ID: 1568
Sample Name: FACTURA.exe
Cookbook: default.jbs
Time: 11:00:42
Date: 08/10/2021
Version: 33.0.0 White Diamond

Table of Contents

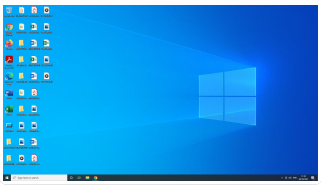
Windows Analysis Report FACTURA.exe

Overview

General Information

Sample Name:	FACTURA.exe
Analysis ID:	1568
MD5:	740463ed3266f7a.
SHA1:	a9310948476693..
SHA256:	fa9e12a03b90948.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

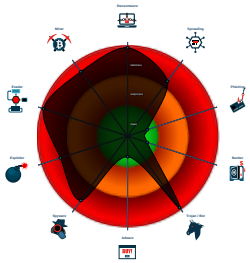
RemCom RemoteAdmin Mimikatz HawkEye Imminent Remcos AESCRYPT Ransomware Annabelle

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

Signatures

- Yara detected PasteDownloader
- Yara detected LaZagne password du…
- Yara detected Metasploit Payload
- Yara detected LazParking Ransomw…
- Yara detected Neshta
- Detected Hacktool Mimikatz
- Yara detected Discord Token Stealer
- Yara detected MailPassView
- Yara detected BlackMoon Ransomw…
- Yara detected Snake Keylogger
- Yara detected Parallax RAT
- Yara detected Zeppelin Ransomware

Classification



Process Tree

- **System is w10x64native**
- FACTURA.exe (PID: 7040 cmdline: 'C:\Users\user\Desktop\FACTURA.exe' MD5: 740463ED3266F7AEE8331978F50C731C)
  - WerFault.exe (PID: 8016 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 848 MD5: 40A149513D721F096DDF50C04DA2F01F)
  - WerFault.exe (PID: 2516 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 856 MD5: 40A149513D721F096DDF50C04DA2F01F)
- UserOOBEBroker.exe (PID: 2888 cmdline: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
- mpam-5e107659.exe (PID: 6940 cmdline: 'C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-5e107659.exe' /q WD MD5: 58454E5B478373BF68420AE5D49380D4)
  - MpSigStub.exe (PID: 5556 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe /stub 1.1.1 8500.10 /payload 1.351.16.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-5e107659.exe /q WD MD5: 01F92DC7A766FF783AE7AF40FD0334FB)
- wevtutil.exe (PID: 4104 cmdline: C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\3A24BB4C-F6EB-A1AC-C6CC-E780FED56A57.man MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 1412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- wevtutil.exe (PID: 6840 cmdline: C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\3A24BB4C-F6EB-A1AC-C6CC-E780FED56A57.man '/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' MD5: C57C1292650B6384903FE6408D412CFA)
  - conhost.exe (PID: 2644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- mpam-fad3e9a8.exe (PID: 1248 cmdline: C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-fad3e9a8.exe MD5: 34B7B3BDFA61E18D3B2C3B0AC92B78EF)
- **cleanup**

Malware Configuration

Threatname: Metasploit


```
{
  "Type": "Execute Command",
  "Command": "\u0001"
}
```


Threatname: CryLock


```
{
  "Extensions": "%d str_charcodeat DosDateTimeToFileTime() failed, err = %d str_tolowercase String.prototype.toLowerCase() is not a constructor const pea_calls_unimplemented_api  Intel(R) Core(TM)2 CPU         T7200  @ 2.00GHz(MSI Stream %d)(Ole Stream %d)0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz._SSF:ScanAllStreamselement.getElementsByTagName() called on non-DOM objectcryptoMpCommon(Message.%zu: %hs - %hs)(Message.%zu)No subject%lld"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000024.00000003.6293943264.00000197A31B6000.00000004.00000001.sdmp	JoeSecurity_Allatori_JAR_Obfuscator	Yara detected Allatori_JAR_Obfuscator	Joe Security	
00000024.00000003.6348926620.00000197A3621000.00000004.00000001.sdmp	Tofu_Backdoor	Detects Tofu Trojan	Cylance	• 0x2f5af:$a: Cookies: Sym1.0 • 0x2f550:$c: 66 0F FC C1 0F 11 40 D0 0F 10 40 D0 66 0F EF C2 0F 11 40 D0 0F 10 40 E0
00000024.00000003.6316460209.00000197A40AB000.00000004.00000001.sdmp	ZxShell_Jul17	Detects a ZxShell - CN threat group	Florian Roth	• 0xf57f:$x1: zxplug -add • 0xf58b:$x2: getxxx c:\xyz.dll
00000024.00000003.6345553259.00000197A36F1000.00000004.00000001.sdmp	JoeSecurity_Coinhive	Yara detected Coinhive miner	Joe Security	
00000024.00000003.6320871262.00000197A4180000.00000004.00000001.sdmp	webshell_php_by_string_obfuscation	PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming	Arnim Rupp	• 0xd5e:$opbs48: se'.(32*2) • 0x179f:$php_short: <? • 0x184cc:$php_short: <? • 0x179f:$php_new2: <?php
Click to see the 565 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
36.3.MpSigStub.exe.197a36f3b2a.205.unpack	MAL_Turla_Agent_BTZ	Detects Turla Agent.BTZ	Florian Roth	• 0x661b:$x5: mfc42l00.pdb • 0x65e8:$s3: %s\system32
36.3.MpSigStub.exe.197a36f3b2a.205.unpack	dump_tool	unknown	@patrickrolsen	• 0x4f2d:$s4: fgdump • 0x4f37:$s5: fgexec • 0x4f37:$s6: fgexecpipe
36.3.MpSigStub.exe.197a359b15e.156.raw.unpack	SUSP_Microsoft_7z_SFX_Combo	Detects a suspicious file that has a Microsoft copyright and is a 7z SFX	Florian Roth	• 0x15744:$s1: 7ZSfx%03x.cmd • 0x85d:$c1: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F ... • 0x144d:$c1: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F ... • 0x205d:$c1: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F ...
36.3.MpSigStub.exe.197a3f84db6.63.raw.unpack	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x16a3d:$s1: stratum+tcp://
36.3.MpSigStub.exe.197a3f84db6.63.raw.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Click to see the 445 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Pony

Antivirus detection for URL or domain

Found malware configuration

Yara detected Njrat

Yara detected Predator

Yara detected AveMaria stealer

Multi AV Scanner detection for domain / URL

Yara detected RevengeRAT

Location Tracking:

Yara detected Hancitor

Exploits:

Yara detected UACMe UAC Bypass tool

Privilege Escalation:

Detected Hacktool Mimikatz

Bitcoin Miner:

Yara detected Coinhive miner

Yara detected BitCoin Miner

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

Spreading:

Yara detected Neshta

Yara detected Autohotkey Downloader Generic

Networking:

Yara detected PasteDownloader

Yara detected Meterpreter

Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected LaZagne password dumper

Yara detected Linux EvilGnome RC5 key

Yara detected VBKeyloggerGeneric

Yara detected LimeRAT

E-Banking Fraud:

Yara detected Pony

Yara detected Njrat

Yara detected Predator

Yara detected AveMaria stealer

Yara detected RevengeRAT

Spam, unwanted Advertisements and Ransom Demands:

- Yara detected LazParking Ransomware
- Yara detected BlackMoon Ransomware
- Yara detected Zeppelin Ransomware
- Yara detected Ragnarok ransomware
- Yara detected Apis Ransomware
- Yara detected Wannacry ransomware
- Yara detected MegaCortex Ransomware
- Yara detected Cobra Locker ransomware
- Yara detected RekenSom ransomware
- Yara detected Avaddon Ransomware
- Yara detected Babuk Ransomware
- Yara detected Nemty Ransomware
- Yara detected BLACKMatter Ransomware
- Yara detected Clay Ransomware
- Yara detected Thanos ransomware
- Yara detected Jigsaw
- Yara detected CryLock ransomware
- Yara detected Sapphire Ransomware
- Yara detected OCT Ransomware
- Yara detected Snatch Ransomware
- Yara detected AESCRYPT Ransomware
- Yara detected RansomwareGeneric
- Yara detected Silvertor Ransomware
- Yara detected Ouroboros ransomware
- Yara detected Annabelle Ransomware
- Yara detected Gocoder ransomware
- Yara detected WannaRen ransomware
- Yara detected Chaos Ransomware
- Yara detected Mock Ransomware
- Yara detected Conti ransomware
- Yara detected NoCry Ransomware
- Yara detected ByteLocker Ransomware
- Yara detected RegretLocker Ransomware
- Yara detected Clop Ransomware
- Yara detected Ryuk ransomware
- Yara detected Porn Ransomware
- Yara detected LockBit ransomware
- Yara detected DarkSide Ransomware
- Yara detected LOCKFILE ransomware
- Yara detected Cerber ransomware
- Yara detected HiddenTear ransomware
- Yara detected Rhino ransomware
- Yara detected Mailto ransomware
- Yara detected CoronaCrypt Ransomware
- Yara detected Voidcrypt Ransomware
- Yara detected Buran Ransomware
- Yara detected GoGoogle ransomware
- Yara detected VHD ransomware
- Yara detected Axiom Ransomware
- Yara detected Artemon Ransomware
- Yara detected Netwalker ransomware
- Yara detected Jcrypt Ransomware

Yara detected Covid19 Ransomware
Yara detected Delta Ransomware
Yara detected LokiLocker Ransomware
Yara detected Cryptolocker ransomware
Yara detected Marvel Ransomware
Yara detected Cute Ransomware
Yara detected Xorist ransomware
Found potential ransomware demand text
Found string related to ransomware
May drop file containing decryption instructions (likely related to ransomware)
Deletes shadow drive data (may be related to ransomware)

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader
Yara detected MaliciousMacro
Yara detected Costura Assembly Loader
Yara detected AllatoriJARObfuscator
Yara detected MSILLoadEncryptedAssembly
Yara detected VB6 Downloader Generic
Yara detected BatToExe compiled binary
Binary or sample is protected by dotNetProtector

Persistence and Installation Behavior:

Yara detected Neshta
Sample is not signed and drops a device driver

Boot Survival:

Yara detected Neshta
Yara detected LimeRAT

Hooking and other Techniques for Hiding and Protection:

May modify the system service descriptor table (often done to hook functions)
Contains functionality to hide user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3
Yara detected LimeRAT
Yara detected generic Shellcode Injector
Yara detected Windows Security Disabler
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected LimeRAT
May enable test signing (to load unsigned drivers)

Stealing of Sensitive Information:

- Yara detected LaZagne password dumper
- Yara detected Neshta
- Yara detected Discord Token Stealer
- Yara detected MailPassView
- Yara detected Snake Keylogger
- Yara detected Parallax RAT
- Yara detected Valak
- Yara detected Mini RAT
- Yara detected Koadic
- Yara detected Pony
- Yara detected Generic Dropper
- Yara detected Telegram RAT
- Yara detected Njrat
- Yara detected Vidar stealer
- Yara detected Predator
- Yara detected Mimikatz
- Yara detected AveMaria stealer
- Yara detected Nukesped
- Yara detected Codoso Ghost
- Yara detected Growtopia
- Yara detected Dorkbot
- Yara detected RevengeRAT
- Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality:

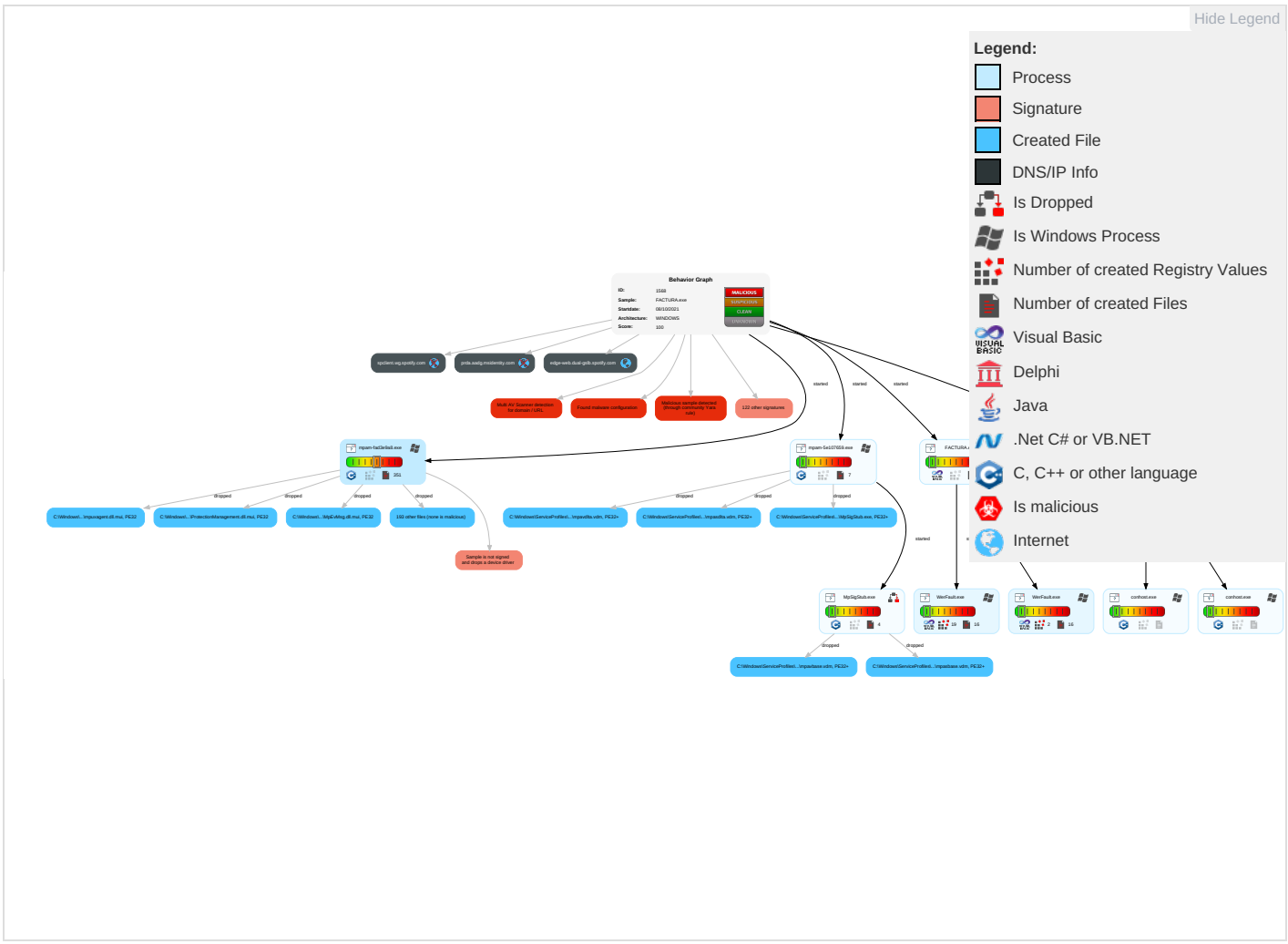
- Yara detected Metasploit Payload
- Yara detected Discord Token Stealer
- Yara detected Snake Keylogger
- Yara detected Parallax RAT
- Yara detected Valak
- Yara detected NetWire RAT
- Yara detected Linux EvilGnome RC5 key
- Yara detected Mini RAT
- Yara detected Koadic
- Yara detected Pony
- Detected Imminent RAT
- Yara detected Hancitor
- Yara detected Meterpreter
- Yara detected Telegram RAT
- Yara detected Njrat
- Yara detected Vidar stealer
- Yara detected Predator
- Detected HawkEye Rat
- Yara detected AveMaria stealer
- Yara detected Nukesped
- Detected Remcos RAT
- Yara detected Codoso Ghost
- Yara detected Growtopia
- Yara detected Dorkbot
- Yara detected RevengeRAT

Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Replication Through Removable Media 1	Command and Scripting Interpreter 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Desktop Protocol 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Remote Access Software 5	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Windows Service 1	Windows Service 1	Software Packing 1	Credential API Hooking 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Data from Local System 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2	Timestomp 1	Input Capture 2 1	File and Directory Discovery 1	SMB/Windows Admin Shares	Credential API Hooking 1	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Proxy 1	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 3	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Users 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

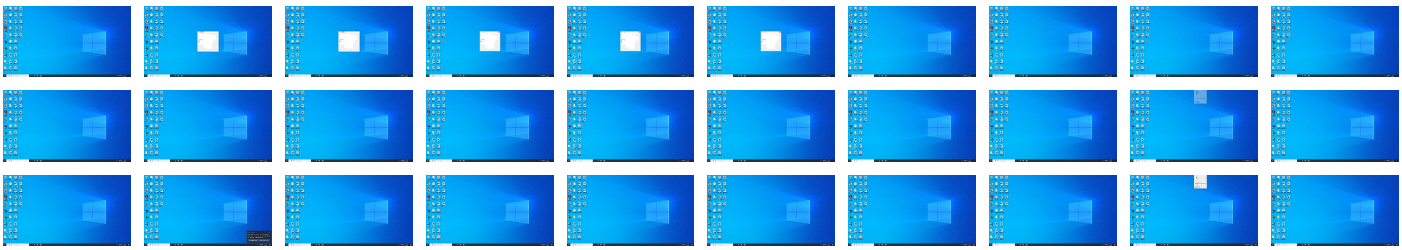
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdBoot.sys	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdDevFlt.sys	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdFilter.sys	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdNisDrv.sys	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpAzSubmit.dll	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpClient.dll	0%	ReversingLabs		
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCmdRun.exe	0%	Metadefender		Browse
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCmdRun.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
36.3.MpSigStub.exe.197a3f84db6.63.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a378e45a.139.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a4734ab6.49.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
36.3.MpSigStub.exe.197a4673aed.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a46aeebe.25.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a497a30f.132.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
36.3.MpSigStub.exe.197a31af2c4.73.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a45c0136.172.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a45c0136.47.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a46f017a.26.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a31aed77.165.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a46f017a.58.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a3f84db6.95.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a46aeebe.14.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a31aed77.74.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a357b147.154.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a31ae82a.75.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a31eb36e.135.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a45c0136.31.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a32a3acd.179.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a3f84db6.208.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.3.MpSigStub.exe.197a31ae82a.166.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a3578ac5.153.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.3.MpSigStub.exe.197a31af2c4.167.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kiranacorp.com/oja	1%	Virustotal		Browse
http://kiranacorp.com/oja	0%	Avira URL Cloud	safe	
http://www.bonusesfound.ml/update/index.php	13%	Virustotal		Browse
http://www.bonusesfound.ml/update/index.php	0%	Avira URL Cloud	safe	
http://www.cooctdlfast.com/download.php?	3%	Virustotal		Browse
http://www.cooctdlfast.com/download.php?	0%	Avira URL Cloud	safe	
http://110.42.4.180:	13%	Virustotal		Browse
http://110.42.4.180:	0%	Avira URL Cloud	safe	
http://stmichaelolivewood.com/templates/landofchrist/css/msg.jpg	0%	Avira URL Cloud	safe	
http://minetopsforums.ru/new_link3.php?site=	0%	Avira URL Cloud	safe	
http://today-friday.cn/maran/sejvan/get.php	0%	Avira URL Cloud	safe	
http://ati.vn	0%	Avira URL Cloud	safe	
http://errors.statsmyapp.comxa	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://185.172.110.217/robx/remit.jpg	0%	Avira URL Cloud	safe	
http://https://anonfiles.com/	0%	Avira URL Cloud	safe	
http://www.whitehouseknutsford.co.uk/invoice-status/please-pull-invoice-684594/	0%	Avira URL Cloud	safe	
http://https://sumnermail.org/sumnerscools/school.php	0%	Avira URL Cloud	safe	
http://139.162.	0%	Avira URL Cloud	safe	
http://rghost.net/download/	0%	Avira URL Cloud	safe	
http://127.0.0.1:8000/web.html?url=yac.mx&rate=501&id=%s&key=%s&pm=1x	0%	Avira URL Cloud	safe	
http://install.outbrowse.com/logTrack.php?x	0%	Avira URL Cloud	safe	
http://usa-national.info/gpu/band/grumble.dot	0%	Avira URL Cloud	safe	
http://https://jovial-pasteur.159-89-118-202.plesk.page/wp-content/uploads/index.php	0%	Avira URL Cloud	safe	
http://canonicalizer.ucsuri.tcs/3	0%	Avira URL Cloud	safe	
http://sesame96.orange.ero0101.com/set_inf.php?id=ero257.wmv&sid=	0%	Avira URL Cloud	safe	
http://mexicorxonline.com/glad/imagenes.html?disc=abuse&code=7867213	0%	Avira URL Cloud	safe	
http://spywaresoftstop.com/load.php?adv=141	0%	Avira URL Cloud	safe	
http://https://sotheraho.com/wp-content/fonts/reportexcelnew.php	0%	Avira URL Cloud	safe	
http://walden.co.jp/wp/divorce/divorce.php?id=zxjpyy5tb3jyaxnvb	0%	Avira URL Cloud	safe	
http://eduardovolpi.com.br/flipbook/postal/services/parcel)	0%	Avira URL Cloud	safe	
http://https://sweetsizing.com/vip/	0%	Avira URL Cloud	safe	
http://5.149.248.85/flashupdate.exe	0%	Avira URL Cloud	safe	
http://security-updater.com/binaries/	0%	Avira URL Cloud	safe	
http://www.fbcom.review/d/9.doc	0%	Avira URL Cloud	safe	
http://5starvideos.com/main/K5	0%	Avira URL Cloud	safe	
http://aklick.info/d.php?date=	0%	Avira URL Cloud	safe	
http://77.81.225.138/carnaval2017.zip	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.slotch.com/ist/softwares/v4.0/istdownload.exe	0%	Avira URL Cloud	safe	
http://https://go.wikitextbooks.info	0%	Avira URL Cloud	safe	
http://https://bemojo.com/ds/161120.gif	0%	Avira URL Cloud	safe	
http://esiglass.it/glassclass/glass.php	0%	Avira URL Cloud	safe	
http://https://xmrig.com/wizard	0%	Avira URL Cloud	safe	
http://https://rotf.lol/3u6d9443	0%	Avira URL Cloud	safe	
http://https://kiwisanagustin.com/wp-admin/includes/opo.php%22%20method%3d%22post%22%20style%3d%22box-sizin	0%	Avira URL Cloud	safe	
http://m.mworld.vn/MWorld30/data20.xm?a=getip&g=3&sex=Android	0%	Avira URL Cloud	safe	
http://www.niepicowane.pl/	0%	Avira URL Cloud	safe	
http://office-service-secs.com/blm.task	0%	Avira URL Cloud	safe	
http://https://irecruiter.immentia.com/storage/framework/cache/data/0e/nC7vWe43YwJjj.php	0%	Avira URL Cloud	safe	
http://js.f4321y.com/	0%	Avira URL Cloud	safe	
http://www.searchmaid.com/	0%	Avira URL Cloud	safe	
http://tbapi.search.ask.comxb	0%	Avira URL Cloud	safe	
http://www.mva.by/tags/ariscanin1.e	0%	Avira URL Cloud	safe	
http://masgiO.info/cd/cd.php?id=%s&ver=g	0%	Avira URL Cloud	safe	
http://sds.clrsch.com/x	0%	Avira URL Cloud	safe	
http://https://blackstonesbarandgrill.net/wp-includes/js/service/jp/login.php	100%	Avira URL Cloud	phishing	
http://boscumix.com/optima/index.php	0%	Avira URL Cloud	safe	
http://playsong.mediasongplayer.com/	0%	Avira URL Cloud	safe	
http://207.154.225.82/report.json?type=mail&u=$muser&c=	0%	Avira URL Cloud	safe	
http://www.xiuzhe.com/ddvan.exe	0%	Avira URL Cloud	safe	
http://t.zer9g.com/	0%	Avira URL Cloud	safe	
http://149.3.170.235/qw-fad/	0%	Avira URL Cloud	safe	
http://maringareservas.com.br/queda/index.php	0%	Avira URL Cloud	safe	
http://shdjhgftyhgjklolkjio.dns.navy/bcz/document.doc	100%	Avira URL Cloud	malware	
http://seunelson.com.br/js/content.xml	0%	Avira URL Cloud	safe	
http://costacars.es/ico/ortodox.php	100%	Avira URL Cloud	malware	
http://82.98.235.	0%	Avira URL Cloud	safe	
http://verred.net/?1309921	0%	Avira URL Cloud	safe	
http://https://pigeonious.com/img/	0%	Avira URL Cloud	safe	
http://data1.yoou8.com/	0%	Avira URL Cloud	safe	
http://https://jabaltoor.com/copy/img/blog/cat-post/r7gnor1h0.php	0%	Avira URL Cloud	safe	
http://handjobheats.com/xgi-bin/q.php	0%	Avira URL Cloud	safe	
http://www.pcpurifier.com/buynow/?	0%	Avira URL Cloud	safe	
http://www.chatzum.com/statistics/?affid=$RPT_AFFID&cztbid=$RPT_UID&inst=$RTP_SETINST&sethp=$RTP_SET	0%	Avira URL Cloud	safe	
http://https://longurl.in/tllwu	0%	Avira URL Cloud	safe	
http://%63%61%39%78%2e%63%6f%6d/ken.gif	0%	Avira URL Cloud	safe	
http://https://cdn4.buysellads.net/pub/tempmail.js?	0%	Avira URL Cloud	safe	
http://www.mybrowserbar.com/cgi/coupons.cgi/	0%	Avira URL Cloud	safe	
http://200.159.128.	0%	Avira URL Cloud	safe	
http://psynergi.dk/data	0%	Avira URL Cloud	safe	
http://mndyprivatecloudshareandfileprotecthmvb.freeddns.org/receipt/invoice_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
edge-web.dual-gslb.spotify.com	35.186.224.25	true	false		high
spclient.wg.spotify.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1568
Start date:	08.10.2021
Start time:	11:00:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 20m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FACTURA.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	46
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.spre.troj.spyw.expl.evad.mine.winEXE@13/235@1/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:02:51	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
edge-web.dual-gslb.spotify.com	bpSrG4K6tH.msi	Get hash	malicious	Browse	• 35.186.224.25
	Proforma invoice Shipping documents.exe	Get hash	malicious	Browse	• 35.186.224.25
	#U017dIADA#U0164 O PONUKU 07-10-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 35.186.224.25
	Zahteva za ponudbo 07-10-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 35.186.224.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Zapytanie ofertowe 189245.exe	Get hash	malicious	Browse	• 35.186.224.25
	Monex Payment Declined CTE21081157582 EUR 81300.00 _PDF.exe	Get hash	malicious	Browse	• 35.186.224.25
	FACTURA.exe	Get hash	malicious	Browse	• 35.186.224.25
	Swift Copy.exe	Get hash	malicious	Browse	• 35.186.224.25
	Justificante de la transfer.exe	Get hash	malicious	Browse	• 35.186.224.25
	Sipari#U015f-05.10..2021.exe	Get hash	malicious	Browse	• 35.186.224.25
	justificante de la transfer.exe	Get hash	malicious	Browse	• 35.186.224.25
	udI2NcR8Lj.exe	Get hash	malicious	Browse	• 35.186.224.25
	bthGMpTA2L.exe	Get hash	malicious	Browse	• 35.186.224.25
	MT103_SWIFT.exe	Get hash	malicious	Browse	• 35.186.224.25
	CpUNO6WMEm.exe	Get hash	malicious	Browse	• 35.186.224.25
	EVLb7JeDaK.dll	Get hash	malicious	Browse	• 35.186.224.25
	Struggleres5.exe	Get hash	malicious	Browse	• 35.186.224.25
	Zapytanie ofertowe (SHELMO Sp. z o.o. 09272021).exe	Get hash	malicious	Browse	• 35.186.224.25
	Pago de factura.exe	Get hash	malicious	Browse	• 35.186.224.25
	payment confirmation.exe	Get hash	malicious	Browse	• 35.186.224.25

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe	l8w9YB1n38.exe	Get hash	malicious	Browse	
	Monex Payment Declined CTE21081157582 EUR 81300.00 _PDF.exe	Get hash	malicious	Browse	
	Udtrt.exe	Get hash	malicious	Browse	
	MT103_SWIFT.exe	Get hash	malicious	Browse	
	MT103_SWIFT.exe	Get hash	malicious	Browse	
	EVOLUTION TRADE Sp. z o.o. OFERTA 09212.exe	Get hash	malicious	Browse	
	tZz20galQf.exe	Get hash	malicious	Browse	
	Guloader.exe	Get hash	malicious	Browse	
	8hIPR0n66X.dll	Get hash	malicious	Browse	
	Struggleres5.exe	Get hash	malicious	Browse	
	FACTURA.exe	Get hash	malicious	Browse	
	LISTA DE PEDIDO DE COMPRA.exe	Get hash	malicious	Browse	
	Unreal.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_FACTURA.exe_cb81e593c48dde2c87ceaa821c837590e0a7c7_bff3f8cd_d206a9ef-8028-44f6-92fb-9cf809282c0d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11732
Entropy (8bit):	3.79062410076042
Encrypted:	false
SSDEEP:	96:m9FAjVIs7l2ok7JAivXIxcQjc6qcElcw3T+HbHg/TVG4rmMoVazWLnNOyEHWmXEP:SajVIVm9uPsjEU1cDu76hfAIO81I
MD5:	8941668CAB60C0215D1EC389145BBDB7
SHA1:	4952BC92170DA42F9FA91C72FF46777F00CF523F
SHA-256:	4D6ED959A3D591CD4C36BEA42B70C547FC9E6EEEF11A9B2FF8B8844FAC34EDE4
SHA-512:	AFE8BC6B46E56862853D28BBE6B2D990ABDC63108B1974F0417CBE0DA9480B84410DD77319F87712890907809A72F8B06803D96CFAE114DBE87E2A249716053F
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_FACTURA.exe_cb81e593c48dde2c87ceaa821c837590e0a7c7_bff3f8cd_d206a9ef-8028-44f6-92fb-9cf809282c0d\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.1.6.0.9.6.5.6.5.1.2.5.3.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.8.1.6.0.9.6.8.4.4.7.4.7.3.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.2.0.6.a.9.e.f.-.8.0.2.8.-.4.4.f.6.-.9.2.f.b.-.9.c.f.8.0.9.2.8.2.c.0.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.9.e.b.4.e.6.9.-.4.5.4.8.-.4.7.6.3.-.9.8.4.7.-.8.b.b.f.a.f.f.8.5.e.3.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.F.A.C.T.U.R.A...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.o.u.n.t.e.r.f.o.i.l.7...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.8.0.-.0.0.0.1.-.0.0.1.1.-.4.b.8.d.-.5.6.9.d.2.b.b.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.7.9.4.a.e.3.6.d.f.0.9.7.b.e.6.3.8.a.5.2.f.8.b.d.4.a.4.a.8.4.f.0.0.0.0.0.9.0.4.!.0.0.0.0.a.9.3.1.0.9.4.8.4.7.6.6.9.3.d.7.2.b.e.9.3.7.f.2.3.e.1.b.5.3.b.3.6.0.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_FACTURA.exe_f1a70186ac6be91eea4c46237a7631b697b3fec_bff3f8cd_540f6c51-464c-4fd2-b6f3-af609fbfd780\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11644
Entropy (8bit):	3.7843540337003194
Encrypted:	false
SSDEEP:	96:4REdV3s7l2pf7ISZvXIxcQac6pcEccw3Q+HbHg/TVG4rmMoVazWLnNOyEHWmXECA:tV39m0tGNjEU1cDu76WfAIO8Is
MD5:	2AD23BDB55C1B87BD138CBAF872AC194
SHA1:	BB677F56DD5E6E5FA81257F25090AC56A9F120B6
SHA-256:	D25EFD7F048C650730597A81B5159FAEB87A77EF2C922E2A5C59C2F123F9BA65
SHA-512:	8A8BDE480844A4D91DF960404F5C13F682C988AE28015A5C04270BEBD051750731DDFD88381B1638D9F542EDFBB61C739F80C2CE84789E51C8994BA3B0192052
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.1.6.0.9.5.8.4.9.7.6.0.8.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.4.0.f.6.c.5.1.-.4.6.4.c.-.4.f.d.2.-.b.6.f.3.-.a.f.6.0.9.f.b.f.d.7.8.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.2.6.2.c.8.6.a.-.b.d.3.5.-.4.d.3.0.-.9.c.4.d.-.0.b.c.a.6.3.c.7.3.f.4.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.F.A.C.T.U.R.A...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.o.u.n.t.e.r.f.o.i.l.7...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.8.0.-.0.0.0.1.-.0.0.1.1.-.4.b.8.d.-.5.6.9.d.2.b.b.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.7.9.4.a.e.3.6.d.f.0.9.7.b.e.6.3.8.a.5.2.f.8.b.d.4.a.4.a.8.4.f.0.0.0.0.0.9.0.4.!.0.0.0.0.a.9.3.1.0.9.4.8.4.7.6.6.9.3.d.7.2.b.e.9.3.7.f.2.3.e.1.b.5.3.b.3.6.0.7.b.f.9.2.f.!.F.A.C.T.U.R.A...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.1.1././.1.0././.0.9.:.2.3.:.1.8.:.3.6.!.2.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB13.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Oct 8 10:02:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	50612
Entropy (8bit):	2.0716034299451516
Encrypted:	false
SSDEEP:	192:hVG8v9IdWYZ9ZrQfEUbtuWhJTz4y0lnEXQys7HoHEsM:nzvqZrtmTOnEQoHnM
MD5:	23CEFD70E33DC0D6BDC88ED2F3987B40
SHA1:	69FE452C943862189F1FA790D061C3E3CFCCE1BC
SHA-256:	A6C0B0022B40227C0C5EDCAA2E2336C223BD5F53A36FE758792E6B263EAE0B2A
SHA-512:	A60CD3D95AA8A48B34E855FA2A19DA6BAB42C639520F4F0C1336169041608284195C819F37FE9E3AEBF89AD9607DB6B185C6552BB806800D5A3007E5F43CB600
Malicious:	false
Preview:	MDMP..a..... .....?.`a.....bJ.....GenuineIntel.....T.....:.`a.....0..2.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.9.0.4.1...5.4.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE8F.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8354
Entropy (8bit):	3.6953427483028567
Encrypted:	false
SSDEEP:	192:R9l7lZNiMtX6b6YwDTSUnMDgmfjapvApNW89b9Rh1fa/Bm:R9lnNiMt6b6YoSUnMDgmfjaps9RjfU8
MD5:	E3B35980F5666F714315C3B06351E314
SHA1:	C107494DB837F74F5811B46FC6EFE99AEC9697A0
SHA-256:	0A4B88C1D3A1AB5B29F2A025ACD1168C7A0D2AA7FACF4D68F5809C6203AD4D78
SHA-512:	12C4926A84FCFD9FA0420AAD3E884FC2BB7AD4E8D1919A1638354F7D4EA92A2180671EF6BBA1DD5F22D668B5E996838B8D4A7816EA89ACB595C515DFF5E93D1
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE8F.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.4.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF5B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4879
Entropy (8bit):	4.494495658736333
Encrypted:	false
SSDEEP:	48:cvIwwtl8zsPe702l7VFJ5WS2Cfjkvms3rm8M4JPDePF9b+q8veDeAQPuBZBd:uILfm7GySPfi5J8KsQPYZBd
MD5:	F9DD9D728E59554057CF0644DD151A4A
SHA1:	E3A98FEDE993EDFC3A0C8140F4934D06263BDFF6
SHA-256:	2BCF71826FA54E3C640C02FEF82A5AEDE5EB0A175A6CE2BE0EF6801124F389A7
SHA-512:	F4E6B523EF71402A6E706F808A8B1356CCDEF66346E78B10D39A4371BF9786C21B7816A255614631E4B743B088BD95BCE6295816E2E931B045F3D70582F18526
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="221299964" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD708.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Oct 8 10:02:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1079572
Entropy (8bit):	1.6381935303241613
Encrypted:	false
SSDEEP:	1536:Y0rEEwgeqMnZHWLQ7DlFOaCtxPcy4zG0dI5OXGFdy+nMmNJw8psUl:QjXWM7Dl8aCtxkBG0drodHnVzpvl
MD5:	96C1BB43466C43560602BB3E8F2A34F4
SHA1:	1A935D79C6A0CD68165D889205052D274D27B28B
SHA-256:	249E26BAFBFC8A7F157A15E9A85E96FFCF44525ABD81371F2587C859DAF8491C
SHA-512:	6DF8B1642BEACAB1E36F077C1BD2BC23982199CDC4D9818241CF317BA4B09186E92B036C167AC4E19FB0F0807D834599DA42E7B45264362A072C0878AC314FB
Malicious:	false
Preview:	MDMP..a..... .....F.`a.....bJ.....GenuineIntel.....T.....:.`a.....0..2.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.9.0.4.1...5.4.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDDF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8338
Entropy (8bit):	3.7041735654765717
Encrypted:	false
SSDEEP:	192:R9l7lZNiMtL6ogk8e6YwDpSU0hpgmfkBXn/ApD489bC5lfbOA2m:R9lnNiMx626YiSUwpgmfkBoCrfbOY
MD5:	362D1A0185C1EFB98B7CF66D58B85025
SHA1:	0C10AF262A8FCFC508854639A09A1050D7FB99B9
SHA-256:	64A03DBD3174644EBCCAC1F6715DCF02B62A9C027EC0B150A0A3CD8A738D1CC0
SHA-512:	CDE45E5DE1AC8B862B972EB803AA19F203275CEDCBC3F5ADBF040821D200F7E575FA7B453B8D77B84B1A3173CCEB39AA95D352B56DFD1B8679E23797090CCB2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.4.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF09.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4824
Entropy (8bit):	4.540285559935987
Encrypted:	false
SSDEEP:	48:cvIwwtl8zsCe702I7VFJ5WS2CfjkRhs3rm8M4JPDKF1+q86s+QPuBZwd:uILfn7GySPfzJKvQPYZwd
MD5:	7B31EF70527F0A303502E0C8B2014B7D
SHA1:	A30F0D92A5E5E6098A8894C228B7DE849FEE0C75
SHA-256:	BE7377D3E30538337F060F7F2A26971B980737405EAC29B45B3D155C88F85776
SHA-512:	1CDCA71A053033B643BF5DE55E15A6F620E12760B9D6425A1FB5AD2ADDABD5AEB6184C3DAE4F49FCF2BB5BD4F73C43C1BC8C37A29CDBF6EA86ABEB579FF5 6322
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg n m="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="221299965" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11 .789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\1.1.18500.10_to_1.1.18600.4_mpengine.dll._p	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	data
Category:	dropped
Size (bytes):	2651471
Entropy (8bit):	**7.999536880042175**
Encrypted:	**true**
SSDEEP:	49152:/ATHbjm/iIcfAPkDFdv14M/XGgXqzwoDXK0wo2Ufj8BYuMmLNaCvruHEmWg:/gbHIvq/vlPGgap60PJ8TJaGrMOg
MD5:	1CD7E427BF1B88ED6CA3D330F89F41BA
SHA1:	F202BE4AD9A5C456B8454C40CECFCB4342E84983
SHA-256:	6AD6B43A7EDE4C123CA014EAE51C020C81D663E3145E1E7A1F912A40CAFEFB3B
SHA-512:	1E6FC265D3FF0AF6FF66BE5F837BB91EC5D1B340D9F790FAD2268F19BAA912C205E899F9E918E58945E5A57904AC7D0565AE720E8195C0FD3D78C380DBA9B64 2
Malicious:	false
Preview:	PA19....._a(|f..b...h ..cI....(j!.n.|...w.p...!..D..=....."".H..;%.P.#.Q.....Tm.Rth.(Za.%...Z.;...".....}...5/2-....{0Il....{..no...~o^w.....q....{...o...._.}qwz..l.;...&.z...{..n. [.n.....[oN.....6.MG.@n.O...$..m.K.a.....H.....(..!.P....._./@ $.1....Y.....6.....;Y..\.u...`W.G .d.e....XG+)$A.r$.....H..<....Jf.)..L 0r.mc..n(.K.e @n8.-.A.2Gw..,...lld.32..bs .6....Q.....cj..4.o....L.<21....&r@AlnLb...%.....9..tp.$'Q..r.S..o.9...e].....hr.W...,CAo/I.....~....z.H.....o.$.}.....f..f.....;.9.w.9...3..r.2.6.2*w.....]..T%..I..W.T R.2.47.Q!...,...ie..$.....,M.....Ah..2....P.. .....'y..S}.A.M.....2..U.u.}.A.Q..Km.q.\,..eUQ..0.[G.....]A.y:.-....p..5.c..^._.=a.I^s7..~.....S..\...;.$,8.e]9.].r9=a.:..~3 '...&.x.{.)....L.G5.9.0 ...Bk....2...5.#]...^iM.z@f.....f.n.....Z.{.[%-.}.S]W]..b..$...g}...nM..e....L.V..D+[.....?.~=.....6+..S..R...*...J..O.r.....rC....Vo..+.J>....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\1.349.0.0_to_1.351.0.0_mpasbase.vdm._p	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	data
Category:	dropped
Size (bytes):	6947288
Entropy (8bit):	**7.998652520745969**
Encrypted:	**true**
SSDEEP:	196608:Z6h8S1WVWjjc7Wf7zlW0qg2eUCJj6oZT32FBN6DIz:M+S1q7S7BWvMzJxBYHz
MD5:	46F037977005B7E9F8711C1CE7245C6B
SHA1:	B04BB6DE0F9F5A2B12C52124AD514D324EF3B616
SHA-256:	3D38C95836DB5540D4354BDA13A83091BF144A907A831604898D9F864126A4D0
SHA-512:	8D84FDCE9A81422A10AA1CC6B450EEA1E593F16DBF57D00A313C3AA9B03BB41F6A94FF8D4739C1ED79B3ED6F1CBF203F455BCCE6654C103BB5294599E47CD 16
Malicious:	false
Preview:	MPSP..j.....8..x..]u\.O._:D$$.E0.AEQQLJ.....T..y..n.DA.1PT.n1...nL...;..{.{..q.....&..|."S....J....W..TR..)W..[5J..!..&...e...=...Y.$mdz..R.V.".FQ.....iI.ljk.....!J.Sem...Q>.....+T.6 ..y..\W.u...*P../..=.2Mox...~..k.n...*.....V....O3U....wS%6.*...D.2)NC..q!..2.-J..h=~i.p...DF4.&#.x.....54.z.*\|.(W..Li..`2.R?.^W2.2.kfB.$d..3..(>..iJ...9.$..J..H.dB..*.LcmU.:.. U.....Ua...H.FS..yE...E;..`..P#..M.!.j..6....M..Z.....C...@.<..Kj..T.....mU...2.D.C.....PG.&.)9.M..AU.....LM;fm={..n....!J.SW74.....jS.h-..J9....I.%'.c.....t.*.(.....aQ..X..L.;.....k .i..>N.!.i..y.X.2..g...j.,=.>..7m..A....9@.....5.J.....Kw..0W..r2.)...h...(i>.&>A0...`D.c...).3.mL.....;.&..6.....)...E....)J..?K..%..;..D]..(S.yx.g.B]....D.....5..5...L.+Y.N..R3..z.s.....5H. .Y.....$../o.$....(.fx-/.";.no.M...vn...l..p.f.*.....X.;W..90..A...kH6^C.u..l...6.....:.P.....|.F.k.(..t.....3s..iT...;%.e.D..'m.e.r..YP.....^1,.....2O..,`.....IQ<K.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\1.349.0.0_to_1.351.0.0_mpavbase.vdm._p	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	data
Category:	dropped

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\1.349.0.0_to_1.351.0.0_mpavbase.vdm._p	
Size (bytes):	5295896
Entropy (8bit):	**7.997749364950445**
Encrypted:	**true**
SSDEEP:	98304:+3t2My1jJFqD1nlxml5zN8KGixmH8l2snrho+qico1hSWmnSEOR69MaKJD:+92M8DqTx/dN81iUHooKcofHDZEMaKJD
MD5:	F2E9F2343E044B331ECAF82302F5EC4B
SHA1:	049E866B3C7385DD7B00BBEC39453C30B8D29C28
SHA-256:	77AF289327742CC4F520092AA6429A5B829E24F40653DF71D00E31EFF9F3737F
SHA-512:	080509E98915BE390AE6A1ABA880248E98DE10D77AF107FB266DC34CECD43EED9CE77F53C6568C20FA1222DBA1D3FDB79E820656C0B28E1316DA93500C580A9
Malicious:	false
Preview:	MPSP..P..Au.[.Aex.l..xTW.6.I .....'..C\p.Dq.....<..!..Cp.BK..H.B..w.s2....}.{]o.s.....j.)m.e._....N.L.,...:.....!..g.UN.sH.t./...|6F.F.C.f....d..N./.2^.b*c..)..6...F![...BJ&.g\....%....f5.r.:...L..$..L6&.,.v=.Me..F...lF.Ou;.C....R..3.).....G...,.../..f.7U..o.2....VA..OV.7r.\|.....M?.....eS$K...w.ic.....y^S..&S.e.J..3..`2.y..4...iT.3..+mL(W'....L...&..&..1MI_J..|...f..eZ..dZ{&.i.n...e.s.X..).i..th...._M...f..mLgc...3..n.C....25.5=X]..8}.k.!YR..8{>...u...`H.c'.w.K.sxN.....z.0.....MN..m.lk.....&4..zY....?..O..@f..j.@...i ..}..jH..tf5ekb.....^...T.4...m.c[.ZY....YZ.l.T..u.....g1..~.eV. F....d.o....M<.5L7..AOl.+.....D`l...hO.'..X..;.x...=q....zS..c".J.....1D.s...(1T..`zc...q...Q.74..I.ug.(.0..g.D;1..Ty..3.....t.}.....a...`.D..I.`"1..L7.`....A.p.....g..M.....J.../.6..._..-e.i.h.z.J...ALw..[...3d...iLo.)..$.?Nk..,a...V*.++..v.-I.T~..M..'1}qj.,.....O.....X..3_.p...|z6.pm.....+.).,....^.j.h...d4..D..[,.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	803176
Entropy (8bit):	6.37118649960636
Encrypted:	false
SSDEEP:	24576:Ghj1QlBYDgtUUvie3n+pB3+ojRlcD1VyZTFXk:GhpQlBHtBYla1VyZpU
MD5:	01F92DC7A766FF783AE7AF40FD0334FB
SHA1:	45D7B8E98E22F939ED0083FE31204CAA9A72FA76
SHA-256:	FA42B9B84754E2E8368E8929FA045BE86DBD72678176EE75814D2A16D23E5C26
SHA-512:	BEA5F3D7FB0984C4A71720F25644CE3151FCDC95586E1E2FFE804D04567AAF30D8678608110E241C7DDF908F94882EDDD84A994573B0C808D1C064F0E135A583
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: l8w9YB1n38.exe, Detection: malicious, Browse • Filename: Monex Payment Declined CTE21081157582 EUR 81300.00_PDF.exe, Detection: malicious, Browse • Filename: Udtrt.exe, Detection: malicious, Browse • Filename: MT103_SWIFT.exe, Detection: malicious, Browse • Filename: MT103_SWIFT.exe, Detection: malicious, Browse • Filename: EVOLUTION TRADE Sp. z o.o. OFERTA 09212.exe, Detection: malicious, Browse • Filename: tZz20galQf.exe, Detection: malicious, Browse • Filename: Guloader.exe, Detection: malicious, Browse • Filename: 8hIPR0n66X.dll, Detection: malicious, Browse • Filename: Struggleres5.exe, Detection: malicious, Browse • Filename: FACTURA.exe, Detection: malicious, Browse • Filename: LISTA DE PEDIDO DE COMPRA.exe, Detection: malicious, Browse • Filename: Unreal.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..#...#..#..EV...#...Q...#...Q...#...Q...#...Q...#...#..."..EV..#..EV N..#..EV...#..Rich.#.....PE..d.....P....."......`.....@.....0.....-....`..... .....t..d..... .....D... ..h!... .....d...p..... (.....8.....0.....text...2R.....`..... ..`.rdata.....p... ...p.....@..@.data..../..... .....@....pdata...D.....P.....@..@.rsrc... ....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\mpasbase.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	53072304
Entropy (8bit):	**7.997563930648501**
Encrypted:	**true**
SSDEEP:	1572864:P0U1SslLDBQpTRKb0o76I0RUgRS2uc62zNWPy:P0UplL2tRW0aV0RpS2lTey
MD5:	0157CF1D00DB2F06270440CED26AD2DA
SHA1:	E0DA67E235AF6B8DDBA9736504E7638BFF4DB4B0
SHA-256:	15C43FFD2F73BA5E6A0E0A3B845A6FD61EE9E12220C0D98CBDB9E59D6E188914
SHA-512:	0264329D824734BC9BFE3129E4653E5293EFC96555EE98909DD19B37A010747C6368247784972AE478DBC16EF5E031FF99A283CF371F21278DBCE9E94DABAAC5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....<_a....." .....)..... .....)..... .....)...`..... .....)..... .....)..!.....rdata..p.....@..@.rsrc.....).. ....)..... .....@..@.....<_a.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ...)..rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\mpasdlta.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	56256
Entropy (8bit):	7.8865781490907585
Encrypted:	false
SSDEEP:	1536:JwR66b4yTEWjtF1x6Xuj/95BE9EzeTj3:J06y/PtTxAuZ5+W2
MD5:	D4A106B61C81FEEAD6CFB5C528812E1F
SHA1:	DFBFDED32E2BF05D407C9CB5B18FD8E8B3EE21DE
SHA-256:	3066FDA0371BAEBF09CF54502B77BB6CA9060966BD70C693D4A56DA01AB0F729
SHA-512:	AB8E503AC883CFEFB12178FBC8950655D371A92F533ADDE64CBE63EC2CF9DFAF843ACCBC33028C214704FA8F6B82DF0C78CB97C7EB20D68DF8806073F16E9(A3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d...]._a....."..... .....`.....!.....rdata..p.....@..@.r src..... .....@..@....]._a.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... .....rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\mpavbase.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	55848880
Entropy (8bit):	**7.995585481148423**
Encrypted:	**true**
SSDEEP:	1572864:iy6w1liQqicAsNBasl5IY/hOO0S7WGB9F9L4hxZB:B6uiQqiTE8kIYJn+wFZ4XB
MD5:	7E2B83A39CC26B2B617F404A89B6661C
SHA1:	198F9D59A90993247182EE11AE33AB52E5011C44
SHA-256:	8ED02ED1D817FA7B68466F11F55A2289D82BDD22A360246624BA0F9220D17EE3
SHA-512:	BF29A223DFF577DB8967DBEA610DC6DB2D6C0152A896E8BCC851EB67E84AF5367E4A01AC6110554C2813E974EBA9B8C04C2EB03422DCCDE00B1FA8D7F629C5F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....<_a.....".....T..... .....0T.....T...`.....@.T.....T..!.....rdata..p..... ....@..@.rsrc...@.T.. ....T.....@..@.....<_a.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ....T..rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\mpavdlta.vdm	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	modified
Size (bytes):	27072
Entropy (8bit):	7.694916420706485
Encrypted:	false
SSDEEP:	384:bW+dNWba5rbEmIxwjJPnLH5quZaC6HTY/0k2IYWmsntxQSElLlmF+gEQmDWlGs3R:7dPnZtjJPLZqucH5xIXnDQSi1zU
MD5:	F80B853B4DE2B156C4927CC201A1BD46
SHA1:	974333665EB814A71294FBE557DE6BDDBA39DA3C
SHA-256:	94E30E97B9D162D2CAF884F4796D704ED1A2E374A895A90429B4CE26CF3801A6
SHA-512:	E01DA9AAAEB50BA88814E7FB5A9F0A0B4BC25E3D856B2B2C0B93255C93B0EC0E62F6AFF4F157C7AF580DEF352F2AC9A094FC597475ED252FEBE9407EE2B7446E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d...]._a.....".....F..... .....p.....8....`.....C.....H...!.....rdata..p..... ....@..@.rsrc....C... ...D.....@..@....]._a.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01..... ...B...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ConfigSecurityPolicy.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	454904
Entropy (8bit):	6.2829164628823575
Encrypted:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ConfigSecurityPolicy.exe	
SSDEEP:	6144:p+BaOdQrqYpWVCPpYXe14f6eFL+TFFzE/tzkY5WwuTWOahE:kQ2YpWkPiXe14f6eFL6FA/zWwgChE
MD5:	065E4E5BE96865266D1FC4449274CE20
SHA1:	C6FF45B448F7B828D8C6369B5DE95B41E685F502
SHA-256:	98E3951BA9FACFB2B878D98D237D63C675878A09D9B6E18640C96746B6665041
SHA-512:	E63A5CF20678757F3FA277C56576F0DFBFF41DCBE61BEEFF28C608EE5D2BE2766E16A93E2FC423E6697670AC7E164E2B29EE5755AADAAE1C58B6F6F3FE1A6481
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._..._.._...^..._..x_..._K..^..._K..^..._K..^N.._K..^..._..._..._..._...^..._..._...^..._Rich..._.....PE..d.....m.....".....P.....u.....@.....]....`..... .....#...p...9..... ..... ...8f..p..... .....8...(.....8.....`...8.....text..... ..`.rdata...u.....@..@.data...PD... ...0... .....@....pdata...9...p...@...P.....@..@.rsrc....#.....0.....@..@.reloc.. .....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\DefenderCSP.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	303352
Entropy (8bit):	6.103843753653899
Encrypted:	false
SSDEEP:	6144:6CFCIAsyTqaF2uNoLQ7iF5K8+v5y8hCs2Y:6ypfyTqIL6LQ7iF5K8+484BY
MD5:	8C7A45FC0FDFB95104C84A68EAFBD170
SHA1:	D770064F1956FF05248E4C56DCF511928A7D8C3F
SHA-256:	B0A45EEB123840F105A40DB938553801C54DC5EED5FD2F710AC7EA24E16D0B56
SHA-512:	CD0B5A72D12B513B9EE160C1A18275893480488378A0E8E241600F0DCB1275B1F3CDC3C0096345D9A2B942C800484DC0E5210E0C4B409D5FE69B94716CE432F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q[.'5:}t5:}t5:}t.O\|u7:}t.O~u4:}t<B.t1:}t.H\|u,:}t5:\|tM;}t.Hyu(:}t.H~u;:}t .Hxu.:}t.O}u4:}t.Otuy:}t.O.t4:}t.O.u4:}tRich5:}t.....PE..d...c..P....." .....`A.....0...p.....p.... ...@..`$..... .....8.....p.....h@..(...0?..8.....@.....text...L..... ..`.rdata.....@..@.data....-..... .....@....pda ta..`$...@...0...0.....@..@.rsrc.....p.....`.....@..@.reloc..8.....p.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdBoot.sys	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	48520
Entropy (8bit):	6.2073261328907865
Encrypted:	false
SSDEEP:	768:0WfrO9dZBf9slBe+eRPKUjKHWPkKrdtBGgz:1ybZMrCKUjKulLBH
MD5:	1BF7CF2DBA97C71FF1876F0DE67421C3
SHA1:	48DFEC30B75138FCAF5DFFE16CB9822BA4CC4178
SHA-256:	B946398AB34EF5BF16DC3461D32261664760C0F86E8A281BCD90361A170E27FD
SHA-512:	11E1E1C339F9BFFC83919946ACFA6F3D5CC1C7494A21629332004E2445AAE919A0E014366DFDCE7764C934E1F7C2C0CABAAFF0179C8A145DBB0759BAE218F50
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....kM.W/,../,../,...,...^..*,...^..,,...^..=,...^..),...Y..$,...Y}..,...Y.....Ri ch/,.....PE..d...9....."....d...4.....`A.....q..<.....`....`.....!.....@....8..p.....@0..8..... .....p..`.....text..... ....h.rdata..0....0.....$.....@..H.data.....P.....8.....@....pdata.....`.....<.....@..H.idata.....p.....@..... ...@..HPAGE...../.....0...H..... ..`INIT.....x..... ..bGFIDS...$.....@..B.rsrc...`.....@..B.reloc.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdDevFlt.sys	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	164072
Entropy (8bit):	6.14800914066086
Encrypted:	false
SSDEEP:	3072:A1y1RnaePd+RhtbV0vgn8wNgaZp8kdiQfH4M4mD:3naePkRhtbV0vrwNgaZp8G7fYe
MD5:	26B890C2237E48DAF8B9B901EBE7A0C1
SHA1:	08976CF446255E9BB538B8540BBE0DD4BF3E8A65
SHA-256:	B1D793E12DBF2CE5197960454F0A5AE6C93703FA5BF2D7622EC0FDFBAC183211

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdDevFlt.sys	
SHA-512:	F580903A15E67888F714CA073D4B56C349131D2C03769092794656E538E0501CCAAC4B563311346B22AD8F81302FE2FBE22F4F6B1BD352BC4213EAED7F7F25D1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.i. ... ...#... .....'.....%.....!.....!...Rich ....PE..d...I:.....".....X.....A.....P....p.....`... .....p.....Pb..8..... .....text...*O.....P..... ..h.rdata...Y...`...\...T.....@..H.data.....@....pdata.....@..H.idata..... .....@. .HPAGE....!).....,..... ..`INIT.....)...0...,..... ..bGFIDS.....`.....@.....@..B.rsrc.....p.....D.....@..B.reloc.....L.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdFilter.sys	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	434424
Entropy (8bit):	6.350342003442293
Encrypted:	false
SSDEEP:	6144:EF/vuF3th9Gf4GYapoQm1RGpIk6IjKtGnpPVzcZYac3UA2dwcSogCYog:EYFdhQgGYNPR8lv1gpP+2oG
MD5:	B6C6FFC05B52D2F8A433DD12C3A11D30
SHA1:	F221740A99726722E5F5DF8CC3A0182436060A46
SHA-256:	666259E830F5EAC0707B2D957944B7468FA645271C60B8EA54E5130B8336D1F6
SHA-512:	1B0ABBB15A3018B584B0239C04A94E38FE433D382771BF8CFFAECC5B8776AC87DBC4278B4D2E0A341026F3B9FF43B84F604A52797D134E2C3881ADF03C9358F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Qm.0..kc..kc..kc..jc..kc.~jb..kc.~nb..kc.~ob..kc.~hb..kc.ycb-. kc.y.c..kc.yib..kcRich..kc.....PE..d....5.....".....L...4.....H.....=.....A.....P....p.....`..4#..... .....!..p..... .....P...8.....text..... ..h.rdata..H}.....@..H.data...d....P.....D.....@....pdata..4#...`...$...L.....@..H.idat a...,.....0...p.....@..HPAGE.....-.....0..... ..`INIT.....[.....\..... ..bINIT.....P.....,.....@...GFIDS...<....`.....4.....@..B.rsrc.....p.....8..... .@..B.reloc.....0...P.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Drivers\WdNisDrv.sys	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	86264
Entropy (8bit):	6.087010539108971
Encrypted:	false
SSDEEP:	1536:xFbk8rfBGjiGUQiQ5Df0uEWWH1shZJ+Rb7NvmoHPNr:xFbprZGuzQnjR81shW5JvmCFr
MD5:	9C4361259D5F0D7A36A10BD28D000F90
SHA1:	F1CB41DB2356666AD123686B0AD52A2112D91474
SHA-256:	7445476DE9BAB0D9C975DBDF63BD928D7E3139DF3FC69463BF08897E3B087575
SHA-512:	55863A0B999439CD0C1747A81BD34991D81C631571797CC6F6335B60F1D054EB31951418DAF5587ADC43F65F16711482FBC82D0F0C9495CFBA834919FDBF9264
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..U..U.....Q..U..,.....R.....E.....S....Z...%.T....T..RichU..... PE..d....%.....".....\.....`.....`A.....h...P.....0.. .....H...X...p.....8.....@..... .....text...*..... ..h.rdata..p .....$.....@..H.data...(.....@....pdata.....@..H.idata.....@..HPAGE....H ...0...$..... ..`INIT.....`..... ..bGFIDS.....p.....@..B.rsrc.....@..B.reloc.....$.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-AMFilter.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12624
Entropy (8bit):	5.259327730394375
Encrypted:	false
SSDEEP:	192:/5mm9AfGjUa1rIL+FUVin2F/OZDfYj5YbAxqTSSS6S8SzSySovK1ZVuB:/5mm9AfGtML+Fws2Fo7m5YcxHKrVo
MD5:	B6D65A86FC1999A62DA10EA3C4CAD3E4
SHA1:	E79E97C04D8540A2005D21021F7781676E705BCD
SHA-256:	05B2BFD40FB3A344C3AE178C420A7FEA9595815CB1CC07843078112F5F551EAF
SHA-512:	7F13B4930F9BF9ABCFD64E905DA4F0111B34197A533FB0162E43C4C80F39D135ADAA09C3E7AF3E95397BEF5D1D323E75721CEE150517CB13EBED3029C781BE 6

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-AMFilter.man	
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Drivers" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>... .. ********** ********** .. Driver files.. ********** ********** .. -->...<file destinationPath="$(runtime.drivers)" importPath="$(build.campBinaryImportPath)" name="WdFilter.sys" sourceName="WdFilter.sys" sourcePath=".\"></file>...<file destinationPath="$(runtime.drivers)" importPath="$(build.campBinaryImportPath)" name="WdBoot.sys" sourceName="WdBoot.sys" sou

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-NIS.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6173
Entropy (8bit):	5.373156847974759
Encrypted:	false
SSDEEP:	96:/3coK5HjFWr/96Hj+Uul2lewqo3nRtlUl3lflxSDwMKRbRhK18YaKMr4e:/mDFcujBuEgI3nzC1Z6V8f3
MD5:	5562965C32F03AE0DF8B9DEF950F8651
SHA1:	6E5AD734AB6A9F8B82B19024E21007AC2CAD2540
SHA-256:	EA64BE59286B67AE930729FA92B2B08DCE5C2EAEB70FEABE2320C47FB6DDAC6C
SHA-512:	F64D728AFE40800968D0B165019E775F62F2CCA40BFBB370F52F4BA8FCC2574F79D2C4AC41CCAE6E1CEC23082BA24B5E6C0A5531E6B336683BEEEDDA3CB81DE
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-NisSrvEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{102aab0a-9d9c-4887-a860-55de33b96595}" message="$(string.Microsoft-Antimalware-NIS.provider.name)" messageFileName="%ProgramFiles%\Windows Defender\NisSrv.exe" name="Microsoft-Antimalware-NIS" resourceFileName="%ProgramFiles%\Windows Defender\NisSrv.exe" symbol="Microsoft_Antimalware_NIS">.....<tasks>.....<task eventGUID="{b33e041e-3a75-4f52-bf0e-c85d0963b7fb}" name="N

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-Protection.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3369
Entropy (8bit):	5.312049604455802
Encrypted:	false
SSDEEP:	96:/3poK58yFND08uf9zXzUzCzwat0kz9nHHzyPYjHMrje:/FbFHuf9DzUOVJ1HHePv2
MD5:	E4AD891E7B62475FCA109C0DF4DEF16E
SHA1:	B7DC3C04C67D7903E04B0EBF2AB7840AAA717EE0
SHA-256:	DF9AD93CDB61587A35FCDCE996955A64413439A474D85C86133A9E9C185D1966
SHA-512:	0849CB6F3DAA6C80B94F770E29BD389B67D31E089595B22BFAF1D6F25C6E847DA4DCBFF135F6D96E30597991FF6C8CA8EB5306C4E8D1B334016220058B2969E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpClientEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{e4b70372-261f-4c54-8fa6-a5a7914d73da}" message="$(string.Microsoft-Antimalware-Protection.provider.name)" messageFileName="%programfiles%\Windows Defender\MpClient.dll" name="Microsoft-Antimalware-Protection" resourceFileName="%programfiles%\Windows Defender\MpClient.dll" symbol="Microsoft_Antimalware_Protection">.....<tasks>.....<task eventGUID="{7db81ddd-d2be-41bd-

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-RTP.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12885
Entropy (8bit):	5.3652290431980765
Encrypted:	false
SSDEEP:	192:/ozFIItP1HvYoPp5z7YlAZSJwyygPJ2HBfEj:/QFIwP1PYoh5WAZSJwsJ2NC
MD5:	35AC30A8637BC0EB2F7902B8C69BF904
SHA1:	DB4C458A6007F444AECF8F4C49E481CC9935B22C
SHA-256:	FE761134076253DC11CF8C154CA43E762C61C28D0A817E76351FFEF32CCF59C0
SHA-512:	E41E522BF542D3B662D741E04523D1140C66585B64E811F6CD27C74466156F2FB728890C73579D4CFAD0BF8758D4F699A79C5B0B4B98479D60D386ACC26A8C49
Malicious:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-RTP.man	
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XML Schema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpRtpEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{8e92deef-5e17-413b-b927-59b2f06a3cfc}" message="$(string.Microsoft-Antimalware-RTP.provider.name)" messageFileName="%programfiles%\Windows Defender\MpRtp.dll" name="Microsoft-Antimalware-RTP" resourceFileName="%programfiles%\Windows Defender\MpRtp.dll" symbol="Microsoft_Antimalware_RTP">.....<maps>.....<valueMap name="DlpOperationType">.....<map message="$(string.Ope

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Antimalware-Service.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	31904
Entropy (8bit):	5.2624632476710405
Encrypted:	false
SSDEEP:	384:/VFriW4cboWcauSi6fZeeCifUhwqh+46AJJCZvsp33icjEtFBR2EaXU1Hgb1RVxq:tFriHcblBLuJ1ycgtR6XNxB4
MD5:	B003B1DFFD9221745ED31E2979B28574
SHA1:	FBCEB9767657E596CEA5E29EBDA57207F5B08A5D
SHA-256:	5AE7493F638252D49F18B084D7CEA4E88D3AF6B1170C8C16EABF5C6AE849E3C9
SHA-512:	B731F60AC20548A54C465BFC3B20334946A384895C8AA4DF4C1DA969FB71F4B7C1BEC50044C4C5A9555B68B68C8A96EC45AE78FC5EBCD406102AE144A737FF2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XML Schema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Service-MpSvcEtw" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<instrumentation>....<events xmlns="http://schemas.microsoft.com/win/2004/08/events" xmlns:ms="http://manifests.microsoft.com/win/2004/08/windows/events" xmlns:win="http://manifests.microsoft.com/win/2004/08/windows/events">.....<provider guid="{751ef305-6c6e-4fed-b847-02ef79d26aef}" message="$(string.Microsoft-Antimalware-Service.provider.name)" messageFileName="%programfiles%\Windows Defender\MpSvc.dll" name="Microsoft-Antimalware-Service" resourceFileName="%programfiles%\Windows Defender\MpSvc.dll" symbol="Microsoft_Antimalware_Service">.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Microsoft-Windows-Windows Defender.man	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	149152
Entropy (8bit):	5.478121035794876
Encrypted:	false
SSDEEP:	1536:5oQofFA+1KSYfSN8bvc0/E/EvJ4rXVEc+ICO+PV5FqGc9HCOKK1HVX:SBfErIHKK1HVX
MD5:	36F8A68EECFB5B89C4C571F6A63E3ECA
SHA1:	242DC76813FE0BE2E676D37538FD887292803E68
SHA-256:	4D76246642181E38F87B623AF82BF7454050D05775F546506CFACA1608BE9633
SHA-512:	C483FCE988F96156FAAACA093F1CE948B0CC42C006012F6F29308F4ED09D295951F59C79A547341578616E58561CAF858135881AF305B3166E1D4474B48D35C8
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v3" xmlns:xsd="http://www.w3.org/2001/XML Schema">...<assemblyIdentity buildType="release" language="neutral" name="Windows-Defender-Events" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384" versionScope="nonSxS"></assemblyIdentity>...<dependency discoverable="false" optional="false" resourceType="Resources">....<dependentAssembly>.....<assemblyIdentity buildType="release" language="*" name="Windows-Defender-Events.Resources" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" version="10.0.10011.16384"></assemblyIdentity>....</dependentAssembly>...</dependency>... .. ********** ********** BEGIN FILES SECTION .. ********** ********** .. --

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpAsDesc.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	209144
Entropy (8bit):	5.205036912846813
Encrypted:	false
SSDEEP:	6144:PmiTVVmVVV8VVNVVVcVVVxVVVPVVlVVVRVVVtVVWV60jVLVVOVVUVZVVVVVjVVJL:tr
MD5:	A27F0ABF90F3B468C6F15CDAFBBC3312
SHA1:	D75B9FD570E9650F583F15F0F0F37EB2CBC39EC4
SHA-256:	503DF4EF842D6621139D4A15D68955E4926C0C6B5CCCEF60323290A6FC08343F
SHA-512:	9716144577A19591E12BB10732FF135D00928D1C5951AB220057A4A00D42B74E8980825D6DD60A8486EE1EC75CBAEA7C5525D4F4E600F5F869BEABA53C7D5FE2
Malicious:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpAsDesc.dll

Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..d....z....." ....`A..... ....T.....rdata..... .....@..@.rsrc..... ....@..@.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpAzSubmit.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1409272
Entropy (8bit):	6.2399898718653075
Encrypted:	false
SSDEEP:	24576:5k4dJL+FQJApr2tz1+lC2zxw6y2os4OXB7vcHFzqh7OcI:5k4dJK+Jur2tz1+lC2VO2osDy
MD5:	C10F256B7606EE5B1BED880020F68912
SHA1:	76B51FDD50A3EEBD4B55D97E3C9A8B8C79EDF978
SHA-256:	C649EC99F87F684D22157755E5F8E0AF7C1EFD54853493965A673A3F0FFB4AC6
SHA-512:	A5A9C4190A831D1FE2EADD1AB9FE97A0BE39FE4EE97A0F223D0AC42E80C72FA2B77AA0D2F929A3B2F10E7AB4E850BC7DF1DE420CAFD7289C08C763D951D99 7CB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`J.v3J.v3J.v3..u2K.v3..w2Y.v3J.w3u.v3..u2Y.v3..r2a.v3..s2.. v3..3H.v3..v2K.v3...2.v3..3K.v3..t2K.v3RichJ.v3.....PE..d....." .....P... .....f.....r4....`A.....`b.....c.....@.... ...@.....`... ...P...,..|k..p.....(.....8.....text...HO.....P..... ..`.rdata..$....`... ...`.....@..@.data...8.....@....pda ta.....@..... .....@..@.rsrc.....@..... .....@..@.reloc.....P...0...0.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpClient.dll

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1151224
Entropy (8bit):	6.1798062394748685
Encrypted:	false
SSDEEP:	24576:MLG0IKv+HzAmqQBrTPQWNRIyQhZBcfy0RkgJ:cGFu+HzAmqEQWNRIypfy0J
MD5:	FD7D2158F21085FF8E8C46829839708E
SHA1:	1749008645208E9769DD68D36124113E71923F6D
SHA-256:	DE50D8BB61B7F0BB423E4A50A6775192C4809F63C18BE9426C4AC2E127BB9DA9
SHA-512:	03707AEAF1FED4C2BDC2CA4167498C5F7C57153A47F386D9C6A7A0DF75CD5B3C54D01A42AB56B6FDBF9A10E26213A6540FDE19F5036DC8E659500F19D728AF 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.....?.....i.....V.....V.... ....?.....V.k.....V.....Rich.....PE..d...f....." .....g.....[.....3.....`A.....8...T....@.....p... ...P...!.....p..... .....(o..(.....8.....Po.....text..... ..`.rdata...R.....`.....@..@.data.....@....pdata.....@..@.di dat.....0..... .....@....rsrc.....@.....0.....@..@.reloc...!...P...0...@.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCmdRun.exe

Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	884544
Entropy (8bit):	6.103389158363899
Encrypted:	false
SSDEEP:	12288:b1SQ6UqCplyaRffknhoV55jmvuN7Wk0mCBRUe:b+UbnkhoVLmvuNqBGe
MD5:	D50CBCB0B8B3282CD169E0032361D418
SHA1:	948E0431282837D2E654BFD805461967B99E63B4
SHA-256:	F7B6EB6E4D8E04C7243AB0AB73CEC6E20E980F07E03267ED4B0CA69CF9CDAB3D
SHA-512:	13184B5DFD5E82C44F1451AD426B7FB8ACE63923679D4210C3B2CACE6691DBACD113E9D55FFB041D1C79C46A80C128EE5D2A97E874487A938DBCF08C03A1C EC
Malicious:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCmdRun.exe	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`..`...`..z....`..z....`..&....`..&....`...l..`..&....`..&....`..`...b..z...l`..... `..z....`..z....`..Rich.`.....PE..d.....".....0.....@.....P.....j..... .....p.....,O...@..@?...@.....p.. .....J..(....(..8.....@J.....8.....text...[..... ..`.rdata..>.... ..... .....@..@.data....M.....@.....@....pdata..,O.....P.....@ ..@.didat.....`.....P.....@....rsrc.....p.....`.....@..@.reloc.....@.....0.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCommu.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	352504
Entropy (8bit):	6.026593673622959
Encrypted:	false
SSDEEP:	6144:yOoa9kPfLM055gj5qDj8qdzRf8IGRx7Ur9opJtwEKLoi7GG75li:yXHjgjELzRf4q9oduLR77i
MD5:	98DE76E6BD6919C81785F34F3E4E4025
SHA1:	9E1BF8C617D7D629623D16DE29889659F4623066
SHA-256:	A5D1C85E15E4454D0CF4E613107F688B540A046659F1DDECA859B395335BD50D
SHA-512:	5F233E59E8C4BB320C5BCD42505300EFEAA519FE35B1877A7213CB471162A1BB613C027FBDB1126FB6E747A704CDE4D799FC4421808819650126D4A9EB282557
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I...I...I.....K.....H.....E.....G.....A...@.o.X...I.....e.....H..... ...H.....H...RichI.....PE..d....5.}....." .....`.....f.....P.....n.....`A.....0.....,...@... ...@..(...I...p..... .....H...(.....8.....p.....text...5..... ..`.rdata..... .....@..@.data....#..... .....@....pdata...,.....0.....@..@.didat..X.... .....@....rsrc.....0..... .....@..@.reloc..(....@.....0.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpCopyAccelerator.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	165576
Entropy (8bit):	5.403399700794782
Encrypted:	false
SSDEEP:	3072:Obc/k/710XdiWNGKTeoKeMK9OQWExQc5W:OIM/72IWb9n9OQWEno
MD5:	B613F7C352DB0471338A01FA7CF94521
SHA1:	04618A6DD7100D957E6B190F70C263F1FF775CAB
SHA-256:	71ABD7C64E51AF9A750A31BAC218F9E6781C913869D97AA4024C2456E101CB20
SHA-512:	0D538585A972252EF6FF99C3ABB8F682201EE33A0FDFADB5BDCBEEE65E38D2C64BF8893B1691276ABF8F44303309BECF89AE0E74C3248609FB93FA22A6CD8F5 D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F.....F.....B....F.....F.....Ric h.....PE..d.....J....."....P.....@.....`..... .....Z.....<....`...&...P..4....8..p.....(.....8..... ..8.....text..... ..`.rdata..].....`.....@..@.data.....p.....p.....@....pdata..<.....@..@.rsrc..... @..@.reloc..4....P.....P.....@..B.....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpDetours.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	164088
Entropy (8bit):	5.889246599238573
Encrypted:	false
SSDEEP:	3072:LhAcjxmGnxakZmOpjZrppk4sGFO5SVyT+/t5xRbOz8kKbc/3u:LKc4GnQeVaGs5ZgbRk6cG
MD5:	6694C427D876FEEC65126E7734886E88
SHA1:	F6F08ADEEA556B241E4010F538DA7E6C32047628
SHA-256:	A76E653BA8D251379133B748B685C08672A69D1CF95493549E563CFAD8A8D7A5
SHA-512:	620A52BF3D503B82D82799C48A23CF4AA8BD7E399C343192EDB52E28FA6815976C90621D1B2E5EB841B0711F5F4191BFB141529CC341EAA215A8905A65FA0010
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpDetours.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:Q..~0t.~0t.~0t..Ew..0t..Bu.n0t..Bp.r0t..Bw.y0t.wH.q0t.~0u.M1t ..Bq.W0t..Et..0t..E}.60t..E...0t..Ev..0t.Rich~0t.....PE..d.....x....." .....p.....`A.....P.....0.....`... ...`.....@...p.....(...`...8.....text....v..... ..`.rdata.....@..@.data.....@....pdata.....0... ... ..... .....@..@.rsrc.....P.....@.....@..@.reloc.....`.....P.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpDetoursCopyAccelerator.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	102632
Entropy (8bit):	5.416424506292462
Encrypted:	false
SSDEEP:	1536:dnC8TM3nUZtTOwts7XxhrTNCfDgFvFJ2m6K2mPegHPxG:ZTM3UZtTOwW7XTNCfDGdBx2mPeqk
MD5:	50E2C916D6B2E5CDCED1BF18BEF5B9E6
SHA1:	523DA8427550B397352D0C7D9770BBE57E31C5CD
SHA-256:	C880E519887E5AFD35612BDAF4F987D79ED294050A4D291B54B18F7F3C80A89D
SHA-512:	C95F1D480DC1EF5587C9B9CE89F9C58550B2CD7E1E2389DE3A02DFBF541C9BBF66AFEC724767B574C81236FF0F5AE9C25D99702BA76FFC214290536C32BD6FD
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.v. .v. .v. U..!.v. ...!.v. ...!.v. ...!.v. ..U .v. .v. .w. ...!.v. U..!.v. U..!.v. U.9 .v. U..!.v. Rich.v. .....PE..d...F[.S....." .....^.....j....`A.....0...H...x.....`..X....P.....p.. ...p.....p..... .....h...(...0...8.....0.....text...R..... ..`.rdata..*W.....`.....@..@.data.....0.....0.....@....pdata.....P.....@.....@. .@.rsrc...X....`.....P.....@..@.reloc.....p.....`.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpDlpCmd.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	372176
Entropy (8bit):	5.810540726487847
Encrypted:	false
SSDEEP:	6144:SqKvKD0BvxUWJsoyvdnja6lHfF2tZLmiTVVmVVV8VVNVVVcVVVxVVVPVVlVVVRVi:jyBWGxyvmR1
MD5:	9DA1C405AF787EFBAF735B76388F867F
SHA1:	7C9F2DD2C72A15B2954534BB7021C9DB3F850DA1
SHA-256:	7E7180B5534BE4BF2E531DCCE4BD8C0CB55EEC93759625283A162C0F6149464F
SHA-512:	66190E1EA2D6FA7EE048D204746216B8C8146C0F17114CA1651B566632F32970F2F6113131338D96D43FDCA33A9266D142016DCD6369F27CE6657DF12FB823E5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.8...k...k...k7v.j...k7v.j...kkq.j...kkq.j...k.{sk...kkq.j...kkq.k...kkq.j...k.. .k...k7v.j...k7v.k...k7v.j...kRich...k.....PE..d...V..F....."....9.....@.....y..... .....4...@....p.....P..<.....-.. ....l...P...p.....(...`...8.....h.....text...E..... ..`.rdata...}.....@..@.data.....0.....0.....@....pdata..<....P... ...@ .....@..@.rsrc.....p.....`.....@..@.reloc..l.....p.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpEvMsg.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	143608
Entropy (8bit):	3.8404828233814126
Encrypted:	false
SSDEEP:	768:7r/gwWulQnuBkG22Tumo0cTH6QKqCmuKqrWmNKq4mZKqdmjd4KqgmXyGgR1PRGzm:QIBkG2usKoHPim
MD5:	E6BA4B06A514B05F1A6F67E02776CB12
SHA1:	40CE66816509483AD45B8B6DE05D5F9AC23671CB
SHA-256:	3E69F409180506A6636CA8F0620AB0CC9B57F1393AC5986CC8BBE50BEF12C9C2
SHA-512:	C8DDB425AEA945C86742ED8E8940E655BC24AB66EE4FAEDB7F29FA7A187809DABD326A529777691481E53C55D5119402D4016CDED33919840AC98D9C636C30
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..d....." ....`A..... ....T.....rdata..... .....@..@.rsrc..... ....@..@..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpOAV.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	495848
Entropy (8bit):	6.009124528357715
Encrypted:	false
SSDEEP:	6144:l7A3ZwUGB8s0MYG75D5DU3b9EV0ShqJULr0XVCOPmiTVVmVVV8VVNVVVcVVVxVVV:lk3a7J5DS9EV0MqJULrkkMo
MD5:	507A1C4DC135D31E60E46C911F518352
SHA1:	94D0E5C74AD632CDE21A967FD6A06999153B6CC7
SHA-256:	07AA7775DEC86AFEF867C3B902BCF47CCB36E224433171EB6C4C0E3D80F753AB
SHA-512:	FD980B28BA5E60536D695707716B4AC5B2AD63EEF1AF82534B326E2DBF6CA349DDA189C70CAF638C2AB6C3D6EB187F3C613FC5097C645C4272D9C60E8E2BE3 05
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M...#...#...#.v. ...#.*."..#..."..#.*.'..#.*. ...#.*.&.>.#.v.#...#.v.*..#.v..... #.v.!...#.Rich..#.....PE..d...A....." .....`A.....D...x.....`...#...p... .....t.....p.....8..(. ..P7..8.....8..p.....text..."..... ..`.rdata.....@..@.data....0... ... ... .....@....pdata...#...`...0...@.....@..@.rsrc..... .p.....@..@.reloc..t.....`.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpRtp.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1478904
Entropy (8bit):	6.324410065456569
Encrypted:	false
SSDEEP:	24576:43IcInwFd0DDgUkXbikt2m94TdJdiLyvBW+IYHMb1ie:4YrvDDgsm2mWJdiLiBWZQMb1ie
MD5:	EABFAF1CE6CB8843DA42FBA01E8BF069
SHA1:	ADBD3EF5C4EBD0D395B157489A3B5D34EAB8CFFF
SHA-256:	CA99B8EAA6ED8C706590551BE37107D027BBD53CC9E52805446ADF59B3AEDC1E
SHA-512:	AFF68BBE9B8A086E2E49BDBC864DE8FA8E5990F23F38B385CDEE56C189C52088B24DD492A779EA2ECDD751AB682B81041B674E854DCB190F8EBD10079FC1F6 8C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H...)...)...)..M\...)..M\...)...[...)...)...(...[...)...[...)...[...)..M\...)..M\ ...)..M\W..)..M\...)..Rich.).....PE..d...t`....." .....^.....`A.....P...d..... ...B...p.....p... ...p.....`...p..... .....(.....8.....(.....4... .....text....t..... ..`.rdata..^V.....`.....@..@.data...<p.....`.....@....pdata.....p.....P.....@..@.didat..X. .....@....rsrc....B... ...P.....@..@.reloc.....p... ...P.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpSigStub.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	803176
Entropy (8bit):	6.37118649960636
Encrypted:	false
SSDEEP:	24576:Ghj1QlBYDgtUUvie3n+pB3+ojRlcD1VyZTFXk:GhpQlBHtBYla1VyZpU
MD5:	01F92DC7A766FF783AE7AF40FD0334FB
SHA1:	45D7B8E98E22F939ED0083FE31204CAA9A72FA76
SHA-256:	FA42B9B84754E2E8368E8929FA045BE86DBD72678176EE75814D2A16D23E5C26
SHA-512:	BEA5F3D7FB0984C4A71720F25644CE3151FCDC95586E1E2FFE804D04567AAF30D8678608110E241C7DDF908F94882EDDD84A994573B0C808D1C064F0E135A583
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..#...#...#..EV...#...Q...#...Q...#...Q...#...Q...#...#...#..."..EV..#..EV N..#..EV...#..Rich.#.....PE..d.....P....."....`.....@.....0.....-....`..... .....t..d..... .....D... ..h!... .....d...p..... (.....8.....0.....text...2R.....`..... ..`.rdata.....p... ...p.....@..@.data..../..... .....@....pdata...D.....P.....@..@.rsrc... ....@..@.reloc..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpSvc.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3113208

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpSvc.dll	
Entropy (8bit):	6.304406527619417
Encrypted:	false
SSDEEP:	49152:RThS41BElO7Jyf4HtxHnXXnh/vz1ztLm0exGP9lbw6ieBh4wBg:nR/EE7ofGx1fFxg
MD5:	0618D6AA4B96E666F1C3B79CA1531187
SHA1:	037AA87516FA27ADAE6499FFE314601262FE8E8A
SHA-256:	89FD82BABFEE76643CA0F3DC4730302575E2BCCB00F744090D9E253A8CD9EE53
SHA-512:	457ECDAF9CC2AB3E6E26F8899831979AC5B1D0D59483CFC30A815280CD362173E0E349F5CC28F45DE25E2AB9DF4731768CF06A0C8E66E595847A67A43833F48
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....!.\Z@..Z@..Z@...5..X@...5..[@...2..H@...2..H@...2..S@..S8*.M@ ..Z@...B...2..j@...2D.X@...5..[@...5..?A..}...]@...5F.[@...5..[@..RichZ@.....PE..d....." .....".....\...../.....;0...`A..... .....B,.d....C,.h.....`....p-.d1...`/.. ...P/.h4.../(.p.....#.(.....".8.....#.....;,.@.....text....q".....".....  ..`.rdata.....".....".....@..@.data... .....,.....,.....@....pdata..d1...p-..@...@-.....@..@.didat.....@....rsrc...`.....@..@.reloc..h4...P/..@... /.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpUpdate.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	151800
Entropy (8bit):	5.674686738982597
Encrypted:	false
SSDEEP:	1536:LJ9Z2WHykjzKo81vmwUGKyBA3LTqjSL0fieoeKTePoWQbzkDHP+W:LJ9b3Kd1vm/GymuL0fieoeKTePovbzsT
MD5:	BA4E1FC83B68F72927F58BBFA064C294
SHA1:	F0F57EB79F2478D7BFE4AD4D18361D2F09E3E03A
SHA-256:	23C224794D0342F3C97D6F104B40465A8C314186DD3A9F0CBBC9A9441700AE83
SHA-512:	789D52FF5491488B162422BFB4A6D4FB9D40E905B6A370AD2A9F20BA095B9485D5AF07EB8CD660D2BF4F4906DC1FA68ACD223ACFE913FC5F99F78FBDA56DDC A4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ew9{!.W(!.W(!.W(.cT) .W(.cV)#.W(.dV)0.W(.dS),.W(.dT)&.W((n.(/. W(!.V(q.W(.dR)..W(.cW) .W(.c^)n.W(.c.(.W(.cU) .W(Rich!.W(.....PE..d.... 3"....." ....h.....@.....`A..... ..L...\..... .....0... ...0.....@...p.....xU..(...@T..8.....U.....text..... ..... ..`.rdata..D....0.....0.....@..@.data... ....@....pdata..... .....@..@.rsrc..... .....@..@.reloc.....0..... .....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MpUxAgent.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	545016
Entropy (8bit):	5.974310663865527
Encrypted:	false
SSDEEP:	6144:j/zDRgR8KZHQf7uiJRpqVCy6H5gAH2IGCXl/2UWYbyKHiTVVmVVV8VVNVVVcVVVB:7zDRvDp/qVC1gAH2IGCXlPh4S
MD5:	68228D20DFAA033D246B8BED272CF92C
SHA1:	F351C4991FFC3190131B279E06A0F58856EBC375
SHA-256:	C44F961691C4F91AD370985D5EB281F843EB5DCF6F5EC98D9C9A509E789CB7E8
SHA-512:	2B327EB01858A1B7C80275B9F5B3B642592DFE0AD357B3C65D7C483D0CB59178CB33A245408BC0A962F28594B504C0F17521F567A8AD5CA981A770CC9B85791
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>7._Y.._Y.._Y..*Z.._Y..*X.._Y.Y-X.._Y.Y-]..Y.Y-Z.._Y..'.._Y. ._X..^Y.Y-\.._Y.Y-...Y..*Y.._Y..*P.._Y..*...Y..*[.._Y.Rich._Y.....PE..d.....2....." .....&.....0.....;.....A.....8.... ....0..\.....#...0... ... .p.....X...(... ...8.....x.....text...%..... ..`.rdata..x..... .....@..@.data....-.....0.....@....pdat a...#.....0.....@..@.rsrc...\....0.....0.....@..@.reloc..... ....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MsMpEng.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	128392
Entropy (8bit):	5.775533067291842
Encrypted:	false
SSDEEP:	3072:gPkBbbztTh/9kcexTIJO0gj7KTe9q7CTttUSkh6e5:gPIfRh/9kUJDZuttUNse
MD5:	15D205854CA62B75C0BF447F9DD8119D
SHA1:	F1A1874738E310CE76D37C1045EA00C0CEFCF64B

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MsMpEng.exe	
SHA-256:	B815A94D49CC0E8DB03456CBBAFB4A052F481531F8768CE704A2A012FD84B7AB
SHA-512:	A6B324F884525875849994EE2247B98BF3D389A49B4E387A578F05E92FB754CEF6AD917D5CE201A40E88FDAA0A117C6D23EB5B7FEA6F4765F48EE957AB471B85
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-.U.L...L...L..W9...L...>...L...>...L...4...L...>...L...>...L...L...M.. W9...L..W9y..L..W9...L..Rich.L.....PE..d....MCD.....".....@.....N.....tj.....\|.....%.....`....<..p.. .....$..(...."..8.....@$.....text...B..... ..`.rdata...Y... ...`... .....@..@.data.....@....pdata..|..... .....@ ..@.rsrc.....@..@.reloc..`.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\MsMpLics.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	20728
Entropy (8bit):	4.482228069977977
Encrypted:	false
SSDEEP:	192:7rPEnfKWgFHWaALc2Fu462TNOxjB1RDBQABJpI4BOk9qnajR5d:7rPEniWgFHWa1MJERDBRJpxBhl95
MD5:	7B842DAC975E04C90F9B23B7D04B5160
SHA1:	DE370B7FBC16E36955A700D472BAD83A029F2B52
SHA-256:	61D412008B89D3B931BC9E8AD731F792DD9EF2D2F147916103B8F9392CF8D501
SHA-512:	7D7891BC65B67D9FB9CBA00953A3B86FEFD987EAE2718C79C36B17E1DDAC054A40E3DDE7AF662C8126C2B8440F172C7DF01C24469A8C0D57BD719255BD432F 2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..d....I?....." ....0.....P.....`A..... .....0... .....T.....rdata..... .....@..@.rsrc..... ....@..@..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\NisSrv.exe	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2855512
Entropy (8bit):	6.440503543687848
Encrypted:	false
SSDEEP:	49152:JwgA1BydF9JuPAdoZ6Ig1hUcN2DARtfp+Q4s+W8:JqTi7cW
MD5:	054F919445EDBC999989A1413FD87437
SHA1:	597196C3A4C1CDC1DB5F1A0C39C37CB6C4FC1FB1
SHA-256:	A124EBD9240AAA542962CB2A1059B6315E9F2183CBFD08B4E8029EE15B6A009F
SHA-512:	38C530ABE67F12EEE0A6734CE51FCC24C0CD81AAFD232137A41E221B79FEE9BA07253DA7F50EBEE0E9BFF0FEBCC547C1CCFAE4AE7B222A13B8DC9A3097E2 ED50
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h.C.....C\|.....C\|.....{.....{.....{.....{.....q;.....{.....{U..... ....C\|..i...C\|W.....C\|.....Rich.....PE..d....\k....."......0#.....]!.....@..... .,.....+...`.....(.,.....+.H....`*..P....+.X.....+. .0.. .$.p.....h.#.(...0.#.8.....#.0....|(.....text...?'#.....0#..... ..`.rdata...i...@#..p...@#.....@..@.data...@.....(.....(.....@....pdata...P...`*. .`...P).....@..@.didat.....+.....*.....@....rsrc...H.....+.....*.....@..@.reloc...0....+..@....*.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\Defender.psd1	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	13827
Entropy (8bit):	5.952601509916055
Encrypted:	false
SSDEEP:	384:6B7YQ0ExG5Ju4mSFCsCow7+xPcgGywK85lbkn+uwgGhF887:4YQ0Ec5Ju4mweozx0gGyu5Sn+uDuF8c
MD5:	9346D71D826DC7B6580C6206FD1A272E
SHA1:	21B45677AE39E36928CC1DE58958350CF7B49FE7
SHA-256:	EE3344F2D9FE64E0593B1DCE5FC4743D4891DAA6528A0650C41ED0D3F455D48E
SHA-512:	FD976F99CF3B47D6D9E17CEEBF5322C2F9583FA0F9D65E3C6D5144926911861DA3B4E57BD4E72CF3DBF7826BE5B5EF107BAEEB0C1DDF433BE4020B91D03467 C9
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\Defender.psd1	
Preview:	@{.. GUID = 'C46BE3DC-30A9-452F-A5FD-4BF9CA87A854'.. Author="Microsoft Corporation".. CompanyName="Microsoft Corporation".. Copyright="Copyright (C) Microsoft Corporation. All rights reserved.".. ModuleVersion = '1.0'.. NestedModules = @('MSFT_MpComputerStatus.cdxml',.. 'MSFT_Mp Preference.cdxml',.. 'MSFT_MpThreat.cdxml',.. 'MSFT_MpThreatCatalog.cdxml',.. 'MSFT_MpThreatDetection.cdxml',.. 'MSFT_MpScan.cdxml',.. 'MSFT_MpSignature.cdxml',.. 'MSFT_MpWDOScan.cdxml',.. 'MSFT_MpPerforman ceRecording.psm1'..).... FormatsToProcess = @('MSFT_MpPerformanceReport.Format.ps1xml').... FunctionsToExport = @('Get-MpPreference',.. 'Set-MpPreference',.. 'Add-MpPreference',.. 'Remove-MpPreference',..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpComputerStatus .cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	13946
Entropy (8bit):	5.978353470104296
Encrypted:	false
SSDEEP:	384:PX0m6YBOzHQV80tQEFMxOQhCLyTmSKXEllOhalPvnAQEYhW:v0m6YQzHY80tQpOQYLy6SKkIZFvnAQhU
MD5:	58DF8D38469AF7353B672A6F145994DC
SHA1:	DDC641F88A0B3452366CB920306CC3A90961A3C0
SHA-256:	A63B944CF4FB3DB7F758F7E4D94126ABE99916127E451E0C139D71E94744084A
SHA-512:	67B82A79DB97641976C942C448DF9D99317FF5CDC0BE3A1DB1CCA04C3BB8CE3832238E031D22E06CAE4E8ADD3BAB88CEEE29613680C8F33F197599D7863342 5
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="R OOT\Microsoft\Windows\Defender\MSFT_MpComputerStatus">.. <Version>1.0</Version>.. <DefaultNoun>MpComputerStatus</DefaultNoun>.... <InstanceCm dlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. .. </GetCmdletParameters>.. </InstanceCmdlets> .. </Class>.. ..</Powe rShellMetadata>..... SIG # Begin signature block -->.. MIIhZwYJKoZIhvcNAQcCoIIhWDCCIVQCAQExDzANBglghkgBZQMEAgEFADB5Bgor -->.. BgEEA YI3AgEEoGswaTA0BgorBgEEAYI3AgEeMCYCAwEAAAQQH8w7YFlLCE63JNLG -->.. KX7zUQIBAAIBAAIBAAIBAADAxMA0GCWCGSAFlAwQCAQUABCCC GKubREngV5EF -->.. DodK5brTAqlkaVHav/M+SkqGWqFKKqCCC14wggTrMIID06ADAgECAhMzAAAIMJFU -->.. sm0DDuykAAAAAAgwMA0GCSqGSIb3DQEBCwUA MHkxCzAJBgNVBAYTAlVTMRMwEQYD -->.. VQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdSZWRtb25kMR4wHAYDVQQKExVNaWNy -->.. b3NvZnQgQ29y

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpPerformanceRec ording.psm1	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	39934
Entropy (8bit):	5.64362105596826
Encrypted:	false
SSDEEP:	768:yFAwQAuFiCFivo1BWMmr8OGPDKQxV3LqIYQ0Ec5Ju4mweS0+dgGyTi5Sn+UuHA:y14cC4vo1BWMmr8OGPDKQxV3LqY/fSKR
MD5:	CBA32A98D0EC2D6CCCD3306BFF7AD3D2
SHA1:	D8F98682DC20E7AD744DE5208C0A472FCB3A33C9
SHA-256:	B77C1F9B9263345F34FE32EED15BD8E3925D378CAEF5D83FEB49275447BCCED6
SHA-512:	9426238394A6043D1A16E1CDEDA953DBD5C6DF8C7D2DBA3A3F34C3E5F963927A1C9791869E4ACE96F670921827E95D9BAF30544D558C521BD01C0E5AC7CB6F 1
Malicious:	false
Reputation:	unknown
Preview:	## Copyright (c) Microsoft Corporation. All rights reserved.....<#...SYNOPSIS..This cmdlet collects a performance recording of Microsoft Defender Antivirus..scans.....DE SCRIPTION..This cmdlet collects a performance recording of Microsoft Defender Antivirus..scans. These performance recordings contain Microsoft-Antimalware-Engin e..and NT kernel process events and can be analyzed after collection using the..Get-MpPerformanceReport cmdlet.....This cmdlet requires elevated administrator p rivileges.....The performance analyzer provides insight into problematic files that could..cause performance degradation of Microsoft Defender Antivirus. This tool is..pr ovided "AS IS", and is not intended to provide suggestions on exclusions...Exclusions can reduce the level of protection on your endpoints. Exclusions,..if any, should be defined with caution.....EXAMPLE..New-MpPerformanceRecording -RecordTo:.\Defender-scans.etl....#>..function New-MpPerformanceRecording {.. [CmdletBinding()].. par

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpPerformanceRec ording.wprp	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text
Category:	modified
Size (bytes):	4971
Entropy (8bit):	4.542570045638256
Encrypted:	false
SSDEEP:	96:aAPEP3EPGEPJuDhDEMTRBTCq6IQEPvAwWSJNLKI+EPZMhkvyXHkJi2eEPZMUkvy/:aAcPUPpPJfMTRBTr6ILPvAwW6NRPZMh2
MD5:	990729AD92C1325C42B04BC975ECBD57
SHA1:	1CDBE901753CCE8D933DF8D50507CE16A25AA428
SHA-256:	E796454FEE4CF17EFDC25DB5FEEF00A5D7C1B335E6C4B4FE996E8AD7CAB01BC8
SHA-512:	EA0BCD6122068DA9412E5195C7AA3017C187790C790197AC5AF129F3ACF6C23780169C0165627E5C55CB3B99E6931CB18A42E61701C647FF07EAF6DA2740DAE

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpPerformanceRecording.wprp	
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8" standalone='yes'?>..<WindowsPerformanceRecorder Version="1.0" Author="Microsoft Defender for Endpoint" Team="Microsoft Defender for Endpoint" Comments="Microsoft Defender for Endpoint Scan performance tracing" Company="Microsoft Corporation" Copyright="Microsoft Corporation">. < Profiles>. System Providers -->.. <SystemProvider Id="SystemProvider_Scans_Light">. <Keywords>. <Keyword Value="CpuConfig" />. <Keyword Value="ProcessThread" />. <Keyword Value="ProcessCounter" />. </Keywords>. </SystemProvider>.. <SystemProvider Id="SystemProvider_Scans_Verbose" Base="SystemProvider_Scans_Light">. <Keywords Operation="Add">. <Keyword Value="Loader" />. <Keyword Value="SampledProfile"/>. </Keywords>. <Stacks>. <Stack Value="SampledProfile"/>. </Stacks>. </Syste

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpPerformanceReport.Format.ps1xml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	61966
Entropy (8bit):	4.530280013007693
Encrypted:	false
SSDEEP:	768:Bw2C10m6YQzHY80tQcd02cYVWVc80Bv/C:Bw2CTVtZk
MD5:	C9734A297293CCE204D369DD392EDDC9
SHA1:	83C091027F5BE029364DBB6C9D32BB294BC6579A
SHA-256:	CDF89F9602942969AE0493769EAC7DAA8022A1E8295D49403F1206615F92071A
SHA-512:	C474FB8F33E56DE45CB481CF921C9C21019F7610A35405BF16736A8A9C51901E750427E73271580FD1D169271DEB24A4BF1DFF130B76F26870EB4A5BE6201A7F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<Configuration>.. <ViewDefinitions>.. <View>.. <Name>default</Name>.. <ViewSelectedBy>.. <TypeName>MpPerformanceReport.Result</TypeName>.. <TypeName>Deserialized.MpPerformanceReport.Result</TypeName>.. </ViewSelectedBy>.. <CustomControl>.. <CustomEntries>.. <CustomEntry>.. <CustomItem>.. <ExpressionBinding>.. <PropertyName>TopFiles</PropertyName>.. <ItemSelectionCondition>.. <ScriptBlock>($_ | gm -Name:'TopFiles' -MemberType:NoteProperty).Count -gt 0</ScriptBlock>.. </ItemSelectionCondition>.. <CustomControl>.. <CustomEntries>.. <CustomEntry>.. <CustomItem>.. <NewLine />.. <Text>TopFiles</Text>.. <NewLine />.. <Text>========</Text>..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpPreference.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	112029
Entropy (8bit):	4.059259917659887
Encrypted:	false
SSDEEP:	768:5ouSOD2TIBNoNejxo98U0m6YQzHY80tQ4TQWjL+6SNSIZFvnAStOp:5pSODnBNUejx3mVt1LBuA7
MD5:	710B025F9E1944FDB020F27389A2E8B3
SHA1:	C8CB55361A6F483CD6B464C5364ED091AFE46DD3
SHA-256:	AA9021CFDC42493E2A759BAD0159001FFB12110FF83CD16021E57570E6402805
SHA-512:	C01AD9EB3B6394192E69F3C14A9BB5B266F04213B687D754E41D8DA080F2BFD3333ED970A4EBC04E0B657ECF7DBA8D7C44F2AC99857DA5A0A25E05FE3A79329E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="root\Microsoft\Windows\Defender\MSFT_MpPreference" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpPreference</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. </GetCmdletParameters>.. </InstanceCmdlets>.... <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Set" />.. <Method MethodName="Set">.. <ReturnValue>.. <TypePSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter ParameterName="ExclusionPath">..

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpScan.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15262
Entropy (8bit):	5.965807864910325
Encrypted:	false
SSDEEP:	384:7DORD5N4l0m6YBOzHQV80tQEFl3uN+HzbycVZ1gX5BRpBbpm39B4:K0m6YQzHY80tQpNWfgBHBo39B4
MD5:	7528936578CAEAEFE7B398C8EF4E0A47
SHA1:	9BBABA934E9C442A4630233D3BE04A4D4333E352
SHA-256:	A51C86EFD506A132274C37E288B9B697BC865F14D6D6451DA7399C7B5F36751F
SHA-512:	13D7B389428D07A7D33CBC0276919A601C686CF4A0E99059AF1D81AC0784EE61DFC5354E80D3D6E2B6E801769968980B828ACC5DC1885E6CBE73A2941D3823A
Malicious:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpScan.cdxml	
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpScan" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpScan</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Start" />.. <Method MethodName="Start">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter ParameterName="ScanPath">.. <Type PSType="System.String" />.. <CmdletParameterMetadata>.. <ValidateNotNull />.. <ValidateNotNullOrEmpty />.. </CmdletParameterMetadata>.. </Parameter>.. <Parameter ParameterName="ScanType">.. <Type PSType="MpScan.ScanType

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpSignature.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15262
Entropy (8bit):	5.966711820105084
Encrypted:	false
SSDEEP:	384:E6D5YR4l0m6YBOzHQV80tQEFekIqeYQXCSPmTmSI4EllOhalPvnAS/M0b5hsPDG:B0m6YQzHY80tQjqeYQSSO6SmIZFvnASn
MD5:	A212A25B0FA39ACB5D3F02E1CC622730
SHA1:	77846568863D3AEF5453AEF81C4302DD3F7C87BB
SHA-256:	6A8DC2AA231D974A36E0EC86751139873226D6157232EDB63AFB2AEB110CD8F5
SHA-512:	EBE171D29147429ABD182BE10174FE498EECA6D91D8DB8D9A55511E37C6E42F797A1D80892D95A61A116BCFB73DB99CEB0CC2B3365F0506ABF555E6FE80B753
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpSignature" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpSignature</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Update" />.. <Method MethodName="Update">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue>.. <Parameters>.. <Parameter ParameterName="UpdateSource">.. <Type PSType="MpSignature.UpdateSource" />.. <CmdletParameterMetadata>.. <AllowEmptyString />.. <AllowNull />.. <ValidateNotNull />.. <ValidateNotNullOrEmpty />.. <ValidateSet>.. <AllowedValue>In

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpThreat.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	14872
Entropy (8bit):	5.9567543836192955
Encrypted:	false
SSDEEP:	384:T50m6YBOzHQV80tQEFlS+yB+HzbycVZ1gX5BRpBbpmUBv/:l0m6YQzHY80tQUaWfgBHBoUBv/
MD5:	CF0F8A1D51777BDD9D08FEB023A2162A
SHA1:	47066E1FEB3C61779CC76CB52BE02148FC149CDF
SHA-256:	CFFD2BA2255685803B32ADE8D2D238A07AAEB8071EA04BCBB75CE0EF61FE9AE7
SHA-512:	B49A361319B5EA816C1FABB831C6B43C761427D7913D18E2D94AB4FE181A89394B5ADE044C1E9672FAF7B4B15D73F305CB0A8CFD8965348AD292DFD2257D99A8
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreat" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreat</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Remov

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpThreatCatalog.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	14359
Entropy (8bit):	5.974349558252268
Encrypted:	false
SSDEEP:	384:K0m6YBOzHQV80tQEFtVSderomWQfUCzuMKqbeUs:K0m6YQzHY80tQaS6omlfUCqMKqVs
MD5:	125B977FF0EE6A36452A2B6FD5AE2316
SHA1:	0C76D5588B36B5A9BFA5F2E3DD64CEA80FB1930D
SHA-256:	7856F35EB7FB72BBF8CAAAC05FD99CEE139F694209BCFBCA41AEB4C3B4CD2413
SHA-512:	9B9E246807F2890B9530197C5EFC8B236C2E11D2B616BE3E6DC813E9F8984197759A77AC73B8D8AF5FF9C13CBB370980B6DDC768281C4E38FF51CACF0D2E2B2
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpThreatCatalog.cdxml	
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatCatalog" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreatCatalog</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. </Class>..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIhXAYJKoZIhvcNAQcCol

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpThreatDetection.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	14398
Entropy (8bit):	5.977177438588654
Encrypted:	false
SSDEEP:	384:M0m6YBOzHQV80tQEFubg1+/pjK02JsuVRqikVcqgyOTx0vz:M0m6YQzHY80tQt3/M02JVWVcqHSxY
MD5:	7C91EEB90EFFB9A8D11DF34FA04FB359
SHA1:	BDFD38D168DBD76C7EC1045B8C15AFD1D6905C74
SHA-256:	97DF56A7933A45143233D314EA947801BF0A475D55A9D852FB411FFD98CB4123
SHA-512:	141BF2F83BE8728B1480469830AD0B7BD3F2E32A1EDF58EA528C26576E0E4BB5510F64B994D6A4C337EB537CB40AC78D3329637184D844BAFF0FC88CA24CF86
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpThreatDetection" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpThreatDetection</DefaultNoun>.. <InstanceCmdlets>.. <GetCmdletParameters DefaultCmdletParameterSet="DefaultSet">.. <QueryableProperties>.. <Property PropertyName="ThreatID">.. <Type PSType="int64" />.. <RegularQuery>.. <CmdletParameterMetadata IsMandatory="false" Aliases="ID".. CmdletParameterSets="ById" />.. </RegularQuery>.. </Property>.. </QueryableProperties>.. </GetCmdletParameters>.. </InstanceCmdlets>.. </Class>..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIhdwYJKoZIhvcNAQcCoIIhaDCCIW

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\Powershell\MSFT_MpWDOScan.cdxml	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	14145
Entropy (8bit):	5.978998016086098
Encrypted:	false
SSDEEP:	384:LQ0m6YBOzHQV80tQEFl7Qxh34tSZogX5BRpB6WdGtf/P:80m6YQzHY80tQgQx+t6BHBddGtfH
MD5:	0DB7196D0224FBCE614AD6ACA63F8F17
SHA1:	943B7A55F6E584C9BE421871FD4C9E21A0F326EB
SHA-256:	2D87A0FE031420903AE69DB3A30011DC659B489E2B11AA4129FED01ED3F0B00B
SHA-512:	7F9400BDD7DE5F576F6F776F2C0166EB46A68A0040078993574B8226056E419B9C74B738000AFCEC2CFCDD0A5C5CCE3A822DE19E23FEDD63DF47F85755BA17
Malicious:	false
Reputation:	unknown
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<PowerShellMetadata xmlns="http://schemas.microsoft.com/cmdlets-over-objects/2009/11">.. <Class ClassName="ROOT\Microsoft\Windows\Defender\MSFT_MpWDOScan" ClassVersion="1.0">.. <Version>1.0</Version>.. <DefaultNoun>MpWDOScan</DefaultNoun>.. <StaticCmdlets>.. <Cmdlet>.. <CmdletMetadata Verb="Start" />.. <Method MethodName="Start">.. <ReturnValue>.. <Type PSType="System.Int32" />.. <CmdletOutputMetadata>.. <ErrorCode />.. </CmdletOutputMetadata>.. </ReturnValue> .. </Method>.. </Cmdlet>.. </StaticCmdlets>.. </Class> ..</PowerShellMetadata>.. SIG # Begin signature block -->.. MIIhXgYJKoZIhvcNAQcCoIIhTzCCIUsCAQExDzANBglghkgBZQMEAgEFADB5Bgor -->.. BgEEAYI3AgEEoGswaTA0BgorBgEEAYI3AgEeMCYCAwEAAAQQH8w7YFlLCE63JNLG -->.. KX7zUQIBAAIBAAIBAAIBADAxMA0GCWCGSAFlAwQCAQUABCBzAXdbBfjvkCEN -->.. qK7Ym3r0lwef2vQhN9zidTDdkf

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ProtectionManagement.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	725240
Entropy (8bit):	6.056118316914494
Encrypted:	false
SSDEEP:	12288:UqjFjzbVd9Y5TFXnu5aHOf/gehVtN41D3mRy46WegMZ2:XjzbV7Y5BUlN4t2Ry6Ug
MD5:	0F9485E242400DC47A9FCA73A3443120
SHA1:	1BD457062BE7B37EAA252C238A9B3BF4EFFF0485
SHA-256:	8DA908D6AD4F307D6AAF8CFB1A9C27B3F3A285F84B1F3C817F50D7B154DC575F
SHA-512:	B2A83A997985CC7FC5D07705E49BCC96BD9E0382CD4BB722C4EBBA3B35EE793C6507DA94AF23B276CB0808FEB7233A37A7F72CCF5974AE607186831AA5EE5C10
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ProtectionManagement.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.....V.....V.....V..J.....%.....Rich..... ..PE..d...O.5....." .....`.....U<....`A.....X....P...O..... .....F..<...p.....(.....8.....t..... .....text...UX.....`..... ..`.rdata..vI...p...P...p.....@..@.data...T.....p.....@....pdata...O...P...P...0.....@..@.didat.....@....rsrc.. .X.....@..@.reloc...F.....P.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ProtectionManagement.mof	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	C source, Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	91754
Entropy (8bit):	3.59234124916807
Encrypted:	false
SSDEEP:	768:lv7JczQMzhFbvZbY6qyZ+v7JczQMzhFbvZbY6qyZg:RMhWyUMhWya
MD5:	D9619BB89523F47C88DC5FC8BEA50BA0
SHA1:	279098ECBF269FC91585A8D0F7F5A1C72AD2101D
SHA-256:	3ECDCEF5A04C90CA1EB296F3AE4F1C5BC96C371E84BE927C25FA64D6C74C34AF
SHA-512:	F110C9824D5CA8718A4EDA5968DC7DEA7B1C88A498CA2F7706D873D3B6C87FACF8E2ABE7BA20BEF033B8D0322E790C3B0F8CE288166635AE11857B367B9BB9 F7
Malicious:	false
Reputation:	unknown
Preview:	..#.p.r.a.g.m.a. .a.u.t.o.r.e.c.o.v.e.r.....#.p.r.a.g.m.a. .n.a.m.e.s.p.a.c.e.(.".\.\.\.\..\.\.r.o.o.t.\.\.M.i.c.r.o.s.o.f.t.\.\.W.i.n.d.o.w.s.\.\.D.e.f.e.n.d.e.r.".).....I.n.s.t.a.n.c.e. .o.f. . _._.W.i.n.3.2.P.r.o.v.i.d.e.r. .a.s. .$.p.r.o.v.....{..... . .N.a.m.e. .=. .".P.r.o.t.e.c.t.i.o.n.M.a.n.a.g.e.m.e.n.t.".;..... . .C.l.s.I.d. .=. .".{.A.7.C.4.5.2.E.F.-.8.E.9.F.-.4.2.E.B.-.9.F.2.B.- .2.4.5.6.1.3.C.A.0.D.C.9.}.".;..... . .I.m.p.e.r.s.o.n.a.t.i.o.n.L.e.v.e.l. .=. .1.;..... . .H.o.s.t.i.n.g.M.o.d.e.l. .=. .".L.o.c.a.l.S.e.r.v.i.c.e.H.o.s.t.".;..... . .v.e.r.s.i.o.n. .=. .1.0.7.3.7.4.1. 8.2.5.;.....};.....I.n.s.t.a.n.c.e. .o.f. ._._.M.e.t.h.o.d.P.r.o.v.i.d.e.r.R.e.g.i.s.t.r.a.t.i.o.n.....{..... . .P.r.o.v.i.d.e.r. .=. .$.p.r.o.v.;.....};.....I.n.s.t.a.n.c.e. .o.f. ._._.E.v.e.n.t.P.r. o.v.i.d.e.r.R.e.g.i.s.t.r.a.t.i.o.n.....{..... . .P.r.o.v.i.d.e.r. .=. .$.p.r.o.v.;..... . .e.v.e.n.t.Q.u.e.r.y.L.i.s.t. .=. .{.".s.e.l.e.c.t. .*. .f.r.o.m. .M.S.F.T._.M.p.E.v.e.n.t.".};...

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ProtectionManagement_uninstall.mof	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	C source, Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	2570
Entropy (8bit):	3.4549784303178717
Encrypted:	false
SSDEEP:	24:QXbclfUWvlDQzj3WvlDQzCWvlDQzwNWvlDQzYTYWvlDQzfWvlDQzyWvlDQzEWvl5:eTjDGwJ3r24RFZ7a2la2Sa2mWaWP
MD5:	72D045707D108D55B76CD70AD9A84AD6
SHA1:	8FE25F4F289302A49CF2FA0F962FEA4D7D82FB8A
SHA-256:	30A0AD834D7B3F4FB47010B4BB6905576792E83064E9DD858EABF0CCA17FC3DF
SHA-512:	E3C6F3F931AEFCF1F0B1061B7355451692AF1F459F8ED13C39B03951A6A3E833AEBB1031796B5D806C615D3E84C178D628B10AB5EC5CCBC50935CBB0D584FA5 0
Malicious:	false
Reputation:	unknown
Preview:	..#.p.r.a.g.m.a. .n.a.m.e.s.p.a.c.e. .(. .".\.\.\.\..\.\.r.o.o.t.\.\.M.i.c.r.o.s.o.f.t.\.\.W.i.n.d.o.w.s.\.\.D.e.f.e.n.d.e.r.".).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.C.o.m. p.u.t.e.r.S.t.a.t.u.s.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.E.v.e.n.t.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.H.e.a.r.t.B. e.a.t.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.P.r.e.f.e.r.e.n.c.e.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.S.c.a.n.".,.n.o.f. a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.S.i.g.n.a.t.u.r.e.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.T.h.r.e.a.t.".,.n.o.f.a.i.l.).....#. p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.T.h.r.e.a.t.C.a.t.a.l.o.g.".,.n.o.f.a.i.l.).....#.p.r.a.g.m.a. .d.e.l.e.t.e.c.l.a.s.s.(.".M.S.F.T._.M.p.T.h.r.e.a.t.D.e.t.e.c.t.i.o.n.". ,.n.o.f.a.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ThirdPartyNotices.txt	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6717
Entropy (8bit):	5.162252158398129
Encrypted:	false
SSDEEP:	96:+WRspYDLPkQHFom1DW4DlHFposoSKYax9gDCk4Cp1PRsQHdBLe:DaVQHFB0AlHISKYoopoQHdxe
MD5:	CE7313760386B6ABDE405F9B9E6EA51D
SHA1:	F969931AC45991F7ECB6767A69433A7082ECCA2F
SHA-256:	73E26404B3571A9E859B3A1144F54C353172479586E0A23C3A7DDA0C1C0AE919
SHA-512:	CF990FC05FD3ED78FF35F1A1ACD5317626D46745BF7E4F8C62AA068A587ABF52F232080464F82692A2BB8C04A4FFA53599B933A4281BC7E697337720DB65BF29
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ThirdPartyNotices.txt	
Preview:	==========..1. C++ REST SDK (https://github.com/Microsoft/cpprestsdk).... C++ REST SDK ....The MIT License (MIT)....Copyright (c) Microsoft Corporation....All rights reserved.....Permission is hereby granted, free of charge, to any person ob taining a copy of..this software and associated documentation files (the "Software"), to deal in..the Software without restriction, including without limitation the rights to..use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of..the Software, and to permit persons to whom the Software is furnished to do so,..subject to the following conditions:....The above copyright notice and this permission notice shall be included in all..copies or substantial portions of the Software.....THE SOFTWA RE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR..IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANT ABILITY,..FITNESS FOR A PARTICULAR PURPO

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\af-ZA\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29928
Entropy (8bit):	4.969613819843474
Encrypted:	false
SSDEEP:	384:7r/SmH7frhpOJsSYNEYffu1vB+sEqEKSTs/WS8/WWRDBRJZ4UslGsV7:7rbHnZNEYfPDR1PV8
MD5:	2A54A6EFE0D70D2F8120E4F9AE10F2AE
SHA1:	35DD602C81E5E1E086C093BB3C3F97CC68FA2FD6
SHA-256:	F90B4913826DA577A68006FC7211E2390534BE9639934AFC5A375436373B1C71
SHA-512:	8AE2DCEEF670F26A753B1525FD126DC4748A5124B94F5B8ECB632E2A55A2B3C709146C40C936806CCFC64B804A1FF23E31C47293ECD4FF524F5CDC86320D205
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....R .....p.....*.....@..... ..DN.....T.. .....rdata..p..... @..@.rsrc...DN... ...P.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...I...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\am-ET\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22264
Entropy (8bit):	6.043832073272478
Encrypted:	false
SSDEEP:	384:7raKntNfzRKLpPExWUN7W0WVQB82s/BW/pQWS8/W4RDBRJvsl5D2:7r1ntNfzRKLpcjfRxR1Pl
MD5:	F5F731716CA6C6CEFF57DEE03EB33376
SHA1:	FA71CD3569AD3C6518E626E09965053F58AB6D9D
SHA-256:	A2E33041860906CEF0BCE5B2F3FD2AF88E3DB61E97FF9EB16D650CAD1F69F708
SHA-512:	FCCD58F3A698CE9668322C76140E8FE55B2F484962D1A9B51828C00C3CD888D85EA83D3626993B50098271B250DDE6783FA129E5225153112781D5565313553F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....4 .....`.....@..... ...1.....6... .....rdata..p..... @..@.rsrc....1... ...2.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...-...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ar-SA\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	58600
Entropy (8bit):	4.802281589367443
Encrypted:	false
SSDEEP:	768:7r+0QI4V/O4klevfq7mvqaI216icZKfEflxZFcR1Pga1zR3:qCcHPVZ
MD5:	628870D988EFBFC39C06E7BA62495FFE
SHA1:	A3A302666A07A5FE0D7FAD69DE9B1AFBD8F91536
SHA-256:	161D58719676884DB3BDFEA9A5770A55EC7BEBE839D97B6ECA3D20EC5A3D6B2D
SHA-512:	E04ECDC7226C9B18FC86F51F6B70CD6E13345C8F2A8DFEE0845350777580CF46A738271E949B07216D83A647685DAD3666A7F5C2BA36451E11DB1545AFD9F7E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....:2....@..... ..X..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ar-SA\MpAsDesc.dll.mui	

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ar-SA\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	25320
Entropy (8bit):	5.568099766445783
Encrypted:	false
SSDEEP:	384:7r8teWannr4pG2RI96HUy/oV/m9HlCWS8/WWRDBRJWiZEQmDWlGszRo:7r5nnr4pG2RI9AoV+9HVbR1PWJ1zv
MD5:	53F858DC25ADF3684E7E025277A57023
SHA1:	A51A05FFA31010C1B28A63B5B7BBB490239BC1C6
SHA-256:	D57524C7B0D7FE779DC3803F041C341F818381E19703D32BAA988F1697D1175C
SHA-512:	0A7E6808CDB2EB6E31596218FE42B2BFEE9B067B22913D43A1E1C1D5B1832C3018B04FC633E8F92233782163722359 88FE15F2D9FA074AC595046542FF54B9D1
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....@ .....`.....@..... ...>.....B... .....rdata..p..... @..@.rsrc....>... ...>.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..H9...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\as-IN\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29416
Entropy (8bit):	5.632188784867651
Encrypted:	false
SSDEEP:	768:7rOPaPbPAPCPLTPnPWPkP8Pe1lOO6FD6kKOy6OQOQ4LuYz3KUrZPk/4hPrPDV86/:xcNgPHPwc
MD5:	D359F26A958650D3B5A28495DC39D409
SHA1:	3EF8B8E1C4E876E1C2A6157AE92C65E629C7559C
SHA-256:	F2A33F57BED6013E9850AB150C83577862DE7FADA3CAA1C87C94100F486D92A7
SHA-512:	0ED71E0EA79B7AA96E8358B28DDE2C7C419C526168271355AA73C281BB123E9306FE1F3A94A1A9A7BBD4234E54CB0760BA31D6BBF5E13BEB8305460000C3685D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....P .....p.....@..... ...L.....R... .....rdata..p..... @..@.rsrc....L... ...N.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..(H...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\az-Latn-AZ\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28904
Entropy (8bit):	5.231249488030954
Encrypted:	false
SSDEEP:	768:7rOj1wdJ4v3YFcFqFkFJFgFGFYFhrVbFRdtR1Pl/DM2:Gj1gFcFqFkFJFgFGFYFlVbFbtHPl/w2
MD5:	06A297C9B8293DA4AC3B56D304874F2A
SHA1:	A7B7F072E7A7A5837382293CD65ABF10088E6EA9
SHA-256:	C5D1763D4F042FE777BB02E47E26F76EC9008AF689679BDA6480E1541A1158BF
SHA-512:	AB2C0EACEE65A2CC104DE75C86311374227E3E91E8BCEBED89F729B07681E2A79D88BC73F507C471666FCE8753DC18E83C2C37B27D8088D1563EC8634B05EED8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....N .....p.....@..... ...K.....P... .....rdata..p..... @..@.rsrc....K... ...L.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...F...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\az-Latn-AZ\mpuxagent.dll.mui

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\bg-BG\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	64744
Entropy (8bit):	4.650844920332313
Encrypted:	false
SSDEEP:	384:7rTz3pDQHT+ddcOc1jzG/by+psEV++OfYcYQIhJ2YIqqO7a1BQdWhjRDBRJ4NKgY:7rtuDOYz01TO29VqhQ4jR1P4tl51VQ
MD5:	DDFB72494C7DAB2C2DCBBF58F1384BB8
SHA1:	474F7CDEDFEF2B0E5765B5EF151A8DEA7845BE68
SHA-256:	7E28FA6FC9DD05652F3DDCC4B9BC54469DD44995EC69EF149B9477B4C0CE53D6
SHA-512:	6AD3EBF149C1C9A5BE7FF012A2AEE38DD6D2EFADE2EE73E1F41E45393180DA13BB1FB8E079E6D8CBE5D51259A1D57351738D037A3589FF50CF7577C372A1C5 21
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....H....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\bg-BG\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29416
Entropy (8bit):	5.351887592007768
Encrypted:	false
SSDEEP:	384:7rTpJ4DyEhyXvb1vstW33294WS8/WPRDBRJfJs/Al3lKO:7rV4huvUVPmR1PK/KO
MD5:	6275E196D18A7E2E298B30AF3ED5C880
SHA1:	240364A589E90A9DE843CBB9C34555A2E4274793
SHA-256:	06B162090901AC0604283E1CE2EC1928E0A7C651332C3E7BE593E438DB02AC88
SHA-512:	54BFC5FA5D4DB45538E0C60454AB1E58371338C982496A19485BC76A3047E0264F2B30070B5A4E1A30B865FE38A95FF36C758790E5B8C8EE5B8ACEAFA200AEA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....P .....p.....@..... ...M.....R... .....rdata..p..... @..@.rsrc....M... ...N.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...H...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\bn-IN\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29944
Entropy (8bit):	5.555067530565591
Encrypted:	false
SSDEEP:	768:7ruX333303MqF6WVHrS3snXlFwDzffQ6SMn6vvvU98Io/PI44te1eF3r+YR1Ph:F64HK7+YHPh
MD5:	231D5D0EC76C7498E5A94E120943699F
SHA1:	D8DF8518946F02F5C51860983188C574B10A9180
SHA-256:	1807A40E971F9A586671F144CFB34404D2AFAA027EC9E670E323BA70577FC9E4
SHA-512:	E62D8578FA404E1753CA5225AD6DBFDA8AA392B4340C4DCDE8E310CAE522A4960536AD9192D8A18DF47030C8380056D896ECC378A84F3EF9BA2192B6C7DC00 4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....R .....p.....\b...@..... ...O.....T... .....rdata..p..... @..@.rsrc....O... ...P.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...J...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\bn-IN\mpuxagent.dll.mui	

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\bs-Latn-BA\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28392
Entropy (8bit):	5.05898751052722
Encrypted:	false
SSDEEP:	384:7rgBdq0HifHAHyuJv3JSF666n/o001ZAGmIbmLWS8/W+RDBRJilSlGsM3k2:7r8dYuJYyn/oVv3zjR1PihX5
MD5:	6C4B5C9E187A6B13C39FAA41C742EDD6
SHA1:	30A5B3B8826EE8741CD09D5AD65D6BAA2DC68BB0
SHA-256:	9C776358CD7A47CCBA26F992472A0A739C6F0C152B89B5AEDDCACA8AC43684F0
SHA-512:	16E9795DD6EF63CACA9C7D7E96BF0CB2C0177641213F387586D4243E159E6464B1E736A1892071B80433F7F825A0530CEEB72EBABB4F4F7EB3802879AFED916F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....L .....p.....@..... ...I.....N... .....rdata..p..... @..@.rsrc....I... ...J.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...D...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ca-ES-valencia\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29928
Entropy (8bit):	4.978741308381524
Encrypted:	false
SSDEEP:	768:7rleQQmmfwxJvYOmnVmJYlEmnVY4mxYCOAlc50EsUpVJg94T4OCaTR1PD/1zx:9eFlNTHPDdx
MD5:	C9E9AE82C7782DC0E66BFE5EFEFF336C
SHA1:	676F16943FAB27A375C2E3F3AC0CE921AB751367
SHA-256:	CA202FDD69FB81DBF24708D144E942FC10ACCFA4703BE979AAD55FD88B62E7F6
SHA-512:	AE90BB4093A1879E8876D45262004AD10FCC9BE13D4BE1F9164C866827F2C48C28CE170274CDA4D0C13C3CE2EBF8106E5D374300F51EDEDE6E580F38BADD75 A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....R .....p.....@..... ...N.....T... .....rdata..p..... @..@.rsrc....N... ...P.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...J...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ca-ES\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	67816
Entropy (8bit):	4.158464028484954
Encrypted:	false
SSDEEP:	768:7rDj4mcWQ7uhqYxT352UL2dSsq5/8Vczyuz9ppJ4cwQRMC20hvQii98+wEH4cdqd:7WQ170VcfRMZgqHPO/
MD5:	D2A485200AE94654A45301149D87A8A1
SHA1:	501C933C5BC3D5DC9AFADC86FC73D1567DCDADDD
SHA-256:	9164442B33BAA1DAAF4609189D8169CA9DFA67BB673683F66A49ED9145DA7585
SHA-512:	7D763413C96FB4197216F03028046A510E5393EE9789E827DC9665243889491A05E8A4ACDAF813E3E8773E5E952F53960C02AC86FBD4C83EE402B5DEF44CD17B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ..T..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\ca-ES\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29928
Entropy (8bit):	4.970820382866816
Encrypted:	false
SSDEEP:	768:7rAjdTb3dD4GbRVgWV9Hw2b4HX4bi2KwNDFWhGWD3IDRU0MZ8HoR1PX6Lz:Yj0KoHPKf
MD5:	0EC7F6A6BDC86183AA58893F948989A2
SHA1:	ABFAB912AF53106A82CD50158EB147F5EC4A3456
SHA-256:	02FC3320529F9A51D88030CE7C03AC3A62517B8141768FE001B995DCFBB202F4
SHA-512:	CD6FC83F8F2A5F676ED60655BB607D2D6DA7D4A274A809D1CAB0854B2257E20CD7D4E0D0FC0C1A1AFD4D2E99F8F0A99A7B89C2C2EDF2F741F7DED7B3AE1DAD1
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....R .....p.....S....@..... ...N.....T... .....rdata..p..... @..@.rsrc....N... ...P.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..8J...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\com.microsoft.defender.be.chrome.json	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	350
Entropy (8bit):	4.8011887903612696
Encrypted:	false
SSDEEP:	6:3HWSjKNde/Ott+dmvVnEuLrORVCqwvFFaFlLulkNCB+SrxxLxeNCWHyLIo:L2kO+WnEeMOUlLAjB/1N/0o
MD5:	60A2FC65D3CC1D3DE9ECD2C5319738FC
SHA1:	873D18E03523BBE80D1410AA475ED6CC2DAF0D9D
SHA-256:	6C6F52B13235148AF305BD614779EA885C00B64D0BB7CC764E3C67198CC524A2
SHA-512:	36E8930108DA1B953DC07809A9E670F923A4F07EAC9AD2A229844E556595CE7383F35001E43AA6877FF42D9BD42C55BB2BF0ED05E058D4E8CFF65E6B2B7A7BFD
Malicious:	false
Reputation:	unknown
Preview:	{.. "name": "com.microsoft.defender.browser_extension.native_message_host",.. "description": "Native host for Microsoft Defender Browser Extension",.. "path": "mpextms.exe",.. "type": "stdio",.. "allowed_origins": [.. "chrome-extension://echcggldkblhodogklpincgchnpgcdco/",.. "chrome-extension://lcmcgbabdcbngcbcfabdncmoppkajglo/"..]..}

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\cs-CZ\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	62696
Entropy (8bit):	4.4300925979744425
Encrypted:	false
SSDEEP:	768:7rpChXzlbrS2tVdqSp3wbjfKMoW4EEEddewzR1PiM5md:hChXz1Lf04SjfKMoW4t8ewzHPlmd
MD5:	71EA670E1886321DDDDF005D7B47A7FD
SHA1:	FB9AA4F04C6744123C2E38DE746983C1B82A6F00
SHA-256:	BC031DC51AE7128AEE1ADCCDA0F7ACC9EB3BBE8DE121B206B0E9801E956F82B7
SHA-512:	3BB516F32FC0516DE97CB520AED0E3976BC201183144AF54FF392BB73237767C50794F923C84E738D82A7430C6660EE7301891CACD1517F17DBB6C6391B46070
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....+....@..... ..I..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!.....I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\cs-CZ\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	53496
Entropy (8bit):	4.606804840809272
Encrypted:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\cs-CZ\MpEvMsg.dll.mui	
SSDEEP:	768:7rdMyciFk6/zRyodW7/obSxnjEBIR1PbzT:lMyciFk6/zRy+bSxjwIHPPT
MD5:	C40C173214A061E8BCDF28F6328CAD40
SHA1:	A525D0203A18D9011712A7F6AD89FD84D90B5747
SHA-256:	17B281694628800A6B1541826B912F8FF0788D171A900F6DF4BA8A6AC01B3A46
SHA-512:	B72D26D86B1D28308686A1DD0AE513594D9875AD809C891B9B0632207484701548465339D25C89B4EC904F838AD47B0438EB22925CD7C2E70C3686961476760AC
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@.....8.....rdata..... @..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4] .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\cs-CZ\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28408
Entropy (8bit):	5.215365684019082
Encrypted:	false
SSDEEP:	768:7rIXE4QWX0YNoE8gZ04pC5DbUV4qFR1Peizz:Q04QWX0YNojgZ04pC5DbUV4qFHPeYz
MD5:	FFE6628B2AD343CDA7FDFEF38B84B48C
SHA1:	36A72C17996D63635B184CDEC836022A2FD275C7
SHA-256:	B5E81F2E96B81367B16D77BDB21FF45C92B880DF501AD17FEE4F8B1E756C636D
SHA-512:	B20694CA2B5E009BCD981C8FD3E95CF25E16E9293001CCCB53DEC2ABDE6A31535F9213492279BB9527DF0A86B0489DAB7014F3F2A67A3D6D26F26DD1B942B41
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....L .....p.....7....@..... ..DH.....N... .....rdata..p..... @..@.rsrc...DH... ...J.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...C...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\cy-GB\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	30456
Entropy (8bit):	4.937872667222882
Encrypted:	false
SSDEEP:	384:7r9i3aB5tg/hPb1Y2YQYTZYxgaM3cNqng73m3cX3u3cjgTyTKT3TsjxTPTBTnTb2:7rhXP9KV7XcdLks3yRR1Pgz3
MD5:	CF1FB8FA2725C2DC530AE045F1ED8A6B
SHA1:	B64794C057E7F9F1F4A5DB0A9164FE21EFB32151
SHA-256:	EEB5D85389F768042AFEB2B1203BCC151069F53DAFED28DB404122013041241F
SHA-512:	259CC37B8488D7B9244450864F4AD2ABDC9A7C8355833F5A1628D5DC4A3123A2FCDBDCC2B8169DA2613527D8885C081915651B41228DEDAC6E5E70D1CC4F9CD
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....T .....fT....@..... ..TQ.....V... .....rdata..p..... @..@.rsrc...TQ... ...R.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...L...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\da-DK\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	63720
Entropy (8bit):	4.2102783984881755
Encrypted:	false
SSDEEP:	768:7rRXQqbVuA8rmOXbO5OKi9OUsUR1P11zf:JXQqBuA8b6UHPPf
MD5:	BB1447340673FA9F6B96A9987290F278
SHA1:	C43D250E3BEF83C88A2BB5EA7FA68F54895C2FA5

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\da-DK\MpAsDesc.dll.mui	
SHA-256:	A166D52AA0AB379DE33CF5796A5B1861246A36BB8B17D8C87E0F0529338C0AC3
SHA-512:	F0D83F03C31E45C079E1ADE32A4801A6C5B8F71D23421E6D08C655E1216F4A6A3E58F8930C1F3D72CAB8FF25536017D2F1D458FCB97FB848E83830B331A3C3C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....K....@..... ..T..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\da-DK\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54520
Entropy (8bit):	4.3994496582380975
Encrypted:	false
SSDEEP:	384:7rpjcx80WKqt9o5uDwepIRXVCQECoz0NKERDH9rLdGtKWfwLW6RDBRJiOhl95UN:7rWxnkErR1PZzUN
MD5:	849192FB21F761073C9ED4A3F5BD4688
SHA1:	A9AAA641C02833616CC0165FA47499DFC1269D7A
SHA-256:	1EAC8A8C05B8AAFB4505A7828D7E7F98567BD0C71DEE4E08AF467F31D34A9828
SHA-512:	F5216D11DC25B246567A1F31B1613533EB57A28FC88AAF7D1064426D6E9488C597F5F3BC7DCA29D3FEC4D239EB86675476488EAE4309F239649740F9D739297E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....V.....@..... ....8.....rdata.....@ ..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4]. ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\da-DK\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28904
Entropy (8bit):	5.034399544515469
Encrypted:	false
SSDEEP:	384:7rV9LJoeS3TVu8td5dCWS8/WtRDBRJjfVslGsJ/Qw:7r7LEVHJlR1PjzLw
MD5:	C63C9C4C55D3B4172BADC2FB45014D5D
SHA1:	DC46D629995E862BA72C80ADC45F62DAD3590728
SHA-256:	88346BDE6D5FC1C0CADFA5755944F466F8960C9CC17A5339851A2BAD42376C70
SHA-512:	F838B0338C194BA2E820B10EC4E2397511AE61A14C6684AF99996DCABED5D225F9672BC4053DF9AAB6F2D586806908DC07BA43C2ADC191081C5F3E5D58E1485D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....N .....p.....@..... ..XJ.....P... .....rdata..p..... @..@.rsrc...XJ... ...L.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$...E...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70392
Entropy (8bit):	4.18694461018496
Encrypted:	false
SSDEEP:	1536:g9J3VugBgOPS611GRF9QRquPJAQ7GyHPvt:g9J3VugBgOPS611s/QRquRAQ7Ggd
MD5:	FF00B121B166AB8E4857EABE4AAB9BCC
SHA1:	8CA305D4979F693BCC8425A972438A9074B92C5D
SHA-256:	9285FDDC5E40919E750A95C255588332876547495F6E245BAD983D612DAA4704
SHA-512:	2CC52CBB0EDCAD8BBAFD934E3B259048250F0DF4687FE8FC3F9B3764071F5E1E708FA870EB91D8868687F8A91677C9EBA287AAC195478C613042C97B3349528
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\MpAsDesc.dll.mui	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ..@..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54504
Entropy (8bit):	4.451774666927673
Encrypted:	false
SSDEEP:	768:7rBOW84CvPTO3VUtmUz8J0GXv3Y1VKLhR1P+pa:v84kt9qAohHP+pa
MD5:	7AF483C2AFFDD95213DDDC495D001DC0
SHA1:	C65458CBD4209A7B09129D5FDD171C758D6A7991
SHA-256:	155EC9FBBE052BCCF189B89EF0F802DA48547D107A26A9E342BF9A23B4F1ADFF
SHA-512:	6DF51B3E38AFB35BCAA066F3DDD56497B9E104D768C5AB1348A82BB7F1B70ED332CACCF302699AA97CC3095252B915F209BAD52F2495A31210CF90DF194020 F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....S.....@..... ..@..... .....8.....rdata..... @..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4] ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\ProtectionManagement.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	53480
Entropy (8bit):	5.4939020981100315
Encrypted:	false
SSDEEP:	1536:OEH8Kt3U5Pfr9Y5BKqpdmXD6pyFJz1Z9YRHPdE:OKRmpYCmmXXZ9YdS
MD5:	381A9FC19B05718037AA3A552715C54F
SHA1:	01DC93DA9A279EBAC49E7564035849AE3EF4B151
SHA-256:	EA4DDE3088A05BA4A894FB81A8ABF0769DB0A8F79F9D1E5E96BEB916610710C4
SHA-512:	423EDF0088AAF42334F097F7687D964E27293AB508AABDD5A3FF7A2F89E9AB4145FE7BE9FC9E0A00C450F8DBABA2F841252EA9A8A0F7845090E84AA17E5BD34 A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....%..H....rsrc$02.... ...=..E.....'G.:3..t.E... .R<I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	31480
Entropy (8bit):	4.903514449361369
Encrypted:	false
SSDEEP:	768:7rf5229Ah0vyaffaXQQOvR8PMFXNJSMbsHrWzxWaNnmeduHJJ17CpR1PPGLh:n5229Ah0vyaffaXQQOvR8PMFXNJSMbsT
MD5:	16C6FFA34E0C59EE77F916EBF9148AFC
SHA1:	C82E4308AC0A909BF4387B86B62320DA9E1FEF51
SHA-256:	6EE8E608A103E991460B51D87AEFCA126EC8744642559B536F70330A848CFB08
SHA-512:	782A0BEE60D339B86A176201C84A8AE117458C1688AF3D0089696ED8124E2006676A91C15E117904FE1FBBF6E4F72D248E75086E9E24436E16CFE458E8521A8E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....X .....@..... ..@U.....Z... .....rdata..p.....@ ..@.rsrc...@U... ...V.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..xP...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\de-DE\mpuxagent.dll.mui	

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\el-GR\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	75000
Entropy (8bit):	4.68621286355812
Encrypted:	false
SSDEEP:	1536:c3yX1MSgKNnNL+/euj7eCMEE+gL8hKfGujCCaCa52HPJ:c3yX1MSgKNnNL+/euj7eCMEE+gL8hKfH
MD5:	53B61803FB8BDC469ED5D04FB8983233
SHA1:	FB801EDEB5CCBE9E75C2CBA7A28FF05BFEEA270F
SHA-256:	BE1609A94963D07A591C7D38947B28AE79A9D070385E70BD594A1DBD6DF7EB31
SHA-512:	678F7D40E6F54A481353FF0C7AA1C21FAEC66C8B05546CF9AC4B2372EED51918A53A0D4509C12A7DC6B8B2175A86C19C84C5274735560AA2B62B97347A5E279
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... ....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\el-GR\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	60152
Entropy (8bit):	4.994721555651978
Encrypted:	false
SSDEEP:	768:7rpd0tgeGeGsnEstzuFtGFil0a9+R1PEcz3:OgTsnPtzuFtGFil0i+HPF
MD5:	9B6F194F0D0EB1ED21B000E07B0CBDCD
SHA1:	FB2E6FF6B553B1E25C142FBD5CF868B98A0E8C2F
SHA-256:	E1A7E2391FFF39162293DD3AE201ADC393D8CC91E83A4B33C2C9A089EE69D203
SHA-512:	F64454892E8E12A33A887CE930A6DFD708CDDD1F76CFEFD909D5AA6ECF0098DB49AC263F4DD2C601A7A12FEC6221F806C4035A5EC8C928CC785550D644720E 0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....(.....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4] ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\el-GR\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	30952
Entropy (8bit):	5.453443722839373
Encrypted:	false
SSDEEP:	384:7rqYFfMlN2vyRBNd/gy0b5DYpOLjNB4Okn8OM3mnUJOeTPn5yLOe0FZQiJZhFD7a:7rP6EBZa2z6R1PV/rF
MD5:	222D67D112493530069E47CD64364BAF
SHA1:	F4F6F74D62470C5301BDC537ADC451FEAFBCCEBD
SHA-256:	B6E4B5BF805802069890DF5FD769D48F370620E607809E48E233C78EFE6F90F1
SHA-512:	4A8EEA2ADEDFC1E7267E13F369F50E17AE2A578E28CC15C248F54444925D0196F509F8FF16E8011DC30EB28A8A3E9620F0716E27B50D6933B1283433BF2A88F3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....V ....^....@..... ...S.....X... .....rdata..p..... @..@.rsrc....S... ...T.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..@N...rsrc$02..... ....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-GB\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	58600
Entropy (8bit):	4.25269307683972
Encrypted:	false
SSDEEP:	768:7rSJb3XsmqEiqcTr247sEBhEChEehELQRQ4hEYDGR1PYq:qJb3XDqZqc/7skv7rfGHPYq
MD5:	8DE66C308CA2A9340CC9E84F753FAA56
SHA1:	8D70F8339E74BD7730E0E876D3B23412CCB1DA63
SHA-256:	AE6A41CA40A926287BCC94503AC9AD42568D6BB62B4CF2DF60F0599FA9E988FF
SHA-512:	E0E6D0919E21049618E23F7850F83015A9EBB2A802EED22A9ED547421552F3BD2AD3B76BBC66966BA935EF5A152B235EB4A4D5C60379CCA4A2223D5514674ED
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ....8.....rdata.....@. .@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!.....I .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-GB\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	27880
Entropy (8bit):	5.0955466583627835
Encrypted:	false
SSDEEP:	384:7rTHD0EhR32NSWS8/W5RDBRJqH24rlGsQhJ+:7rbYhtMR1P26LQ
MD5:	DD65190763621E8E1B642A4305D5E801
SHA1:	D9BCFD1CBDC637B9F1211BADEF89F55B8C19D1E3
SHA-256:	8CBEC55311F2B7234D1FBD9C46AB6CF33A165610960132FE73C19FF725579658
SHA-512:	C51D7DC6B9410AFE72BD2C65989469FFF3ED6B41C5D5C9ED1320EEAD78742B840CED18C2B479DB06959B9DF69F28C116B047AE8D4A5ABBF3AB9546713E878 7D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....J .....p.....R....@..... ...F.....L... .....rdata..p..... @..@.rsrc....F... ...H.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..HA...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-US\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59128
Entropy (8bit):	4.293356301291751
Encrypted:	false
SSDEEP:	768:7rxiJbyt33aEhrdTTm147vXahEzhEthEGQRQwhE3DbR1PR:5iJbytHa6rdd7vM+4ImbHPR
MD5:	BC78A3B5260E268C292724EA573194F9
SHA1:	02D4A4E683609B5B61834520D27B138EF3F9F7C4
SHA-256:	2C4B8F48370B6ADEA49A21F2D89F2400E54C3EE937120152B50A94FFE5F5F7A9
SHA-512:	985B104584656A099A5C20C85C77488D2575CA518353DF585B99E37B0596A46BFF5C32DF197A823569BF6909755406C48B9D41861A1C4A947BF1FE616519AF90
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-US\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	51944
Entropy (8bit):	4.448866330393985

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-US\MpEvMsg.dll.mui	
Encrypted:	false
SSDEEP:	384:7rsorOioFEr4H1n3/Dtkby/g1mwhqfB9hyINcNkHoal34Y0wNl8yWucBW+RDBRJD:7rcBH1/b4Y0wNl8Cc5R1PeX8
MD5:	0D87F3932078B4049523B8CDD3EE5692
SHA1:	EA172545FB8E872BE0FC9AF0B58C3FA8CAF6F970
SHA-256:	46022C8F7CC601BF73D231C213612BFAED0E95A76BC510DA08B7323EC1CCB2EE
SHA-512:	51CFF3304353B5992D63C2F0C1CA71ACD74E3A4E8EF009B525BD6720BA4BCEA83A212516E41E086AFDB74E7A36DE0E4674517CAD84D8EB2E7545E34773D355 4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....}(....@..... ..$..... .....8.....rdata..... @..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4] .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-US\ProtectionManagement.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	52456
Entropy (8bit):	4.449895321849691
Encrypted:	false
SSDEEP:	768:7rypn9K/Gd67WzUi+YXCujpbemXuQx/Vhjhxp1ZR1P4M8/GQT:ap9KOPZXC+XLjZHPQ/x
MD5:	57DD5DCD626332FA892BF1526D09C1D9
SHA1:	B0D2C0D3CC46C7E7F560D11117C5DD7C2817AF5C
SHA-256:	385171BD15127FB8546EF4378CBEA2BF25F5063E6E731DFEB4EF868829FB25B9
SHA-512:	4F59C6E5DE864D07A675ECA116AB308C25CFA67EBB8345376FC98ECEFDA49CBF0BFD96A7371E398EC661E7F546C84C49D6E98556F767B32432E03BFFED04C2 8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....l.....T...8...8.....l.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....%..H....rsrc$02.... ...=..E.....'G.:3..t.E... .R<l..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\en-US\mpuxagent.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	5.027883032614938
Encrypted:	false
SSDEEP:	384:7rHwnD0qkg1Wl+R0UdhR3ZVdZFzd4SWS8/WNRDBRJbQl5c:7rQnYqkg1Wl+R0U7VXFzdOIR1PbT
MD5:	FEA5726C8962F98A3601E47EADB5A3E9
SHA1:	FDDCB373EEC6E22B7706A588CDDA4F0822237538
SHA-256:	FC18C509866893EB03BC82F49C0EF07C344640CF8D6FA3963247ABB7521A4A56
SHA-512:	CB63D5656B1822668285B6C1B1594BBE1B364EF45AC4C5618D7C436C93BD38623B06140383DE58A610EA7FEB92BB741AC7477AAB104A0CCBF671125D2D83CA5 C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.]..S....\.S...Q.\.S.Rich].S.....PE..L....JVa.....!.....H .....p.....@..... ...E.....J... .....rdata..p..... @..@.rsrc....E... ...F.....@..@.....JVa.....T.....rdata.....T....rdata$zzzdbg.... .....rsrc$01.....$..@A...rsrc$02..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\endpointdlp.dll	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	647416
Entropy (8bit):	6.2677434000059975
Encrypted:	false
SSDEEP:	12288:RE74OZLauRb4Z7W42oza9hlXTzq+g57U2ibvko43Shu/6U:toLauRaWMTPg9U2ibcH3SU
MD5:	BBDFA9DA2F8E10903C095F504A2188B1

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\endpointdlp.dll	
SHA1:	E670D3739742A460C8C3AA5A2CC911A4ACFEFA8D
SHA-256:	4B3DE446F41D0410C06E9FAFF8823D380BCBDADB5B381C702CE3A5E2535A7142
SHA-512:	A30280A65726142551F2CBFB3A41337B309BDBEABCF710B5654CBD1415453AD2D69A7EC7C753A4E297557755D4204CABA4881938F805E667888523CD99F338FF
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M2`..S...S...S..!...S...S..S..!...S...!..+S..!...S..!...S...&...S... &..XS...&...S...&...S..Rich.S.....PE..d...+s.P....." ..... .....`M.....|....`A.....(....`...K..... ..... G..p.....(.....8.....text..... ..`.rdata...m.....p.....@..@.data....9... ...0... .....@....pdata...K...`...P...P..... .....@..@.rsrc...(.....@..@.reloc.....@..B..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\es-ES\MpAsDesc.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	67816
Entropy (8bit):	4.139143013850931
Encrypted:	false
SSDEEP:	768:7r690VA3iN3v240ynoFXuAQ8UyCNbHQSfr+FABZgdTypKR1PJl:iyHGyoFXXfW7Q2r+FAodTypKHPJl
MD5:	B6A28B3D905B28545AC4EC448846C6F4
SHA1:	C59E0A7600A0A76B25B46A7B5D1574BA09FC6826
SHA-256:	89404202E75E8D03AF2458906D9622C7ECD43F4B30180B079B143B77EA6BA6A4
SHA-512:	650319B0A81FB5A1BACE4760C14BA37245A9FB23F4A7E5B18B3BE279A5EDF5063BB1CF5C8631AEC30ACEDCF3F92219B63279A4B01DA80C21B2182C88F56F915 8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....}.....@..... ..h..... .....8.....rdata..... @..@.rsrc..... .....@..@.....I.....T...8...8.....I.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....(..X....rsrc$02.... .....d...!Z...!.4@e_/x!..... .I..... .....

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\A3755C46-599C-4124-9378-CC4837F46662\es-ES\MpEvMsg.dll.mui	
Process:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	58616
Entropy (8bit):	4.347687086754615
Encrypted:	false
SSDEEP:	768:7ruyfm07DjkGDxibCs79eoh9ewh/6L3NM6MAM8rbrubOezWyi4JzOcfQT/ZsH+KY:5H6BJdLd0dZLTOy+JdVfQT/eNNTvHPtW
MD5:	1CEB1C751D2CF63A0856B30A74486565
SHA1:	7D388EF3D300849D5E08FFA8F37DBB72765EED9B
SHA-256:	4421F31079246BD5A8B2C76B305BD88251DE81DAA0DBFDC393ACE55198B58F34
SHA-512:	00929E60E67BB9ABD2D4081D387B13D25D819DDCEFABE3384C0FB70C47566FE675499768C1455DDAB7480D1696F956A2448DF1064E7A9DA72085F04A19EE39B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k=.].S.].S.].S.....\.S...Q.\.S.Rich].S.....PE..L.....!..... .....H.....@..... ....8.....rdata..... @..@.rsrc..... .....@..@.....].....T...8...8.....].....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... ..8....rsrc$02.... ..._<.....5..\Z2.....~..4] ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.2442298972838195
TrID:	• Win32 Executable (generic) a (10002005/4) 99.01% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Visual Basic Script (13500/0) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	FACTURA.exe

General

File size:	143360
MD5:	740463ed3266f7aee8331978f50c731c
SHA1:	a9310948476693d72be937f23e1b53b3607bf92f
SHA256:	fa9e12a03b909482d5bacd2d7ab1a8d672528bfcf43402c04b6d3a30702b0c4d
SHA512:	15bd20faadbcc09b236e8408cf0b5f0903ad39cb1183b99e9a767e0a58ddc65624f27fa0fc983900af669bbe43a7766e7e6493d4e002833b3d3e5026b63079af
SSDEEP:	3072:tPM2YNAkMB0fkeX4QKDmBnmY4tmT9tzh/jrVB:tPM2YNAkMBykeX4wrLrVB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L....+.N.....@.....

File Icon

Icon Hash:	00e4d2c2dac20042

Static PE Info

General

Entrypoint:	0x4018dc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4E922BCC [Sun Oct 9 23:18:36 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d0ac0bdf3a5152bcac064d77eed21690

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x184f0	0x19000	False	0.479140625	data	6.34090617011	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0xd20	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x75f9	0x8000	False	0.238891601562	data	5.20756276635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 8, 2021 11:05:32.716264963 CEST	192.168.11.20	1.1.1.1	0x26f1	Standard query (0)	spclient.wg.spotify.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 8, 2021 11:05:32.754240036 CEST	1.1.1.1	192.168.11.20	0x26f1	No error (0)	spclient.wg.spotify.com	edge-web.dual-gslb.spotify.com		CNAME (Canonical name)	IN (0x0001)
Oct 8, 2021 11:05:32.754240036 CEST	1.1.1.1	192.168.11.20	0x26f1	No error (0)	edge-web.dual-gslb.spotify.com		35.186.224.25	A (IP address)	IN (0x0001)
Oct 8, 2021 11:11:00.805844069 CEST	1.1.1.1	192.168.11.20	0x321e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: FACTURA.exe PID: 7040 Parent PID: 3440

General

Start time:	11:02:34
Start date:	08/10/2021
Path:	C:\Users\user\Desktop\FACTURA.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\FACTURA.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	740463ED3266F7AEE8331978F50C731C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 8016 Parent PID: 7040

General

Start time:	11:02:36
Start date:	08/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 848
Imagebase:	0x3e0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 2516 Parent PID: 7040

General

Start time:	11:02:42
Start date:	08/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 856
Imagebase:	0x3e0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Analysis Process: UserOOBEBroker.exe PID: 2888 Parent PID: 1036

General

Start time:	11:08:03
Start date:	08/10/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff617640000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: mpam-5e107659.exe PID: 6940 Parent PID: 6040

General

Start time:	11:08:08
Start date:	08/10/2021
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-5e107659.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-5e107659.exe' /q WD
Imagebase:	0x7ff67cd30000
File size:	15598000 bytes
MD5 hash:	58454E5B478373BF68420AE5D49380D4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MpSigStub.exe PID: 5556 Parent PID: 6940

General

Start time:	11:08:11
Start date:	08/10/2021
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\9B256797-6DAD-4B73-B8E9-EA48023428D4\MpSigStub.exe /stub 1.1.18500.10 /payload 1.351.16.0 /program C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-5e107659.exe /q WD
Imagebase:	0x7ff77d6a0000
File size:	803176 bytes
MD5 hash:	01F92DC7A766FF783AE7AF40FD0334FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000024.00000003.6293943264.00000197A31B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Tofu_Backdoor, Description: Detects Tofu Trojan, Source: 00000024.00000003.6348926620.00000197A3621000.00000004.00000001.sdmp, Author: Cylance • Rule: ZxShell_Jul17, Description: Detects a ZxShell - CN threat group, Source: 00000024.00000003.6316460209.00000197A40AB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6345553259.00000197A36F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6320871262.00000197A4180000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RemCom_RemoteCommandExecution, Description: Detects strings from RemCom tool, Source: 00000024.00000003.6327269415.00000197A3790000.00000004.00000001.sdmp, Author: Florian Roth • Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6324198203.00000197A492C000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6324198203.00000197A492C000.00000004.00000001.sdmp, Author: Joe Security • Rule: WScript_Shell_PowerShell_Combo, Description: Detects malware from Middle Eastern campaign reported by Talos, Source: 00000024.00000003.6334856272.00000197A372A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: clearlog, Description: Detects Fireball malware - file clearlog.dll, Source: 00000024.00000003.6291492327.00000197A37E5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6321843775.00000197A2FD4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6321843775.00000197A2FD4000.00000004.00000001.sdmp, Author: Joe Security • Rule: Amplia_Security_Tool, Description: Amplia Security Tool, Source: 00000024.00000003.6345862795.00000197A47E3000.00000004.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6345862795.00000197A47E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6317535190.00000197A4F30000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6317535190.00000197A4F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: APT_DeputyDog_Fexel, Description: unknown, Source: 00000024.00000003.6317535190.00000197A4F30000.00000004.00000001.sdmp, Author: ThreatConnect Intelligence Research Team • Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6322693408.00000197A3BC3000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6322693408.00000197A3BC3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6291090515.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source:

00000024.00000003.6291090515.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6291090515.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6332905468.00000197A3592000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6416783153.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6416783153.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6416783153.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000024.00000003.6336234827.00000197A31B6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6301822800.00000197A4E6B000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000024.00000003.6301822800.00000197A4E6B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6301822800.00000197A4E6B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6307634469.00000197A2ED4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hacktool_Strings_p0wnedShell, Description: p0wnedShell Runspace Post Exploitation Toolkit - file p0wnedShell.cs, Source: 00000024.00000003.6271796009.00000197A32DD000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000024.00000003.6271796009.00000197A32DD000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source: 00000024.00000003.6271796009.00000197A32DD000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6318964208.00000197A48A9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6320453518.00000197A412F000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6320453518.00000197A412F000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6320453518.00000197A412F000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6320453518.00000197A412F000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6320453518.00000197A412F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RemCom_RemoteCommandExecution, Description: Detects strings from RemCom tool, Source: 00000024.00000003.6335436052.00000197A3016000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_RemComRemoteAdmin, Description: Yara detected RemCom RemoteAdmin tool, Source: 00000024.00000003.6335436052.00000197A3016000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6415513577.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6415513577.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6415513577.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6319425963.00000197A492C000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6319425963.00000197A492C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6323089969.00000197A3C04000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6323089969.00000197A3C04000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6351148277.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_bitcoinminer, Description: Yara detected BitCoin Miner, Source: 00000024.00000003.6351148277.00000197A49F2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hacktool_Strings_p0wnedShell, Description: p0wnedShell Runspace Post Exploitation Toolkit - file p0wnedShell.cs, Source: 00000024.00000003.6274276311.00000197A2E51000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source: 00000024.00000003.6274276311.00000197A2E51000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6274276311.00000197A2E51000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6274276311.00000197A2E51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6274276311.00000197A2E51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6422770651.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6422770651.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6422770651.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6349431685.00000197A36F1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000024.00000003.6437415503.00000197A38EC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6333813745.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6333813745.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6333813745.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6336709311.00000197A33E4000.00000004.00000001.sdmp,

Author: Joe Security
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6336709311.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6336709311.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6423333763.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6423333763.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6423333763.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6320126679.00000197A4068000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6320126679.00000197A4068000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6303130875.00000197A4DA4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6303130875.00000197A4DA4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6303130875.00000197A4DA4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000024.00000003.6438683964.00000197A371E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: APT9002Strings, Description: 9002 Identifying Strings, Source: 00000024.00000003.6438683964.00000197A371E000.00000004.00000001.sdmp, Author: Seth Hardy
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000024.00000003.6303735122.00000197A3500000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: APT_DeputyDog_Fexel, Description: unknown, Source: 00000024.00000003.6303735122.00000197A3500000.00000004.00000001.sdmp, Author: ThreatConnect Intelligence Research Team
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6340510692.00000197A4B3C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6337630194.00000197A492C000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6337630194.00000197A492C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000024.00000003.6283020613.00000197A471D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6312003576.00000197A3DD5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6343593773.00000197A4DA5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6343593773.00000197A4DA5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6343593773.00000197A4DA5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6337978043.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_bitcoinminer, Description: Yara detected BitCoin Miner, Source: 00000024.00000003.6337978043.00000197A49F2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6435320664.00000197A4AB7000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Buran, Description: Yara detected Buran Ransomware, Source: 00000024.00000003.6435320664.00000197A4AB7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Gocoder_3, Description: Yara detected Gocoder ransomware, Source:

00000024.00000003.6435320664.00000197A4AB7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source: 00000024.00000003.6286857920.00000197A49B1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000024.00000003.6280960340.00000197A4381000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Certutil_Decode_OR_Download, Description: Certutil Decode, Source: 00000024.00000003.6280960340.00000197A4381000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000024.00000003.6280960340.00000197A4381000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CredTheft_MSIL_ADPassHunt_2, Description: unknown, Source: 00000024.00000003.6269788057.00000197A4C44000.00000004.00000001.sdmp, Author: FireEye
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6269788057.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6332385174.00000197A4180000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6337394565.00000197A4314000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6341931442.00000197A45E4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6341931442.00000197A45E4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6341931442.00000197A45E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Base64_PS1_Shellcode, Description: Detects Base64 encoded PS1 Shellcode, Source: 00000024.00000003.6441079311.00000197A4E6A000.00000004.00000001.sdmp, Author: Nick Carr, David Ledbetter
- Rule: WScript_Shell_PowerShell_Combo, Description: Detects malware from Middle Eastern campaign reported by Talos, Source: 00000024.00000003.6441079311.00000197A4E6A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000024.00000003.6441079311.00000197A4E6A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Msfpayloads_msf_psh, Description: Metasploit Payloads - file msf-psh.vba, Source: 00000024.00000003.6346866223.00000197A4C8E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: TA17_293A_malware_1, Description: inveigh pen testing tools & related artifacts, Source: 00000024.00000003.6279246359.00000197A4A35000.00000004.00000001.sdmp, Author: US-CERT Code Analysis Team (modified by Florian Roth)
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6279246359.00000197A4A35000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6325389459.00000197A496F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6325389459.00000197A496F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6272159714.00000197A331E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6290858289.00000197A33BE000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6314983719.00000197A2F51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6356649431.00000197A36F1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6323451282.00000197A3C46000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6323451282.00000197A3C46000.00000004.00000001.sdmp,

Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6287415616.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_bitcoinminer, Description: Yara detected BitCoin Miner, Source: 00000024.00000003.6287415616.00000197A49F2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6355237590.00000197A3E9A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source: 00000024.00000003.6304100006.00000197A2F93000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6300924417.00000197A4314000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6325869951.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_bitcoinminer, Description: Yara detected BitCoin Miner, Source: 00000024.00000003.6325869951.00000197A49F2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: USG
- Rule: IMPLANT_5_v3, Description: XTunnel Implant by APT28, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: US CERT
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_cerber, Description: Yara detected Cerber ransomware, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_NoCry, Description: Yara detected NoCry Ransomware, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: Joe Security
- Rule: malware_red_leaves_memory, Description: Red Leaves C&C left in memory, use with Volatility / Rekall, Source: 00000024.00000003.6439501262.00000197A4A33000.00000004.00000001.sdmp, Author: David Cannings
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6309425115.00000197A492C000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6309425115.00000197A492C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6354837161.00000197A4180000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000024.00000003.6338261504.00000197A4590000.00000004.00000001.sdmp, Author: Avast Threat Intel Team
- Rule: webshell_php_obfuscated_encoding, Description: PHP webshell obfuscated by encoding, Source: 00000024.00000003.6338261504.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6338261504.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6338261504.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: Tofu_Backdoor, Description: Detects Tofu Trojan, Source: 00000024.00000003.6341599132.00000197A3621000.00000004.00000001.sdmp, Author: Cylance
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6275847061.00000197A4698000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source:

00000024.00000003.6351629812.00000197A3C46000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6351629812.00000197A3C46000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6327908307.00000197A40EC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: xtremrat, Description: Xtrem RAT v3.5, Source: 00000024.00000003.6327908307.00000197A40EC000.00000004.00000001.sdmp, Author: Jean-Philippe Teissier / @Jipe_
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6350988033.00000197A3FA2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6421798400.00000197A3D81000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6421798400.00000197A3D81000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6421798400.00000197A3D81000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Oilrig_IntelSecurityManager_macro, Description: Detects OilRig malware, Source: 00000024.00000003.6306777580.00000197A39F4000.00000004.00000001.sdmp, Author: Eyal Sela (slightly modified by Florian Roth)
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6306777580.00000197A39F4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6304560058.00000197A2FD4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6304560058.00000197A2FD4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6278189283.00000197A3970000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6314037891.00000197A4314000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000024.00000003.6429536769.00000197A4656000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Voidcrypt, Description: Yara detected Voidcrypt Ransomware, Source: 00000024.00000003.6429536769.00000197A4656000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6429536769.00000197A4656000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000024.00000003.6429536769.00000197A4656000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000024.00000003.6280199077.00000197A44B4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CredTheft_MSIL_ADPassHunt_2, Description: unknown, Source: 00000024.00000003.6355645936.00000197A4C44000.00000004.00000001.sdmp, Author: FireEye
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6355645936.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: APT_MAL_Sandworm_Exaramel_Configuration_Key, Description: Detects the encryption key for the configuration file used by Exaramel malware as seen in sample e1ff72[..., Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: FR/ANSSI/SDO
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: Joe Security

- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6342863444.00000197A4F72000.00000004.00000001.sdmp, Author: Joe Security
- Rule: WScriptShell_Case_Anomaly, Description: Detects obfuscated wscript.shell commands, Source: 00000024.00000003.6323790490.00000197A4866000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Voidcrypt, Description: Yara detected Voidcrypt Ransomware, Source: 00000024.00000003.6323790490.00000197A4866000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6433381009.00000197A3C87000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6269311104.00000197A4C03000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: PUA_CryptoMiner_Jan19_1, Description: Detects Crypto Miner strings, Source: 00000024.00000003.6269311104.00000197A4C03000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6269311104.00000197A4C03000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6352999953.00000197A3469000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_gogoogle, Description: Yara detected GoGoogle ransomware, Source: 00000024.00000003.6436704102.00000197A4AFA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Wannacry, Description: Yara detected Wannacry ransomware, Source: 00000024.00000003.6436704102.00000197A4AFA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6339772836.00000197A3E9A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6440763384.00000197A4E29000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6440763384.00000197A4E29000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Certutil_Decode_OR_Download, Description: Certutil Decode, Source: 00000024.00000003.6439967654.00000197A4446000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6330651040.00000197A36F1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6324553749.00000197A3B81000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6324553749.00000197A3B81000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6324553749.00000197A3B81000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6308253805.00000197A3EDD000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6308253805.00000197A3EDD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Oilrig_IntelSecurityManager_macro, Description: Detects OilRig malware, Source: 00000024.00000003.6290353787.00000197A39F4000.00000004.00000001.sdmp, Author: Eyal Sela (slightly modified by Florian Roth)
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6290353787.00000197A39F4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source: 00000024.00000003.6271076584.00000197A3A37000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: SUSP_PowerShell_IEX_Download_Combo, Description: Detects strings found in sample from CN group repo leak in October 2018, Source: 00000024.00000003.6271076584.00000197A3A37000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000024.00000003.6271076584.00000197A3A37000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6271076584.00000197A3A37000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RemCom_RemoteCommandExecution, Description: Detects strings from RemCom tool, Source:

00000024.00000003.6322218555.00000197A3016000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_RemComRemoteAdmin, Description: Yara detected RemCom RemoteAdmin tool, Source: 00000024.00000003.6322218555.00000197A3016000.00000004.00000001.sdmp, Author: Joe Security
- Rule: APT_Backdoor_Win_GoRat_Memory, Description: Identifies GoRat malware in memory based on strings., Source: 00000024.00000003.6284057981.00000197A47A0000.00000004.00000001.sdmp, Author: FireEye
- Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: USG
- Rule: Certutil_Decode_OR_Download, Description: Certutil Decode, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: yara@s3c.za.net
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: WScriptShell_Case_Anomaly, Description: Detects obfuscated wscript.shell commands, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Ham_backdoor, Description: unknown, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: Cylance Spear Team
- Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000024.00000003.6437789522.00000197A392D000.00000004.00000001.sdmp, Author: David Cannings
- Rule: webshell_php_base64_encoded_payloads, Description: php webshell containing base64 encoded payload, Source: 00000024.00000003.6430342028.00000197A4BC0000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6430342028.00000197A4BC0000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6430342028.00000197A4BC0000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_known_webshell, Description: Known PHP Webshells which contain unique strings, lousy rule for low hanging fruits. Most are catched by other rules in here but maybe these catch different versions., Source: 00000024.00000003.6430342028.00000197A4BC0000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_hidden_tear, Description: Yara detected HiddenTear ransomware, Source: 00000024.00000003.6430342028.00000197A4BC0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000024.00000003.6282540905.00000197A4590000.00000004.00000001.sdmp, Author: Avast Threat Intel Team
- Rule: webshell_php_obfuscated_encoding, Description: PHP webshell obfuscated by encoding, Source: 00000024.00000003.6282540905.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6282540905.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6282540905.00000197A4590000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6350622822.00000197A3F60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6350622822.00000197A3F60000.00000004.00000001.sdmp, Author: Joe Security
- Rule: WScript_Shell_PowerShell_Combo, Description: Detects malware from Middle

Eastern campaign reported by Talos, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: HackTool_Samples, Description: Hacktool, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: unknown
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Wannacry, Description: Yara detected Wannacry ransomware, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: MirageStrings, Description: Mirage Identifying Strings, Source: 00000024.00000003.6430077076.00000197A46D9000.00000004.00000001.sdmp, Author: Seth Hardy
- Rule: Trojan_Win32_PlaKeylog_B, Description: Keylogger component, Source: 00000024.00000003.6313066347.00000197A4615000.00000004.00000001.sdmp, Author: Microsoft
- Rule: DeepPanda_htran_exe, Description: Hack Deep Panda - htran-exe, Source: 00000024.00000003.6313066347.00000197A4615000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6313066347.00000197A4615000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6331669561.00000197A4068000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6331669561.00000197A4068000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CredTheft_MSIL_ADPassHunt_2, Description: unknown, Source: 00000024.00000003.6285143119.00000197A4C44000.00000004.00000001.sdmp, Author: FireEye
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6285143119.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6289584259.00000197A3F60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6289584259.00000197A3F60000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6283505070.00000197A475E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6310770552.00000197A4B3C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: HackTool_MSIL_SharPersist_2, Description: unknown, Source: 00000024.00000003.6312336240.00000197A3E16000.00000004.00000001.sdmp, Author: FireEye
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000024.00000003.6300197684.00000197A42BB000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Growtopia, Description: Yara detected Growtopia, Source: 00000024.00000003.6300197684.00000197A42BB000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6329279249.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000024.00000003.6329279249.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6329279249.00000197A33E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6290223213.00000197A39E2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6330297949.00000197A369B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6330297949.00000197A369B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable,

Source:
00000024.00000003.6441407992.00000197A4404000.00000004.00000001.sdmp,
Author: Florian Roth

- Rule: WScriptShell_Case_Anomaly, Description: Detects obfuscated wscript.shell commands, Source:
00000024.00000003.6441407992.00000197A4404000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source:
00000024.00000003.6441407992.00000197A4404000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source:
00000024.00000003.6441407992.00000197A4404000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source:
00000024.00000003.6289251468.00000197A3F1F000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source:
00000024.00000003.6424034919.00000197A3D91000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source:
00000024.00000003.6424034919.00000197A3D91000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6424034919.00000197A3D91000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source:
00000024.00000003.6413956773.00000197A3D81000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source:
00000024.00000003.6413956773.00000197A3D81000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6413956773.00000197A3D81000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: Oilrig_IntelSecurityManager_macro, Description: Detects OilRig malware, Source:
00000024.00000003.6294532862.00000197A39F4000.00000004.00000001.sdmp,
Author: Eyal Sela (slightly modified by Florian Roth)
- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source:
00000024.00000003.6294532862.00000197A39F4000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: APT_Backdoor_Win_GoRat_Memory, Description: Identifies GoRat malware in memory based on strings., Source:
00000024.00000003.6356061064.00000197A47A0000.00000004.00000001.sdmp,
Author: FireEye
- Rule: JoeSecurity_cerber, Description: Yara detected Cerber ransomware, Source:
00000024.00000003.6434542406.00000197A437F000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: JoeSecurity_cerber, Description: Yara detected Cerber ransomware, Source:
00000024.00000003.6435021591.00000197A4A76000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source:
00000024.00000003.6435021591.00000197A4A76000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: webshell_php_generic, Description: php webshell having some kind of input and some kind of payload. restricted to small files or big ones inclusing suspicious strings, Source:
00000024.00000003.6437085765.00000197A4B7D000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source:
00000024.00000003.6437085765.00000197A4B7D000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source:
00000024.00000003.6437085765.00000197A4B7D000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: Oilrig_IntelSecurityManager_macro, Description: Detects OilRig malware, Source:
00000024.00000003.6437085765.00000197A4B7D000.00000004.00000001.sdmp,
Author: Eyal Sela (slightly modified by Florian Roth)
- Rule: JoeSecurity_Cobra_Locker, Description: Yara detected Cobra Locker ransomware, Source:
00000024.00000003.6437085765.00000197A4B7D000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source:
00000024.00000003.6415046546.00000197A3D91000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source:
00000024.00000003.6415046546.00000197A3D91000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6415046546.00000197A3D91000.00000004.00000001.sdmp,

Author: Joe Security
- Rule: webshell_php_generic, Description: php webshell having some kind of input and some kind of payload. restricted to small files or big ones inclusing suspicious strings, Source: 00000024.00000003.6431307677.00000197A4B7D000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6431307677.00000197A4B7D000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000024.00000003.6431307677.00000197A4B7D000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Oilrig_IntelSecurityManager_macro, Description: Detects OilRig malware, Source: 00000024.00000003.6431307677.00000197A4B7D000.00000004.00000001.sdmp, Author: Eyal Sela (slightly modified by Florian Roth)
- Rule: JoeSecurity_Cobra_Locker, Description: Yara detected Cobra Locker ransomware, Source: 00000024.00000003.6431307677.00000197A4B7D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6406320906.00000197A3D81000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6406320906.00000197A3D81000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6406320906.00000197A3D81000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6319752266.00000197A3FE5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6319752266.00000197A3FE5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6319752266.00000197A3FE5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6316141195.00000197A4068000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Conti_ransomware, Description: Yara detected Conti ransomware, Source: 00000024.00000003.6316141195.00000197A4068000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CredTheft_MSIL_ADPassHunt_2, Description: unknown, Source: 00000024.00000003.6340905094.00000197A4C44000.00000004.00000001.sdmp, Author: FireEye
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6340905094.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6414541213.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6414541213.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6414541213.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Ammyy_Admin_AA_v3, Description: Remote Admin Tool used by APT group Anunak (ru) - file AA_v3.4.exe and AA_v3.5.exe, Source: 00000024.00000003.6277859035.00000197A392F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000024.00000003.6277859035.00000197A392F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6277859035.00000197A392F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_Script_Obfuscation_Char_Concat, Description: Detects strings found in sample from CN group repo leak in October 2018, Source: 00000024.00000003.6440424598.00000197A4487000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000024.00000003.6440424598.00000197A4487000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_cerber, Description: Yara detected Cerber ransomware, Source: 00000024.00000003.6440424598.00000197A4487000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Clop, Description: Yara detected Clop Ransomware, Source:

00000024.00000003.6440424598.00000197A4487000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nemty, Description: Yara detected Nemty Ransomware, Source: 00000024.00000003.6440424598.00000197A4487000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6439090002.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: WScriptShell_Case_Anomaly, Description: Detects obfuscated wscript.shell commands, Source: 00000024.00000003.6439090002.00000197A49F2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6439090002.00000197A49F2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: vanquish_2, Description: Webshells Auto-generated - file vanquish.exe, Source: 00000024.00000003.6439090002.00000197A49F2000.00000004.00000001.sdmp, Author: Yara Bulk Rule Generator by Florian Roth
- Rule: SUSP_Script_Obfuscation_Char_Concat, Description: Detects strings found in sample from CN group repo leak in October 2018, Source: 00000024.00000003.6287974454.00000197A4D37000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6333426467.00000197A331E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: hacktool_macos_keylogger_logkext, Description: LogKext is an open source keylogger for Mac OS X, a product of FSB software., Source: 00000024.00000003.6315705690.00000197A4027000.00000004.00000001.sdmp, Author: @mimeframe
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6268699778.00000197A4FF7000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6268699778.00000197A4FF7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6268699778.00000197A4FF7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: MAL_unspecified_Jan18_1, Description: Detects unspecified malware sample, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Vidar, Description: Yara detected Vidar stealer, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_ByteLocker, Description: Yara detected ByteLocker Ransomware, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Artemon, Description: Yara detected Artemon Ransomware, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_lazparking, Description: Yara detected LazParking Ransomware, Source: 00000024.00000003.6431842764.00000197A4D63000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Base64_PS1_Shellcode, Description: Detects Base64 encoded PS1 Shellcode, Source: 00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp, Author: Nick Carr, David Ledbetter
- Rule: Pupy_Backdoor, Description: Detects Pupy backdoor, Source: 00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Meterpreter, Description: Yara detected Meterpreter, Source: 00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_RevengeRAT, Description: Yara detected RevengeRAT, Source: 00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload,

Source:
00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp,
Author: Joe Security

- Rule: JoeSecurity_EvilGnomeRC5Key, Description: Yara detected Linux EvilGnome RC5 key, Source:
00000024.00000003.6428495405.00000197A2E93000.00000004.00000001.sdmp,
Author: unknown
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source:
00000024.00000003.6324954542.00000197A3C46000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source:
00000024.00000003.6324954542.00000197A3C46000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source:
00000024.00000003.6347606531.00000197A3C46000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source:
00000024.00000003.6347606531.00000197A3C46000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source:
00000024.00000003.6436377560.00000197A4C85000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6344719591.00000197A3659000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source:
00000024.00000003.6339257691.00000197A45E4000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source:
00000024.00000003.6339257691.00000197A45E4000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6339257691.00000197A45E4000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source:
00000024.00000003.6407260909.00000197A3D91000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source:
00000024.00000003.6407260909.00000197A3D91000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6407260909.00000197A3D91000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6299736334.00000197A2ED4000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source:
00000024.00000003.6277539520.00000197A4590000.00000004.00000001.sdmp,
Author: Avast Threat Intel Team
- Rule: webshell_php_obfuscated_encoding, Description: PHP webshell obfuscated by encoding, Source:
00000024.00000003.6277539520.00000197A4590000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source:
00000024.00000003.6277539520.00000197A4590000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source:
00000024.00000003.6277539520.00000197A4590000.00000004.00000001.sdmp,
Author: Arnim Rupp
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source:
00000024.00000003.6315364038.00000197A2FD4000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source:
00000024.00000003.6315364038.00000197A2FD4000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source:
00000024.00000003.6270634530.00000197A4698000.00000004.00000001.sdmp,
Author: Joe Security
- Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source:
00000024.00000003.6438240606.00000197A36DD000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source:
00000024.00000003.6438240606.00000197A36DD000.00000004.00000001.sdmp,
Author: Florian Roth
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source:

00000024.00000003.6438240606.00000197A36DD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Clop, Description: Yara detected Clop Ransomware, Source: 00000024.00000003.6438240606.00000197A36DD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Cute, Description: Yara detected Cute Ransomware, Source: 00000024.00000003.6438240606.00000197A36DD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000024.00000003.6284577103.00000197A4BC1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6407733822.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6407733822.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6407733822.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_by_string_known_webshell, Description: Known PHP Webshells which contain unique strings, lousy rule for low hanging fruits. Most are catched by other rules in here but maybe these catch different versions., Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: Oilrig_IntelSecurityManager, Description: Detects OilRig malware, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Eyal Sela
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Winexe_tool, Description: Yara detected Winexe tool, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6348335236.00000197A3259000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_by_string_obfuscation, Description: PHP file containing obfuscation strings. Might be legitimate code obfuscated for whatever reasons, a webshell or can be used to insert malicious Javascript for credit card skimming, Source: 00000024.00000003.6328572357.00000197A4180000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: Mimikatz_Memory_Rule_1, Description: Detects password dumper mimikatz in memory (False Positives: an service that could have copied a Mimikatz executable, AV signatures), Source: 00000024.00000003.6309767237.00000197A3869000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6309767237.00000197A3869000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000024.00000003.6273475176.00000197A3D51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MSIL_Load_Encrypted_Assembly, Description: Yara detected MSIL_Load_Encrypted_Assembly, Source: 00000024.00000003.6273475176.00000197A3D51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CVE_2018_4878_0day_ITW, Description: unknown, Source: 00000024.00000003.6273475176.00000197A3D51000.00000004.00000001.sdmp, Author: unknown
- Rule: CredTheft_MSIL_ADPassHunt_2, Description: unknown, Source: 00000024.00000003.6334441396.00000197A4C44000.00000004.00000001.sdmp, Author: FireEye
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6334441396.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_PowerShell_IEX_Download_Combo, Description: Detects strings found in sample from CN group repo leak in October 2018, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: webshell_php_generic, Description: php webshell having some kind of input and some kind of payload. restricted to small files or big ones inclusing suspicious strings, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_generic_eval, Description: Generic PHP webshell which uses any eval/exec function in the same line with user input, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp,

Author: Arnim Rupp
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: ChinaChopper_Generic, Description: China Chopper Webshells - PHP and ASPX, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_mock, Description: Yara detected Mock Ransomware, Source: 00000024.00000003.6432316317.00000197A4DA4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: WScriptShell_Case_Anomaly, Description: Detects obfuscated wscript.shell commands, Source: 00000024.00000003.6278908021.00000197A4866000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Voidcrypt, Description: Yara detected Voidcrypt Ransomware, Source: 00000024.00000003.6278908021.00000197A4866000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6316787263.00000197A40EC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: xtremrat, Description: Xtrem RAT v3.5, Source: 00000024.00000003.6316787263.00000197A40EC000.00000004.00000001.sdmp, Author: Jean-Philippe Teissier / @Jipe_
- Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000024.00000003.6287839327.00000197A4D21000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6273910781.00000197A3D92000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6273910781.00000197A3D92000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6273910781.00000197A3D92000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6342326827.00000197A41F5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6342326827.00000197A41F5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6342326827.00000197A41F5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: GoldDragon_Aux_File, Description: Detects export from Gold Dragon - February 2018, Source: 00000024.00000003.6434024184.00000197A433E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6434024184.00000197A433E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6434024184.00000197A433E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: HackTool_Samples, Description: Hacktool, Source: 00000024.00000003.6304991595.00000197A4237000.00000004.00000001.sdmp, Author: unknown
- Rule: PS_AMSI_Bypass, Description: Detects PowerShell AMSI Bypass, Source: 00000024.00000003.6304991595.00000197A4237000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6304991595.00000197A4237000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Pupy_Backdoor, Description: Detects Pupy backdoor, Source: 00000024.00000003.6301296808.00000197A4FB5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6301296808.00000197A4FB5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000024.00000003.6301296808.00000197A4FB5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6406830616.00000197A3D91000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded

code that has been base64 encoded, Source: 00000024.00000003.6406830616.00000197A3D91000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6406830616.00000197A3D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Pupy_Backdoor, Description: Detects Pupy backdoor, Source: 00000024.00000003.6436059336.00000197A4C44000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6436059336.00000197A4C44000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6436059336.00000197A4C44000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6294115539.00000197A3970000.00000004.00000001.sdmp, Author: Joe Security
- Rule: SUSP_PowerShell_IEX_Download_Combo, Description: Detects strings found in sample from CN group repo leak in October 2018, Source: 00000024.00000003.6432826435.00000197A3C46000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6432826435.00000197A3C46000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6289913928.00000197A39B3000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6289913928.00000197A39B3000.00000004.00000001.sdmp, Author: Joe Security
- Rule: APT_MAL_Sandworm_Exaramel_Configuration_Key, Description: Detects the encryption key for the configuration file used by Exaramel malware as seen in sample e1ff72[..., Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: FR/ANSSI/SDO
- Rule: webshell_php_gzinflated, Description: PHP webshell which directly eval()s obfuscated string, Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6317874324.00000197A4F72000.00000004.00000001.sdmp, Author: Joe Security
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6429813058.00000197A4697000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Cryptolocker, Description: Yara detected Cryptolocker ransomware, Source: 00000024.00000003.6429813058.00000197A4697000.00000004.00000001.sdmp, Author: Joe Security
- Rule: APT_Backdoor_Win_GoRat_Memory, Description: Identifies GoRat malware in memory based on strings., Source: 00000024.00000003.6288930033.00000197A47A0000.00000004.00000001.sdmp, Author: FireEye
- Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000024.00000003.6308756420.00000197A3F60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000024.00000003.6308756420.00000197A3F60000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_php_dynamic_big, Description: PHP webshell using $a($code) for kind of eval with encoded blob to decode, e.g. b374k, Source: 00000024.00000003.6338624600.00000197A45E4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6338624600.00000197A45E4000.00000004.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_Coinhive, Description: Yara detected Coinhive miner, Source: 00000024.00000003.6338624600.00000197A45E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: webshell_asp_generic_eval_on_input, Description: Generic ASP webshell which uses any eval/exec function directly on user input, Source: 00000024.00000003.6352553916.00000197A34AB000.00000004.00000001.sdmp, Author: Arnim Rupp

Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: wevtutil.exe PID: 4104 Parent PID: 3224

General

Start time:	11:08:42
Start date:	08/10/2021
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wevtutil.exe uninstall-manifest C:\Windows\TEMP\3A24BB4C-F6EB-A1AC-C6CC-E780FED56A57.man
Imagebase:	0x7ff67d560000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1412 Parent PID: 4104

General

Start time:	11:08:42
Start date:	08/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff778030000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wevtutil.exe PID: 6840 Parent PID: 3224

General

Start time:	11:08:43
Start date:	08/10/2021
Path:	C:\Windows\System32\wevtutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wevtutil.exe install-manifest C:\Windows\TEMP\3A24BB4C-F6EB-A1AC-C6CC-E780FED56A57.man '/resourceFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/messageFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll' '/parameterFilePath:C:\ProgramData\Microsoft\Windows Defender\Definition Updates\StableEngineEtwLocation\mpengine_etw.dll'
Imagebase:	0x7ff67d560000
File size:	291840 bytes
MD5 hash:	C57C1292650B6384903FE6408D412CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 2644 Parent PID: 6840

General

Start time:	11:08:44
Start date:	08/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff778030000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mpam-fad3e9a8.exe PID: 1248 Parent PID: 6040

General

Start time:	11:08:52
Start date:	08/10/2021
Path:	C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\mpam-fad3e9a8.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-fad3e9a8.exe
Imagebase:	0x7ff7755b0000
File size:	7855240 bytes
MD5 hash:	34B7B3BDFA61E18D3B2C3B0AC92B78EF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis