00 31 00 2e 00 33 00 36 00 37 00 2e 00 30 00 2e 00 30 00 20 00 20 00 0d 00 0a 00 20 00 20	Original: Updated to: Engine: 1.1.18500.10 1.1.19200.6 AS base VDM: 1.349.0.0 1.367.0.0	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	8302	4	0d 00 0a 00		success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	8306	64	45 00 6e 00 64 00 20 00 74 00 69 00 6d 00 65 00 3a 00 20 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 20 00 31 00 35 00 3a 00 34 00 36 00 3a 00 34 00 32 00 5a 00 0d 00 0a 00	End time: 2022-05-26 15:46:42Z	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	8370	164	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF6F44DA78A	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpSigStub.log	8534	4	0d 00 0a 00		success or wait	1	7FF6F44DA78A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB1}\mpengine.dll	unknown	262144	success or wait	62	7FF6F44DA8F5	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB1}\mpasbase.vdm	unknown	262144	success or wait	195	7FF6F44DA8F5	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB1}\mpavbase.vdm	unknown	262144	success or wait	201	7FF6F44DA8F5	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB1}\mpasdlta.vdm	unknown	262144	success or wait	24	7FF6F44DA8F5	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{7613EEB5-8434-4BF7-8646-AAA934245BB1}\mpavdlta.vdm	unknown	262144	success or wait	19	7FF6F44DA8F5	ReadFile
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\MpClient.dll	unknown	262144	success or wait	5	7FF6F44DA8F5	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	unknown	262144	success or wait	210	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	unknown	262144	success or wait	12	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	unknown	262144	success or wait	178	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	unknown	262144	success or wait	6	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	unknown	262144	success or wait	66	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	unknown	262144	success or wait	4	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasbase.vdm	unknown	262144	success or wait	210	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpasdlta.vdm	unknown	262144	success or wait	12	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavbase.vdm	unknown	262144	success or wait	178	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpavdlta.vdm	unknown	262144	success or wait	6	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\mpengine.dll	unknown	262144	success or wait	66	7FF6F44DA8F5	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\2C39E2B2-9640-4516-B068-8044B49E3F95\MpSigStub.exe	unknown	262144	success or wait	4	7FF6F44DA8F5	ReadFile

Analysis Process: wevtutil.exe PID: **5392**, Parent PID: **3180**

General

Target ID:	8
Start time:	16:46:35
Start date:	26/05/2022
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\3FCB5F68-CD33-FF2F-34AE-798C9A7026D4.man
Imagebase:	0x7ff74a790000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **9144**, Parent PID: **5392**

General

Target ID:	9
Start time:	16:46:35
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8620000
File size:	875008 bytes

MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wevtutil.exe PID: **7292**, Parent PID: **3180**

General

Target ID:	10
Start time:	16:46:37
Start date:	26/05/2022
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\3FCB5F68-CD33-FF2F-34AE-798C9A7026D4.man "/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll" "/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll" "/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll"
Imagebase:	0x7ff74a790000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{0a002690-3839-4e3a-b3b6-96d8df868d99}	NULL	unicode	Microsoft-Antimalware-Engine	success or wait	1	7FF74A7C195C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{0a002690-3839-4e3a-b3b6-96d8df868d99}	ResourceFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{0a002690-3839-4e3a-b3b6-96d8df868d99}	MessageFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{0a002690-3839-4e3a-b3b6-96d8df868d99}	ParameterFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{68621c25-df8d-4a6b-aabc-19a22e296a7c}	NULL	unicode	Microsoft-Antimalware-Engine-Instrumentation	success or wait	1	7FF74A7C195C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{68621c25-df8d-4a6b-aabc-19a22e296a7c}	ResourceFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{68621c25-df8d-4a6b-aabc-19a22e296a7c}	MessageFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{68621c25-df8d-4a6b-aabc-19a22e296a7c}	ParameterFileName	expand unicode	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll	success or wait	1	7FF74A7C1A0C	RegSetValueExW

Analysis Process: conhost.exe PID: **5416**, Parent PID: **7292**

General

Target ID:	11
Start time:	16:46:37
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8620000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mpengine.exe PID: **7860**, Parent PID: **3180**

General

Target ID:	12
Start time:	16:46:41
Start date:	26/05/2022
Path:	C:\ProgramData\Microsoft\Windows Defender\Scans\MpPayloadData\mpengine.exe
Wow64 process (32bit):	false
Commandline:	C:\ProgramData\Microsoft\Windows Defender\Scans\\MpPayloadData\mpengine.exe
Imagebase:	0x7ff71c580000
File size:	91528 bytes
MD5 hash:	C84EBFCFAFEB07D863C3ED18F6FBD40F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **8572**, Parent PID: **7860**

General

Target ID:	13
Start time:	16:46:41
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8620000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpKslDrv.sys PID: **4**, Parent PID: **-1**

General

Target ID:	14
Start time:	16:46:42
Start date:	26/05/2022
Path:	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{EBBB10C2-099A-4A41-A364-F566D3127AB4}\MpKslDrv.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	137464 bytes
MD5 hash:	97D3A85D7EF930E7035DAAC1622AD407
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MpKsl1c70f6d2\Parameters	success or wait	1	FFFFF80571208BB5	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MpKsl1c70f6d2\Parameters\Wdf	success or wait	1	FFFFF80571208BB5	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MpKsl1c70f6d2\Parameters\Wdf	WdfMajorVersion	dword	1	success or wait	1	FFFFF80571208BB5	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MpKsl1c70f6d2\Parameters\Wdf	WdfMinorVersion	dword	15	success or wait	1	FFFFF80571208BB5	NtSetValueKey

Analysis Process: mpam-60574f34.exe PID: **2156**, Parent PID: **4880**

General

Target ID:	16
Start time:	16:46:44
Start date:	26/05/2022
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-60574f34.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-60574f34.exe
Imagebase:	0x7ff700eb0000
File size:	8690936 bytes
MD5 hash:	50BCDEEB6A1DFFF15B62BEDAC2DDACA8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	13	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\endpointdlp.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpAsDesc.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	9	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpClient.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetours.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetoursCopyAccelerator.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpOAV.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MsMpLics.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\endpointdlp.dll	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mpextms.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCmdRun.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCopyAccelerator.exe	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-bg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-bg\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-cz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-cz\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-cz\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-dk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-dk\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-dk\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-de	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-de\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-de\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-de\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-gr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-gr\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-gr\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-us	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-us\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-us\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-us\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-es	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-es\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-es\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-es\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-ee	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-ee\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-fi	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-fi\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-fi\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-fr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-fr\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-fr\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-fr\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-hr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-hr\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-hu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-hu\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-hu\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-it	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-it\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-it\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-it\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-jp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-jp\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-jp\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-jp\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-kr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-kr\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-kr\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-kr\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-lt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-lt\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-lv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-lv\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-no	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-no\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-no\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-nl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-nl\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-nl\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-pl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-pl\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-pl\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-br	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-br\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-br\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-br\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-pt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-pt\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-pt\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-ro	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-ro\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-ru	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-ru\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-ru\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-ru\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-sk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-sk\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-latn-rs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-latn-rs\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-se	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-se\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-se\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-th	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-th\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-tr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-tr\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-tr\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-ua	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-ua\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-vn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-vn\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\mpuxagent.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-cn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-cn\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-cn\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-cn\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-tw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-tw\MpAsDesc.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-tw\MpEvMsg.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-tw\ProtectionManagement.dll.mui	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF700EBB773	CreateDirectoryW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FF700EBB773	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF700EBB1E3	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\endpointdlp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\endpointdlp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpAsDesc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpAsDesc.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpClient.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpClient.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetours.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetours.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetoursCopyAccelerator.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetoursCopyAccelerator.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpOAV.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpOAV.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MsMpLics.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MsMpLics.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\endpointdlp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\endpointdlp.dll	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mpextms.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mpextms.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCmdRun.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCmdRun.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCopyAccelerator.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCopyAccelerator.exe	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Path	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\mpuxagent.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpAsDesc.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpEvMsg.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\ProtectionManagement.dll.mui	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp	success or wait	1	7FF700EB37CA	NtSetInformationFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp	success or wait	1	7FF700EB37CA	NtSetInformationFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml	0	15565	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 43 6f 6d 70 75 74 65 72 53 74 61 74 75 73 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20 20 20 3c 44 65 66 61 75 6c 74 4e 6f 75 6e 3e 4d 70	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT _MpComputerStatus"> <Version>1.0</Version> <DefaultNoun>Mp	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml	0	17203	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 72 6f 6f 74 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 50 72 65 66 65 72 65 6e 63 65 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="root\Microsoft\Windows\Defender\MSFT_MpPreference" ClassVersion="1.0"> <Version>1.0</Version>	success or wait	5	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml	0	16417	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 52 6f 6c 6c 62 61 63 6b 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20 20 20 3c 44	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpRollback" ClassVersion="1.0"> <Version>1.0</Version> <D	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml	0	14920	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 53 63 61 6e 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20 20 20 3c 44 65 66 61 75	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpScan" ClassVersion="1.0"> <Version>1.0</Version> <Defau	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml	0	16877	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 53 69 67 6e 61 74 75 72 65 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20 20 20 3c	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpSignature" ClassVersion="1.0"> <Version>1.0</Version> <	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml	0	13918	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 54 68 72 65 61 74 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreat" ClassVersion="1.0"> <Version>1.0</Version>	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml	0	16048	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 54 68 72 65 61 74 43 61 74 61 6c 6f 67 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatCatalog" ClassVersion="1.0"> <Version>1.0</Version>	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml	0	14135	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 54 68 72 65 61 74 44 65 74 65 63 74 69 6f 6e 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatDetection" ClassVersion="1.0"> <Version>1.0</Version>	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml	0	15776	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 50 6f 77 65 72 53 68 65 6c 6c 4d 65 74 61 64 61 74 61 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 63 6d 64 6c 65 74 73 2d 6f 76 65 72 2d 6f 62 6a 65 63 74 73 2f 32 30 30 39 2f 31 31 22 3e 0d 0a 20 20 3c 43 6c 61 73 73 20 43 6c 61 73 73 4e 61 6d 65 3d 22 52 4f 4f 54 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 65 66 65 6e 64 65 72 5c 4d 53 46 54 5f 4d 70 57 44 4f 53 63 61 6e 22 20 43 6c 61 73 73 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 56 65 72 73 69 6f 6e 3e 31 2e 30 3c 2f 56 65 72 73 69 6f 6e 3e 0d 0a 20 20 20 20 3c 44 65	<?xml version="1.0" encoding="utf-8"?> <PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11"> <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpWDOScan" ClassVersion="1.0"> <Version>1.0</Version> <De	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll	0	15130	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 fd 04 fd 50 fd 57 fd 50 fd 57 fd 50 fd 57 fd 28 17 57 fd 50 fd 57 fd 28 fd 56 fd 50 fd 57 fd 50 fd 57 66 51 fd 57 fd 28 fd 56 fd 50 fd 57 fd 28 fd 56 fd 50 fd 57 fd 28 fd 56 2a 50 fd 57 fd 28 fd 56 fd 50 fd 57 fd 28 fd 56 fd 50 fd 57 fd 28 7b 57 fd 50 fd 57 fd 28 fd 56 fd 50 fd 57 52 69 63 68 fd 50 fd 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$1PWPWPW(WPW(VP WPWfQW(VPW(VPW(V*PW(VPW(VPW({W PW(VPWRichPWPEd	success or wait	14	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll	0	1554	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd fd 1e 3c 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1e 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 10 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEd<"	success or wait	8	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll	0	20746	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 33 fd 5a 01 77 fd 34 52 77 fd 34 52 77 fd 34 52 3c fd 35 53 64 fd 34 52 77 fd 35 52 36 fd 34 52 3c fd 37 53 63 fd 34 52 3c fd 30 53 5c fd 34 52 3c fd 31 53 fd fd 34 52 3c fd fd 52 75 fd 34 52 3c fd 34 53 76 fd 34 52 3c fd 3d 53 6b 34 52 3c fd fd 52 76 fd 34 52 3c fd 36 53 76 fd 34 52 52 69 63 68 77 fd 34 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$3Zw4Rw4Rw4R<5S d4Rw5R64R<7Sc4R<0S\4R<1S4R<Ru4R<4Sv4R<=S4R<Rv4R<6Sv4RRichw4RPEd	success or wait	42	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll	0	23554	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 78 fd fd 19 fd 19 fd 19 fd fd 61 fd 19 fd fd 61 fd fd fd 19 fd fd 61 fd 19 fd 61 60 fd fd 19 fd 19 fd 42 18 fd fd 61 fd fd fd 19 fd fd 61 0e fd fd 19 fd fd 61 fd 19 fd fd 61 fd fd 5c 19 fd cd fd fd 19 fd fd 61 0c fd fd 19 fd fd 61 fd 19 fd 52 69 63 68 fd 19 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$xaaaa`Baaaa\aa Rich	success or wait	39	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll	0	30450	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2a fd fd 5b 6e 4d 08 6e 4d 08 6e 4d 08 25 fd fd 09 60 4d 08 25 fd fd 09 60 4d 08 25 fd fd 09 67 4d 08 67 fd 1e 08 7f 4d 08 6e 4c 08 34 0d 08 25 fd fd 09 43 4d 08 25 fd fd 09 6f 4d 08 25 fd fd 09 35 4d 08 25 fd 72 08 6f 4d 08 25 fd fd 09 6f 4d 08 52 69 63 68 6e 4d 08 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 34 5e 0f 04 00 00 00	MZ@!L!This program cannot be run in DOS mode.$*[nnn%`%`%ggn4%C%o%5%ro%oRichnPEd4^	success or wait	12	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll	0	25066	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 20 25 1c 65 64 44 72 36 64 44 72 36 64 44 72 36 2f 3c 73 37 74 44 72 36 2f 3c 76 37 68 44 72 36 2f 3c 71 37 6c 44 72 36 6d 3c fd 36 6b 44 72 36 64 44 73 36 51 45 72 36 2f 3c 77 37 4e 44 72 36 2f 3c 72 37 65 44 72 36 2f 3c 7b 37 2d 44 72 36 2f 3c fd 36 65 44 72 36 2f 3c 70 37 65 44 72 36 52 69 63 68 64 44 72 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$ %edDr6dDr6dDr6/<s7tDr6/<v7hDr6/<q7lDr6m<6kDr6dDs6QEr6/<w7NDr6/<r7eDr6/<{7-Dr6/<6eDr6/<p7eDr6RichdDr6PEd	success or wait	6	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll	0	15594	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d fd fd 75 69 fd fd 26 69 fd fd 26 69 fd fd 26 22 fd fd 27 63 fd fd 26 22 fd fd 27 65 fd fd 26 22 fd fd 27 61 fd fd 26 60 fd 38 26 66 fd fd 26 69 fd fd 26 79 fd fd 26 22 fd fd 27 40 fd fd 26 22 fd fd 27 68 fd fd 26 22 fd fd 27 56 fd fd 26 22 fd 54 26 68 fd fd 26 22 fd fd 27 68 fd fd 26 52 69 63 68 69 fd fd 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$-ui&i&i&'"c&'" e&'"a&`8&f&i&y&'"@&'"h &'"V&"T& h&'"h&Richi&PEd	success or wait	4	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll	0	10218	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 3d fd 72 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1e 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 10 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEd=r"	success or wait	6	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	0	29402	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7e fd fd 26 3a fd 75 3a fd 75 3a fd 75 71 fd fd 74 2b fd 75 3a fd 75 14 fd 75 71 fd fd 74 21 fd 75 71 fd fd 74 35 fd 75 71 fd fd 74 fd fd 75 71 fd fd 74 3b fd 75 71 fd fd 74 76 fd 75 71 fd 73 75 3b fd 75 71 fd fd 74 3b fd 75 52 69 63 68 3a fd 75 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 45 2c fd 61 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$~&:u:u:uqt+u:uuqt!uqt5uqtuqt;uqtvuqsu;uqt;uRich:uPEdE,a"	success or wait	16	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	0	15826	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a 46 73 3e fd fd 20 3e fd fd 20 3e fd fd 20 75 fd fd 21 29 fd fd 20 3e fd fd 20 2d fd 20 75 fd fd 21 2a fd fd 20 75 fd fd 21 15 fd fd 20 75 fd fd 21 fd fd 20 75 fd 15 20 3c fd fd 20 75 fd fd 21 3f fd fd 20 75 fd fd 21 ac fd 20 75 fd 17 20 3f fd fd 20 75 fd fd 21 3f fd fd 20 52 69 63 68 3e fd fd 20 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd 68 6d fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$zs> > > u!) > u!* u! u! u < u!? u! u ? u!? Rich> PEdhm	success or wait	56	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	0	22722	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 25 fd fd fd 44 fd fd 44 fd fd 44 fd 3c fd fd fd 44 fd fd 44 fd fd 61 44 fd 3c fd fd fd 44 fd 3c fd fd fd 44 fd 3c fd 01 44 fd 3c 09 fd fd 44 fd 3c fd fd 44 fd 3c fd fd fd 44 fd 3c 0b fd fd 44 fd 3c fd fd fd 44 fd 52 69 63 68 fd 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 6a 45 63 00 00 00	MZ@!L!This program cannot be run in DOS mode.$%DDD<DDaD<D <D< D<D<D<D<D<DRichDPE djEc	success or wait	28	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll	0	5050	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 16 fd 67 52 3f fd 52 3f fd 52 3f fd 19 fd fd fd 44 3f fd 19 fd fd fd 41 3f fd 19 fd fd fd 58 3f fd 5b fd 2c fd 45 3f fd 52 3e fd 33 bf fd 19 fd fd fd 63 3f fd 19 fd 42 fd 50 3f fd 19 fd fd fd 53 3f fd 19 fd fd fd 2a 7f fd 75 02 fd fd 55 3f fd 19 fd 40 fd 53 3f fd 19 fd fd fd 53 3f fd 52 69 63 68 52 3f fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$RRRDAX[,ER3cBPS*uU@SSRichR	success or wait	111	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll	0	32426	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 47 32 1c 48 26 5c 4f 48 26 5c 4f 48 26 5c 4f 03 5e 5d 4e 5b 26 5c 4f 03 5e 58 4e 45 26 5c 4f 03 5e 5f 4e 40 26 5c 4f 41 5e fd 4f 46 26 5c 4f 48 26 5d 4f 1b 27 5c 4f 03 5e 59 4e 62 26 5c 4f 03 5e 5c 4e 49 26 5c 4f 03 5e 55 4e 18 26 5c 4f 03 5e fd 4f 49 26 5c 4f 03 5e 5e 4e 49 26 5c 4f 52 69 63 68 48 26 5c 4f 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 62 07 00 00 00	MZ@!L!This program cannot be run in DOS mode.$G2H&\OH&\OH&\O ^]N[&\O^XNE&\O^_N@&\OA^OF&\OH&]O'\O^YNb&\O^\NI&\O^UN&\O^OI&\ O^^NI&\ORichH&\OPEdb	success or wait	5	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll	0	6562	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4b fd fd 04 0f fd fd 57 0f fd fd 57 0f fd fd 57 44 fd fd 56 1b fd fd 57 44 fd fd 56 01 fd fd 57 44 fd fd 56 05 fd fd 57 06 fd 13 57 20 fd fd 57 0f fd fd 57 fd fd fd 57 44 fd fd 56 23 fd fd 57 44 fd 7d 57 0d fd fd 57 44 fd fd 56 0e fd fd 57 44 fd fd 56 6f fd fd 57 44 fd 7f 57 0e fd fd 57 44 fd fd 56 0e fd fd 57 52 69 63 68 0f fd fd 57 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$KWWWDVWDVWDVWW WWWDV#WD}WWDVWDVoWDWWDVWRichWPEd	success or wait	18	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll	0	5274	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd 46 fd 5a 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1e 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 10 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEdFZ"	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll	0	16274	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 27 fd 12 63 fd fd fd 63 fd fd fd 63 fd fd fd 28 f7 fd 70 fd fd fd 63 fd fd fd b6 fd 28 f2 fd 79 fd fd fd 28 f5 fd 6c fd fd fd 28 f3 fd fd fd fd fd 28 f6 fd 62 fd fd fd 28 ff fd fd fd 28 fd 49 fd 62 fd fd fd 28 f4 fd 62 fd fd fd 52 69 63 68 63 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$'ccc(pc(y(l((b((Ib(bRichcPEd	success or wait	25	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\endpointdlp.dll	0	27266	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 6e fd 62 fd 0f fd 31 fd 0f fd 31 fd 0f fd 31 fd 77 fd 30 fd 0f fd 31 fd 0f fd 31 fd 0e fd 31 fd 77 fd 30 fd 0f fd 31 fd 77 fd 30 fd 0f fd 31 fd 77 fd 30 70 0f fd 31 fd 77 77 31 fd 0f fd 31 fd 77 fd 30 fd 0f fd 31 fd 77 fd 30 23 0f fd 31 fd 77 75 31 fd 0f fd 31 fd 77 fd 30 fd 0f fd 31 52 69 63 68 fd 0f fd 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$nb111w0111w01w01w0p1ww11w01w0#1wu11w01Rich1PEd	success or wait	22	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpAsDesc.dll	0	5498	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 7a 31 1e 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELz1!	success or wait	7	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpClient.dll	0	114	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f	MZ@!L!This program cannot be run in DOS mo	success or wait	30	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetours.dll	0	25978	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7f 7a 56 fd 3b 1b 38 fd 3b 1b 38 fd 3b 1b 38 fd 70 63 39 fd 2b 1b 38 fd 70 63 3b fd 30 1b 38 fd 32 63 fd fd 34 1b 38 fd 3b 1b 39 fd 0a 1a 38 fd 70 63 3d fd 1c 1b 38 fd 70 63 38 fd 3a 1b 38 fd 70 63 31 fd 72 1b 38 fd 70 63 3c fd 34 1b 38 fd 70 63 f0 3a 1b 38 fd 70 63 3a fd 3a 1b 38 fd 52 69 63 68 3b 1b 38 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0e fd fd fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$zV;8;8;8pc9+8pc;082c48;98pc=8pc8:8pc1r8pc<48 pc:8pc::8Rich;8PEL	success or wait	4	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetoursCopyAccelerator.dll	0	13418	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 65 fd 47 fd 21 fd 29 fd 21 fd 29 fd 21 fd 29 fd 6a fd 28 fd 2b fd 29 fd 6a fd 2a fd 2a fd 29 fd 28 fd fd fd 2e fd 29 fd 21 fd 28 fd 2d fd 29 fd 6a fd 2c fd 07 fd 29 fd 6a fd 29 fd 20 fd 29 fd 6a fd 20 fd 1e fd 29 fd 6a fd 2d fd 31 fd 29 fd 6a fd b6 20 fd 29 fd 6a fd 2b fd 20 fd 29 fd 52 69 63 68 21 fd 29 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$eG!)!)!)j(+)j**)(.)!(-)j,)j))j)j-1)j)j+)Rich!)PEL	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpOAV.dll	0	15730	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 4e 73 75 fd 2f 1d 26 fd 2f 1d 26 fd 2f 1d 26 fd 57 1c 27 fd 2f 1d 26 fd 2f 1c 26 fd 2e 1d 26 fd 57 1e 27 fd 2f 1d 26 fd 57 18 27 55 2f 1d 26 fd 57 1d 27 fd 2f 1d 26 fd 57 14 27 fd 2f 1d 26 fd 57 19 27 fd 2f 1d 26 fd 57 fd 26 fd 2f 1d 26 fd 57 1f 27 fd 2f 1d 26 52 69 63 68 fd 2f 1d 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 17 31 10 2d 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Nsu/&/&/&W'/&/&.&W'/&W'U/&W'/&W'/&W'/&W&/&W'/&Rich/&PEL1-	success or wait	14	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MsMpLics.dll	0	6778	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 18 31 fd 57 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 00 0e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL1W!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\endpointdlp.dll	0	25986	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 77 fd 60 16 5a fd 16 5a fd 16 5a fd 6e 1b fd 16 5a fd 16 1a fd 17 5a fd 6e 9b fd 16 5a fd 6e 1b 71 16 5a fd 6e 28 fd fd 16 5a fd 6e 5b fd 16 5a fd 6e 5b 27 16 5a fd 6e 5b fd 16 5a fd 6e 2a fd fd 16 5a fd 6e db fd 16 5a 52 69 63 68 fd 16 5a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 51 fd fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$wnnnqn(nn'nn*nRichPELQ	success or wait	17	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe	0	6258	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 01 66 fd 67 60 08 fd 67 60 08 fd 67 60 08 fd 6e 18 fd fd 51 60 08 fd 2c 18 0c fd 46 60 08 fd 2c 18 0b fd 68 60 08 fd 2c 18 0d fd fd 60 08 fd 2c 18 09 fd 7a 60 08 fd 67 60 09 fd fd 61 08 fd 2c 18 01 fd 08 60 08 fd 2c 18 fd fd 66 60 08 fd 2c 18 0a fd 66 60 08 fd 52 69 63 68 67 60 08 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 0c 7e 0e 75 00 00 00	MZ@!L!This program cannot be run in DOS mode.$#fg`g`g`nQ`,F`,h`,`,z`g`a,`,f`,f`Richg`PEd~u	success or wait	16	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe	0	29538	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 63 12 fd 30 12 fd 30 12 fd 30 fd fd 31 d2 fd 30 fd fd 31 92 fd 30 fd fd 36 30 92 fd 30 fd fd 31 a5 30 fd fd 31 d2 fd 30 12 fd 30 fd fd fd 30 fd fd 31 16 fd fd 30 fd 54 fd 30 92 fd 30 fd fd 5a 30 52 fd 30 fd fd 31 52 fd 30 52 69 63 68 12 fd 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$c000101060010100010T00Z0010Rich0PEd	success or wait	31	7FF700EBB2C6	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe</td><td>0</td><td>19578</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 96 fd 40 fd fd fd 13 fd fd fd 13 fd fd fd 13 fd fd fd 12 fd fd fd 13 fd fd fd 12 fd fd fd 13 fd fd 4d 13 fd fd fd 13 fd fd fd 12 fd fd fd 13 fd fd fd 12 fd fd fd 13 fd fd fd 13 fd fd fd 13 fd fd fd 12 fd fd fd 13 fd fd 21 13 fd fd fd 13 fd fd fd 12 fd fd fd 13 52 69 63 68 fd fd fd 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06</td><td>MZ@!L!This program cannot be run in DOS mode.$@M!RichPEd</td><td>success or wait</td><td>6</td><td>7FF700EBB2C6</td><td>WriteFile</td></tr>
<tr><td>C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe</td><td>0</td><td>8554</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 39 fd 27 fd 7d fd 49 fd 7d fd 49 fd 7d fd 49 fd 36 fd 4d fd 73 fd 49 fd 36 fd 4a fd 75 fd 49 fd 74 fd fd fd 6d fd 49 fd 36 fd 4c fd 4f fd 49 fd 36 fd fd fd 7f fd 49 fd 36 fd 48 fd 6a fd 49 fd 7d fd 48 fd 52 fd 49 fd 36 fd 40 fd 4b fd 49 fd 36 fd fd fd 7c fd 49 fd 36 fd 4b fd 7c fd 49 fd 52 69 63 68 7d fd 49 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$9'}I}I}I6MsI6JuItmI6LOI6I6HjI}HRI6@KI6|I6K|IRich}I</td><td>success or wait</td><td>13</td><td>7FF700EBB2C6</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	0	12042	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 42 cf fd 23 fd fd fd 23 fd fd fd 23 fd fd 45 56 fd fd fd 23 fd fd 19 51 fd fd fd 23 fd fd 19 51 fd fd fd 23 fd fd 19 51 fd fd 18 23 fd fd 19 51 fd fd fd 23 fd fd fd 23 fd fd fd 22 fd fd 45 56 fd 67 23 fd fd 45 56 4e fd fd 23 fd fd 45 56 fd fd fd 23 fd fd 52 69 63 68 fd 23 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 a6 0e 50 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$B###EV#Q#Q#Q#Q ##"EV#EVN#EV#Rich#PEdP"	success or wait	26	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe	0	28066	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 52 a7 1d 16 fd fd 4e 16 fd fd 4e 16 fd fd 4e 5d fd fd 4f 1b fd fd 4e 5d fd fd 4f 1e fd fd 4e 1f fd 5a 4e 06 fd fd 4e 5d fd fd 4f 26 fd fd 4e 5d fd fd 4f 1b fd fd 4e 16 fd fd 4e 20 fd fd 4e 5d fd fd 4f 52 fd fd 4e 5d fd 36 4e 17 fd fd 4e 5d fd fd 4f 17 fd fd 4e 52 69 63 68 16 fd fd 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 5a 09 7b fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$RNNN]ON]ONZNN]O&N]ONNN]ORN]6NN]ONRichNPEdZ{	success or wait	5	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe	0	25594	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 54 fd fd fd 07 fd fd fd 07 fd fd fd 07 fd fd fd 06 fd fd fd 07 fd fd fd 06 fd fd fd 07 fd fd fd 06 fd fd fd 07 fd 5c 07 fd fd fd 07 fd fd fd 07 fd fd fd 07 fd fd fd 06 fd fd fd 07 fd fd 32 07 fd fd fd 07 fd 12 fd 07 fd fd fd 07 fd fd fd 06 41 fd fd 07 fd fd 30 07 fd fd fd 07 fd fd fd 06 fd fd fd 07 52 69 63 68 fd fd fd 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$T\2A0Rich	success or wait	96	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mpextms.exe	0	21706	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 68 fd 7e fd 09 fd 2d fd 09 fd 2d fd 09 fd 2d fd 71 fd 2c fd 09 fd 2d fd 71 fd 2c fd 09 fd 2d fd 71 fd 2c 7f 09 fd 2d fd 71 fd 2c fd 09 fd 2d fd 09 fd 2d fd 08 fd 2d fd 71 fd 2c fd 09 fd 2d fd 71 7d 2d fd 09 fd 2d fd 71 fd 2c fd 09 fd 2d 52 69 63 68 fd 09 fd 2d 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 16 7b fd 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 1e 00 50 0a	MZ@!L!This program cannot be run in DOS mode.$h~---q,-q,-q,-q,---q,-q}--q,-Rich-PEd{"P	success or wait	28	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCmdRun.exe	0	210	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 37 fd 14 7c 73 fd 7a 2f 73 fd 7a 2f 73 fd 7a 2f 38 fd 79 2e 62 fd 7a 2f 7a fd fd 2f 65 fd 7a 2f 38 fd 7f 2e 40 fd 7a 2f 38 fd 7b 2e 60 fd 7a 2f 73 fd 7b 2f 20 fd 7a 2f 38 fd 73 2e fd fd 7a 2f 54 0e 04 2f 71 fd 7a 2f 38 fd 7e 2e 64 fd 7a 2f 38 fd	MZ@!L!This program cannot be run in DOS mode.$7|sz/sz/sz/8y.bz/z/ez/8.@z/8{.`z/s{/z/8s.z/T/qz/8~.dz/8	success or wait	25	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCopyAccelerator.exe	0	18682	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 75 0b fd fd 1b 58 fd fd 1b 58 fd fd 1b 58 fd fd 18 59 fd fd 1b 58 fd 48 58 fd fd 1b 58 fd fd 1e 59 fd fd 1b 58 fd fd 1a 59 fd fd 1b 58 fd fd 1a 58 fd fd 1b 58 fd fd 12 59 fd 1b 58 fd fd 1f 59 fd fd 1b 58 fd fd fd 58 fd fd 1b 58 fd fd 19 59 fd fd 1b 58 52 69 63 68 fd fd 1b 58 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 3e 25 fd 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$uXXXYXXXYXYX XX YXYXXXYXRichXPEL>%	success or wait	5	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json	0	350	7b 0d 0a 20 20 22 6e 61 6d 65 22 3a 20 22 63 6f 6d 2e 6d 69 63 72 6f 73 6f 66 74 2e 64 65 66 65 6e 64 65 72 2e 62 72 6f 77 73 65 72 5f 65 78 74 65 6e 73 69 6f 6e 2e 6e 61 74 69 76 65 5f 6d 65 73 73 61 67 65 5f 68 6f 73 74 22 2c 0d 0a 20 20 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 20 22 4e 61 74 69 76 65 20 68 6f 73 74 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 42 72 6f 77 73 65 72 20 45 78 74 65 6e 73 69 6f 6e 22 2c 0d 0a 20 20 22 70 61 74 68 22 3a 20 22 6d 70 65 78 74 6d 73 2e 65 78 65 22 2c 0d 0a 20 20 22 74 79 70 65 22 3a 20 22 73 74 64 69 6f 22 2c 0d 0a 20 20 22 61 6c 6c 6f 77 65 64 5f 6f 72 69 67 69 6e 73 22 3a 20 5b 0d 0a 20 20 20 20 22 63 68 72 6f 6d 65 2d 65 78 74 65 6e 73 69 6f 6e 3a 2f 2f 65 63 68 63 67 67 6c 64 6b	{ "name": "com.microsoft.defender.browser_extension.native_message_host", "description": "Native host for Microsoft Defender Browser Extension", "path": "mpextms.exe", "type": "stdio", "allowed_origins": ["chrome-extension://echcggldk	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man	0	12624	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity buildType="release" la	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man	0	5148	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity buildType="release" la	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man	0	3369	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity buildType="release" la	success or wait	1	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man	0	14126	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity buildType="release" la	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man	0	14248	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity buildType="release" la	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man	0	13701	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 3e 0d 0a 09 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 62 75 69 6c 64 54 79 70 65 3d 22 72 65 6c 65 61 73 65 22 20 6c 61 6e 67 75 61 67 65 3d 22 6e 65 75 74 72 61 6c 22 20 6e 61 6d 65 3d 22 57 69 6e 64 6f 77 73 2d 44 65 66 65 6e 64 65 72 2d 45 76 65 6e 74 73 22 20 70 72 6f 63 65 73	<?xml version="1.0" encoding="UTF-8"?> <assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema"> <assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Events" proces	success or wait	6	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof	0	28085	fd fd 23 00 70 00 72 00 61 00 67 00 6d 00 61 00 20 00 61 00 75 00 74 00 6f 00 72 00 65 00 63 00 6f 00 76 00 65 00 72 00 0d 00 0a 00 23 00 70 00 72 00 61 00 67 00 6d 00 61 00 20 00 6e 00 61 00 6d 00 65 00 73 00 70 00 61 00 63 00 65 00 28 00 22 00 5c 00 5c 00 5c 00 5c 00 2e 00 5c 00 5c 00 72 00 6f 00 6f 00 74 00 5c 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 5c 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 22 00 29 00 0d 00 0a 00 0d 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6e 00 63 00 65 00 20 00 6f 00 66 00 20 00 5f 00 5f 00 57 00 69 00 6e 00 33 00 32 00 50 00 72 00 6f 00 76 00 69 00 64 00 65 00 72 00 20 00 61 00 73 00 20 00 24 00 70 00 72 00 6f 00 76 00 0d 00 0a 00 7b 00 0d	#pragma autorecover#pragma namespace("\\\\.\\root\\Microsoft\\Windows\\Defender")Instance of __Win32Provider as $prov{	success or wait	4	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof	0	2664	fd fd 23 00 70 00 72 00 61 00 67 00 6d 00 61 00 20 00 6e 00 61 00 6d 00 65 00 73 00 70 00 61 00 63 00 65 00 20 00 28 00 20 00 22 00 5c 00 5c 00 5c 00 5c 00 2e 00 5c 00 5c 00 72 00 6f 00 6f 00 74 00 5c 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 5c 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 22 00 29 00 0d 00 0a 00 0d 00 0a 00 23 00 70 00 72 00 61 00 67 00 6d 00 61 00 20 00 64 00 65 00 6c 00 65 00 74 00 65 00 63 00 6c 00 61 00 73 00 73 00 28 00 22 00 4d 00 53 00 46 00 54 00 5f 00 4d 00 70 00 43 00 6f 00 6d 00 70 00 75 00 74 00 65 00 72 00 53 00 74 00 61 00 74 00 75 00 73 00 22 00 2c 00 6e 00 6f 00 66 00 61 00 69 00 6c 00 29 00 0d 00 0a 00 23 00 70 00 72 00 61 00 67 00 6d	#pragma namespace ("\\\\.\\root\\Microsoft\\Windows\\Defender")#pragma deleteclass("MSFT_MpComputerStatus",nofail)#pragm	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui	0	25783	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 6b 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELk*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui	0	24328	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 6c 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELl*Fb!8	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui	0	1703	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui	0	7071	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 6d 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 44 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQL SRichMSPELm*Fb!D	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui	0	12439	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 6f 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELo*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui	0	13191	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 71 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELq*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui	0	14463	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 73 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELs*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\MpAsDesc.dll.mui	0	15215	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui	0	13919	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 74 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELt*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	0	14159	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 75 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELu*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	0	15935	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 78 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELx*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	0	16183	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	0	11823	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 76 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELv*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui	0	12071	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 7a 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPELz*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpAsDesc.dll.mui	0	14359	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpEvMsg.dll.mui	0	15119	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui	0	26119	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 7d 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL}*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\mpuxagent.dll.mui	0	25855	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 7f 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpAsDesc.dll.mui	0	27631	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpEvMsg.dll.mui	0	27879	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\mpuxagent.dll.mui	0	5087	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!^	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpAsDesc.dll.mui	0	3799	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	4	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpEvMsg.dll.mui	0	30159	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\ProtectionManagement.dll.mui	0	7367	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\mpuxagent.dll.mui	0	15807	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!^	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpAsDesc.dll.mui	0	14519	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 06 01 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpEvMsg.dll.mui	0	2991	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\MpAsDesc.dll.mui	0	7335	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\mpuxagent.dll.mui	0	12183	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!N	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\mpuxagent.dll.mui	0	14991	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!N	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpAsDesc.dll.mui	0	17791	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpEvMsg.dll.mui	0	22639	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\ProtectionManagement.dll.mui	0	2415	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\mpuxagent.dll.mui	0	11375	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\MpAsDesc.dll.mui	0	11103	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\mpuxagent.dll.mui	0	7767	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpAsDesc.dll.mui	0	7495	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpEvMsg.dll.mui	0	3647	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\ProtectionManagement.dll.mui	0	9527	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\mpuxagent.dll.mui	0	17967	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\MpAsDesc.dll.mui	0	19239	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES\mpuxagent.dll.mui	0	23079	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR\mpuxagent.dll.mui	0	23839	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!N	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\mpuxagent.dll.mui	0	26647	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpAsDesc.dll.mui	0	26903	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpEvMsg.dll.mui	0	27663	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH\mpuxagent.dll.mui	0	5895	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!`	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\MpAsDesc.dll.mui	0	4087	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	4	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\mpuxagent.dll.mui	0	29431	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!^	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\mpuxagent.dll.mui	0	28135	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!^	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpAsDesc.dll.mui	0	26847	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpEvMsg.dll.mui	0	19415	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\ProtectionManagement.dll.mui	0	22735	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE\mpuxagent.dll.mui	0	30663	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB\mpuxagent.dll.mui	0	30911	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 64 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!d	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES\mpuxagent.dll.mui	0	28079	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN\mpuxagent.dll.mui	0	28839	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\MpAsDesc.dll.mui	0	29079	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\mpuxagent.dll.mui	0	7815	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!@	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN\mpuxagent.dll.mui	0	14207	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\mpuxagent.dll.mui	0	13935	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\MpAsDesc.dll.mui	0	15207	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\mpuxagent.dll.mui	0	14423	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpAsDesc.dll.mui	0	14671	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpEvMsg.dll.mui	0	11335	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\MpAsDesc.dll.mui	0	20279	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\mpuxagent.dll.mui	0	20527	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS\mpuxagent.dll.mui	0	21287	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!N	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\mpuxagent.dll.mui	0	24095	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpAsDesc.dll.mui	0	24343	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpEvMsg.dll.mui	0	21007	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\ProtectionManagement.dll.mui	0	28423	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\mpuxagent.dll.mui	0	4095	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!0	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpAsDesc.dll.mui	0	14583	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 7c 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!|	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpEvMsg.dll.mui	0	5615	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 7a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!z	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\ProtectionManagement.dll.mui	0	29927	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE\mpuxagent.dll.mui	0	6103	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ\mpuxagent.dll.mui	0	6855	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH\mpuxagent.dll.mui	0	7615	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN\mpuxagent.dll.mui	0	8879	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\mpuxagent.dll.mui	0	9119	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!0	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpAsDesc.dll.mui	0	19607	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 7a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!z	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpEvMsg.dll.mui	0	11151	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!p	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\ProtectionManagement.dll.mui	0	5247	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN\mpuxagent.dll.mui	0	14191	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU\mpuxagent.dll.mui	0	15463	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!\	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA\mpuxagent.dll.mui	0	14687	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!J	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\mpuxagent.dll.mui	0	18511	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\MpAsDesc.dll.mui	0	20295	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\mpuxagent.dll.mui	0	18999	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\MpAsDesc.dll.mui	0	21295	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ\mpuxagent.dll.mui	0	20519	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK\mpuxagent.dll.mui	0	21783	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN\mpuxagent.dll.mui	0	21519	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 62 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!b	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN\mpuxagent.dll.mui	0	19207	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY\mpuxagent.dll.mui	0	18935	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT\mpuxagent.dll.mui	0	19175	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\mpuxagent.dll.mui	0	18911	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpAsDesc.dll.mui	0	20695	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpEvMsg.dll.mui	0	21967	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP\mpuxagent.dll.mui	0	199	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\mpuxagent.dll.mui	0	32703	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpAsDesc.dll.mui	0	32439	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpEvMsg.dll.mui	0	28079	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO\mpuxagent.dll.mui	0	5279	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN\mpuxagent.dll.mui	0	7575	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!\	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN\mpuxagent.dll.mui	0	6799	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!\	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\mpuxagent.dll.mui	0	6023	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpAsDesc.dll.mui	0	6271	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpEvMsg.dll.mui	0	887	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\mpuxagent.dll.mui	0	6775	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!Z	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\mpuxagent.dll.mui	0	6511	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpAsDesc.dll.mui	0	7263	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpEvMsg.dll.mui	0	6487	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\ProtectionManagement.dll.mui	0	14415	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpAsDesc.dll.mui	0	23367	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpEvMsg.dll.mui	0	21055	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE\mpuxagent.dll.mui	0	28471	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\mpuxagent.dll.mui	0	29231	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!X	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\MpAsDesc.dll.mui	0	29479	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\mpuxagent.dll.mui	0	27167	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpAsDesc.dll.mui	0	27927	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpEvMsg.dll.mui	0	25103	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\ProtectionManagement.dll.mui	0	31999	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\mpuxagent.dll.mui	0	8175	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\MpAsDesc.dll.mui	0	9959	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\MpAsDesc.dll.mui	0	9183	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\mpuxagent.dll.mui	0	7383	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL\mpuxagent.dll.mui	0	8655	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA\mpuxagent.dll.mui	0	9927	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS\mpuxagent.dll.mui	0	11199	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\mpuxagent.dll.mui	0	11959	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!V	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\MpAsDesc.dll.mui	0	12719	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\mpuxagent.dll.mui	0	11943	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpAsDesc.dll.mui	0	14239	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpEvMsg.dll.mui	0	16023	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN\mpuxagent.dll.mui	0	28039	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!^	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN\mpuxagent.dll.mui	0	26743	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\mpuxagent.dll.mui	0	28015	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 48 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!H	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\MpAsDesc.dll.mui	0	32359	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\mpuxagent.dll.mui	0	4959	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!N	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpAsDesc.dll.mui	0	7767	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpEvMsg.dll.mui	0	8527	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU\mpuxagent.dll.mui	0	19527	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN\mpuxagent.dll.mui	0	21311	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\mpuxagent.dll.mui	0	23095	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\MpAsDesc.dll.mui	0	25391	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK\mpuxagent.dll.mui	0	23079	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 52 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!R	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\mpuxagent.dll.mui	0	24863	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!P	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\MpAsDesc.dll.mui	0	27151	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US\MpAsDesc.dll.mui	0	26375	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\mpuxagent.dll.mui	0	19208	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!$	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\mpuxagent.dll.mui	0	12039	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 46 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL*Fb!$	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpAsDesc.dll.mui	0	25607	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!T	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpEvMsg.dll.mui	0	26879	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!\	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\ProtectionManagement.dll.mui	0	26103	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpAsDesc.dll.mui	0	2799	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!V	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpEvMsg.dll.mui	0	3567	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!^	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\ProtectionManagement.dll.mui	0	2279	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 09 74 3d fd 4d 15 53 fd 4d 15 53 fd 4d 15 53 fd 06 6d fd fd 4c 15 53 fd 06 6d 51 fd 4c 15 53 fd 52 69 63 68 4d 15 53 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 1e 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ@!L!This program cannot be run in DOS mode.$t=MSMSMSmLSmQLSRichMSPEL!	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	0	11743	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a 20 20 3c 56 69 65 77 44 65 66 69 6e 69 74 69 6f 6e 73 3e 0d 0a 20 20 20 20 3c 56 69 65 77 3e 0d 0a 20 20 20 20 20 20 3c 4e 61 6d 65 3e 64 65 66 61 75 6c 74 3c 2f 4e 61 6d 65 3e 0d 0a 20 20 20 20 20 20 3c 56 69 65 77 53 65 6c 65 63 74 65 64 42 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 54 79 70 65 4e 61 6d 65 3e 4d 70 50 65 72 66 6f 72 6d 61 6e 63 65 52 65 70 6f 72 74 2e 52 65 73 75 6c 74 3c 2f 54 79 70 65 4e 61 6d 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 54 79 70 65 4e 61 6d 65 3e 44 65 73 65 72 69 61 6c 69 7a 65 64 2e 4d 70 50 65 72 66 6f 72 6d 61 6e 63 65 52 65 70 6f 72 74 2e 52 65 73 75 6c	<?xml version="1.0" encoding="utf-8"?> <Configuration> <ViewDefinitions> <View> <Name>default</Name> <ViewSelectedBy> <TypeName>MpPerformanceReport.Result</TypeName> <TypeName>Deserialized.MpPerformanceReport.Resul	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1	0	13667	40 7b 0d 0a 20 20 20 20 47 55 49 44 20 3d 20 27 43 34 36 42 45 33 44 43 2d 33 30 41 39 2d 34 35 32 46 2d 41 35 46 44 2d 34 42 46 39 43 41 38 37 41 38 35 34 27 0d 0a 20 20 20 20 41 75 74 68 6f 72 3d 22 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 22 0d 0a 20 20 20 20 43 6f 6d 70 61 6e 79 4e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 22 0d 0a 20 20 20 20 43 6f 70 79 72 69 67 68 74 3d 22 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 22 0d 0a 20 20 20 20 4d 6f 64 75 6c 65 56 65 72 73 69 6f 6e 20 3d 20 27 31 2e 30 27 0d 0a 20 20 20 20 4e 65 73 74 65 64 4d 6f 64 75 6c 65 73 20 3d 20 40	@{ GUID = '[C46BE3DC-30A9-452F-A5FD-4BF9CA87A854](#)' Author="Microsoft Corporation" CompanyName="Microsoft Corporation" Copyright="Copyright (C) Microsoft Corporation. All rights reserved." ModuleVersion = '1.0' NestedModules = @	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1	0	14315	40 7b 0d 0a 20 20 20 20 47 55 49 44 20 3d 20 27 41 35 31 45 36 44 39 45 2d 42 43 31 34 2d 34 31 41 37 2d 39 38 41 38 2d 38 38 38 31 39 35 36 34 31 32 35 30 27 0d 0a 20 20 20 20 41 75 74 68 6f 72 3d 22 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 22 0d 0a 20 20 20 20 43 6f 6d 70 61 6e 79 4e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 22 0d 0a 20 20 20 20 43 6f 70 79 72 69 67 68 74 3d 22 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 22 0d 0a 20 20 20 20 4d 6f 64 75 6c 65 56 65 72 73 69 6f 6e 20 3d 20 27 31 2e 30 27 0d 0a 20 20 20 20 4e 65 73 74 65 64 4d 6f 64 75 6c 65 73 20 3d 20 40	@{ GUID = '[A51E6D9E-BC14-41A7-98A8-888195641250](#)' Author="Microsoft Corporation" CompanyName="Microsoft Corporation" Copyright="Copyright (C) Microsoft Corporation. All rights reserved." ModuleVersion = '1.0' NestedModules = @	success or wait	1	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1	0	16951	23 23 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a 3c 23 0d 0a 2e 53 59 4e 4f 50 53 49 53 0d 0a 54 68 69 73 20 63 6d 64 6c 65 74 20 63 6f 6c 6c 65 63 74 73 20 61 20 70 65 72 66 6f 72 6d 61 6e 63 65 20 72 65 63 6f 72 64 69 6e 67 20 6f 66 20 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 41 6e 74 69 76 69 72 75 73 0d 0a 73 63 61 6e 73 2e 0d 0a 0d 0a 2e 44 45 53 43 52 49 50 54 49 4f 4e 0d 0a 54 68 69 73 20 63 6d 64 6c 65 74 20 63 6f 6c 6c 65 63 74 73 20 61 20 70 65 72 66 6f 72 6d 61 6e 63 65 20 72 65 63 6f 72 64 69 6e 67 20 6f 66 20 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 41 6e 74 69 76 69 72	## Copyright (c) Microsoft Corporation. All rights reserved. <#.SYNOPSISThis cmdlet collects a performance recording of Microsoft Defender Antivirusscans..DEscriptIONThis cmdlet collects a performance recording of Microsoft Defender Antivir	success or wait	2	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys	0	1784	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 2e 14 49 fd 4f 7a 1a fd 4f 7a 1a fd 4f 7a 1a fd 4f 7b 1a fd 4f 7a 1a fd 37 7b 1b fd 4f 7a 1a fd 37 7f 1b fd 4f 7a 1a fd 37 7e 1b fd 4f 7a 1a fd 37 79 1b fd 4f 7a 1a fd 37 72 1b fd 4f 7a 1a fd 37 fd 1a fd 4f 7a 1a fd 37 78 1b fd 4f 7a 1a 52 69 63 68 fd 4f 7a 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 0a 00 fd 49 fd 05 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$.IOzOzOzO{Oz7{Oz7Oz7~Oz7yOz7rOz7Oz7xOzRichOzPEdI"	success or wait	3	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys	0	17720	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 31 57 fd fd 5f 04 fd fd 5f 04 fd fd 5f 04 a5 5a 05 fd fd 5f 04 fd fd 5e 04 57 fd 5f 04 a5 5e 05 fd fd 5f 04 a5 5b 05 fd fd 5f 04 a5 5c 05 fd fd 5f 04 a5 57 05 fd fd 5f 04 a5 fd 04 fd fd 5f 04 a5 5d 05 fd fd 5f 04 52 69 63 68 fd fd 5f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 0a 00 fd fd fd 5b 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1W___Z_^W_^_[__W__]_Rich_PEd[	success or wait	6	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys	0	13360	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 60 5e fd fd 01 30 fd fd 01 30 fd fd 01 30 fd fd 01 31 fd fd 00 30 fd fd 79 31 fd fd 01 30 fd fd 79 35 fd fd 01 30 fd fd 79 34 fd fd 01 30 fd fd 79 33 fd fd 01 30 fd fd 79 38 fd fd 01 30 fd fd 79 d6 fd 01 30 fd fd 79 32 fd fd 01 30 fd 52 69 63 68 fd 01 30 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 fd 3d fd 75 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 1e 00 68 05	MZ@!L!This program cannot be run in DOS mode.$`^00010y10y50y40y30y80y0y20Rich0PEd=u"h	success or wait	15	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys	0	28448	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 34 fd fd fd 55 fd fd fd 55 fd fd fd 55 fd fd fd 2d fd fd fd 55 fd fd fd 55 fd fd fd 55 fd fd fd 2d fd fd fd 55 fd fd fd 2d fd fd fd 55 fd fd fd 2d fd fd fd 55 fd fd fd 2d fd fd fd 55 fd fd fd 2d 4a fd fd 55 fd fd fd 2d fd fd fd 55 fd fd 52 69 63 68 fd 55 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 0a 00 fd 3e fd fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$4UUU-UUU-U-U-U-U-JU-URichUPEd>	success or wait	3	7FF700EBB2C6	WriteFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt	0	3600	3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 0d 0a 31 2e 20 43 2b 2b 20 52 45 53 54 20 53 44 4b 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 4d 69 63 72 6f 73 6f 66 74 2f 63 70 70 72 65 73 74 73 64 6b 29 0d 0a 0d 0a 20 43 2b 2b 20 52 45 53 54 20 53 44 4b 20 0d 0a 0d 0a 54 68 65 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 28 4d 49 54 29 0d 0a 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 0d 0a 0d 0a 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a 50 65 72 6d 69 73 73	============================== ============================== =================== 1. C++ REST SDK (https://github.com/Microsoft/cpprestsdk) C++ REST SDK The MIT License (MIT)Copyright (c) Microsoft CorporationAll rights reserved.Permiss	success or wait	2	7FF700EBB2C6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp	0	4971	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 27 79 65 73 27 3f 3e 0a 0a 3c 57 69 6e 64 6f 77 73 50 65 72 66 6f 72 6d 61 6e 63 65 52 65 63 6f 72 64 65 72 20 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 41 75 74 68 6f 72 3d 22 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 66 6f 72 20 45 6e 64 70 6f 69 6e 74 22 20 54 65 61 6d 3d 22 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 66 6f 72 20 45 6e 64 70 6f 69 6e 74 22 20 43 6f 6d 6d 65 6e 74 73 3d 22 4d 69 63 72 6f 73 6f 66 74 20 44 65 66 65 6e 64 65 72 20 66 6f 72 20 45 6e 64 70 6f 69 6e 74 20 53 63 61 6e 20 70 65 72 66 6f 72 6d 61 6e 63 65 20 74 72 61 63 69 6e 67 22 20 43 6f 6d 70 61	<?xml version="1.0" encoding="utf-8" standalone='yes'?><WindowsPerformanceRecorder Version="1.0" Author="Microsoft Defender for Endpoint" Team="Microsoft Defender for Endpoint" Comments="Microsoft Defender for Endpoint Scan performance tracing" Compa	success or wait	1	7FF700EBB2C6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpComputerStatus.cdxml	unknown	15565	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPreference.cdxml	unknown	116938	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpRollback.cdxml	unknown	16417	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpScan.cdxml	unknown	16893	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpSignature.cdxml	unknown	16877	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreat.cdxml	unknown	16503	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatCatalog.cdxml	unknown	16048	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpThreatDetection.cdxml	unknown	15997	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpWDOScan.cdxml	unknown	15776	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\DefenderCSP.dll	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAsDesc.dll	unknown	210184	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpAzSubmit.dll	unknown	262144	success or wait	6	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpClient.dll	unknown	262144	success or wait	5	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCommu.dll	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetours.dll	unknown	173312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDetoursCopyAccelerator.dll	unknown	103680	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpEvMsg.dll	unknown	144656	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpOAV.dll	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpRtp.dll	unknown	262144	success or wait	7	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSenseComm.dll	unknown	262144	success or wait	4	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSvc.dll	unknown	262144	success or wait	14	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUpdate.dll	unknown	156936	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpUxAgent.dll	unknown	262144	success or wait	3	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpLics.dll	unknown	21768	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.dll	unknown	262144	success or wait	3	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\endpointdlp.dll	unknown	262144	success or wait	3	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpAsDesc.dll	unknown	201992	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpClient.dll	unknown	262144	success or wait	4	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetours.dll	unknown	110864	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpDetoursCopyAccelerator.dll	unknown	63224	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpOAV.dll	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MsMpLics.dll	unknown	13560	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\endpointdlp.dll	unknown	262144	success or wait	3	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ConfigSecurityPolicy.exe	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCmdRun.exe	unknown	262144	success or wait	4	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpCopyAccelerator.exe	unknown	174864	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpDlpCmd.exe	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe	unknown	262144	success or wait	4	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MsMpEng.exe	unknown	133544	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\NisSrv.exe	unknown	262144	success or wait	12	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mpextms.exe	unknown	262144	success or wait	4	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCmdRun.exe	unknown	262144	success or wait	3	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\MpCopyAccelerator.exe	unknown	131632	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\com.microsoft.defender.be.chrome.json	unknown	350	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-AMFilter.man	unknown	12624	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-NIS.man	unknown	6173	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Protection.man	unknown	3369	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-RTP.man	unknown	14126	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Antimalware-Service.man	unknown	33315	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Microsoft-Windows-Windows Defender.man	unknown	149456	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement.mof	unknown	97942	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ProtectionManagement_uninstall.mof	unknown	2664	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\af-ZA\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\am-ET\mpuxagent.dll.mui	unknown	24328	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\MpAsDesc.dll.mui	unknown	60168	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ar-SA\mpuxagent.dll.mui	unknown	27400	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\as-IN\mpuxagent.dll.mui	unknown	32016	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\az-Latn-AZ\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\mpuxagent.dll.mui	unknown	32016	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bg-BG\MpAsDesc.dll.mui	unknown	66832	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bn-IN\mpuxagent.dll.mui	unknown	32528	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\bs-Latn-BA\mpuxagent.dll.mui	unknown	30992	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES-valencia\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\MpAsDesc.dll.mui	unknown	69896	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ca-ES\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\mpuxagent.dll.mui	unknown	30480	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpAsDesc.dll.mui	unknown	64776	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cs-CZ\MpEvMsg.dll.mui	unknown	54536	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\cy-GB\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\mpuxagent.dll.mui	unknown	30992	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpAsDesc.dll.mui	unknown	65288	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\da-DK\MpEvMsg.dll.mui	unknown	55560	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\mpuxagent.dll.mui	unknown	34056	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpAsDesc.dll.mui	unknown	71944	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\MpEvMsg.dll.mui	unknown	55560	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\de-DE\ProtectionManagement.dll.mui	unknown	57096	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\mpuxagent.dll.mui	unknown	34056	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpAsDesc.dll.mui	unknown	77064	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\el-GR\MpEvMsg.dll.mui	unknown	61192	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\MpAsDesc.dll.mui	unknown	60688	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-GB\mpuxagent.dll.mui	unknown	29960	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\mpuxagent.dll.mui	unknown	29968	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpAsDesc.dll.mui	unknown	60688	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\MpEvMsg.dll.mui	unknown	52992	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\en-US\ProtectionManagement.dll.mui	unknown	56576	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\mpuxagent.dll.mui	unknown	33040	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\MpAsDesc.dll.mui	unknown	68872	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-MX\mpuxagent.dll.mui	unknown	33040	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpAsDesc.dll.mui	unknown	69384	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\MpEvMsg.dll.mui	unknown	59656	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\es-ES\ProtectionManagement.dll.mui	unknown	57096	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\et-EE\MpAsDesc.dll.mui	unknown	61696	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\eu-ES\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fa-IR\mpuxagent.dll.mui	unknown	29960	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\mpuxagent.dll.mui	unknown	32512	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpAsDesc.dll.mui	unknown	64776	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fi-FI\MpEvMsg.dll.mui	unknown	54536	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fil-PH\mpuxagent.dll.mui	unknown	34576	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\MpAsDesc.dll.mui	unknown	72960	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-CA\mpuxagent.dll.mui	unknown	34064	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\mpuxagent.dll.mui	unknown	34056	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpAsDesc.dll.mui	unknown	72968	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\MpEvMsg.dll.mui	unknown	62216	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\fr-FR\ProtectionManagement.dll.mui	unknown	57608	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ga-IE\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gd-GB\mpuxagent.dll.mui	unknown	35600	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gl-ES\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\gu-IN\mpuxagent.dll.mui	unknown	32528	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\MpAsDesc.dll.mui	unknown	54032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\he-IL\mpuxagent.dll.mui	unknown	26376	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hi-IN\mpuxagent.dll.mui	unknown	33040	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hr-HR\MpAsDesc.dll.mui	unknown	66320	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpAsDesc.dll.mui	unknown	68872	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\hu-HU\MpEvMsg.dll.mui	unknown	56592	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\MpAsDesc.dll.mui	unknown	65288	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\id-ID\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\is-IS\mpuxagent.dll.mui	unknown	29960	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpAsDesc.dll.mui	unknown	68872	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\MpEvMsg.dll.mui	unknown	58120	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\it-IT\ProtectionManagement.dll.mui	unknown	57096	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\mpuxagent.dll.mui	unknown	22280	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpAsDesc.dll.mui	unknown	41736	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\MpEvMsg.dll.mui	unknown	41224	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ja-JP\ProtectionManagement.dll.mui	unknown	56592	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ka-GE\mpuxagent.dll.mui	unknown	32016	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kk-KZ\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\km-KH\mpuxagent.dll.mui	unknown	31504	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kn-IN\mpuxagent.dll.mui	unknown	32528	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\mpuxagent.dll.mui	unknown	22280	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpAsDesc.dll.mui	unknown	41224	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\MpEvMsg.dll.mui	unknown	38672	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ko-KR\ProtectionManagement.dll.mui	unknown	56592	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\kok-IN\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lb-LU\mpuxagent.dll.mui	unknown	33544	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lo-LA\mpuxagent.dll.mui	unknown	28944	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lt-LT\MpAsDesc.dll.mui	unknown	66832	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\mpuxagent.dll.mui	unknown	30472	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\lv-LV\MpAsDesc.dll.mui	unknown	66312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mi-NZ\mpuxagent.dll.mui	unknown	31504	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mk-MK\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ml-IN\mpuxagent.dll.mui	unknown	35080	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mr-IN\mpuxagent.dll.mui	unknown	33040	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ms-MY\mpuxagent.dll.mui	unknown	32528	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\mt-MT\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpAsDesc.dll.mui	unknown	64264	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nb-NO\MpEvMsg.dll.mui	unknown	54536	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ne-NP\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpAsDesc.dll.mui	unknown	69896	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nl-NL\MpEvMsg.dll.mui	unknown	55568	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\nn-NO\mpuxagent.dll.mui	unknown	30472	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\or-IN\mpuxagent.dll.mui	unknown	33544	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pa-IN\mpuxagent.dll.mui	unknown	33544	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpAsDesc.dll.mui	unknown	70920	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pl-PL\MpEvMsg.dll.mui	unknown	59648	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\mpuxagent.dll.mui	unknown	33032	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\mpuxagent.dll.mui	unknown	32016	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpAsDesc.dll.mui	unknown	66312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\MpEvMsg.dll.mui	unknown	57608	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-BR\ProtectionManagement.dll.mui	unknown	56584	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpAsDesc.dll.mui	unknown	67848	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\pt-PT\MpEvMsg.dll.mui	unknown	58120	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\quz-PE\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\mpuxagent.dll.mui	unknown	32520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ro-RO\MpAsDesc.dll.mui	unknown	67848	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpAsDesc.dll.mui	unknown	68360	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\MpEvMsg.dll.mui	unknown	58640	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ru-RU\ProtectionManagement.dll.mui	unknown	56592	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sk-SK\MpAsDesc.dll.mui	unknown	66312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\MpAsDesc.dll.mui	unknown	67336	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sl-SI\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sq-AL\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-BA\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Cyrl-RS\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\mpuxagent.dll.mui	unknown	32008	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sr-Latn-RS\MpAsDesc.dll.mui	unknown	66312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\mpuxagent.dll.mui	unknown	30472	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpAsDesc.dll.mui	unknown	63752	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\sv-SE\MpEvMsg.dll.mui	unknown	53520	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ta-IN\mpuxagent.dll.mui	unknown	34064	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\te-IN\mpuxagent.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\mpuxagent.dll.mui	unknown	28424	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\th-TH\MpAsDesc.dll.mui	unknown	60168	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\mpuxagent.dll.mui	unknown	29960	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpAsDesc.dll.mui	unknown	64776	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tr-TR\MpEvMsg.dll.mui	unknown	54536	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\tt-RU\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ug-CN\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\mpuxagent.dll.mui	unknown	30472	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\uk-UA\MpAsDesc.dll.mui	unknown	67848	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ur-PK\mpuxagent.dll.mui	unknown	30984	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\mpuxagent.dll.mui	unknown	30480	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\vi-VN\MpAsDesc.dll.mui	unknown	66312	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\x86\en-US\MpAsDesc.dll.mui	unknown	60664	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\mpuxagent.dll.mui	unknown	19208	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\mpuxagent.dll.mui	unknown	19200	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpAsDesc.dll.mui	unknown	31496	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\MpEvMsg.dll.mui	unknown	33544	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-CN\ProtectionManagement.dll.mui	unknown	56072	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpAsDesc.dll.mui	unknown	32000	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\MpEvMsg.dll.mui	unknown	34056	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\zh-TW\ProtectionManagement.dll.mui	unknown	56072	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	unknown	63612	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\Defender.psd1	unknown	15169	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\DefenderPerformance.psd1	unknown	14315	success or wait	1	7FF700EBB365	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.psm1	unknown	47935	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdBoot.sys	unknown	49600	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdDevFlt.sys	unknown	168200	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdFilter.sys	unknown	262144	success or wait	2	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Drivers\WdNisDrv.sys	unknown	90384	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\ThirdPartyNotices.txt	unknown	6717	success or wait	1	7FF700EBB365	ReadFile
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\Powershell\MSFT_MpPerformanceRecording.wprp	unknown	4971	success or wait	1	7FF700EBB365	ReadFile

Analysis Process: MpSigStub.exe PID: **9000**, Parent PID: **2156**

General

Target ID:	19
Start time:	16:47:08
Start date:	26/05/2022
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\724B5320-FE6C-430F-AB77-13F2FD7207BA\MpSigStub.exe /stub 1.1.18500.10 /payload 4.18.2203.5 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-60574f34.exe
Imagebase:	0x7ff7d39b0000
File size:	803176 bytes
MD5 hash:	01F92DC7A766FF783AE7AF40FD0334FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6648**, Parent PID: **932**

General

Target ID:	20
Start time:	16:47:12
Start date:	26/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff655680000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WdNisDrv.sys PID: **4**, Parent PID: **-1**

General

Target ID:	21
Start time:	16:47:12
Start date:	26/05/2022
Path:	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\Drivers\WdNisDrv.sys
Wow64 process (32bit):	

Commandline:	
Imagebase:	
File size:	86264 bytes
MD5 hash:	B757AF9B44B0C0C75103210D9C7026FF
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: NisSrv.exe PID: **4264**, Parent PID: **932**

General	
Target ID:	22
Start time:	16:47:12
Start date:	26/05/2022
Path:	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\NisSrv.exe
Wow64 process (32bit):	false
Commandline:	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\NisSrv.exe
Imagebase:	0x7ff7ae2d0000
File size:	2772856 bytes
MD5 hash:	B7F144CC18AE552E1C3D42051A934902
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4912**, Parent PID: **932**

General	
Target ID:	23
Start time:	16:50:57
Start date:	26/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff655680000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **2928**, Parent PID: **932**

General	
Target ID:	29
Start time:	16:52:31
Start date:	26/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
Imagebase:	0x7ff655680000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly