ID: 626495
Sample Name: vur7t4SumQ
Cookbook: default.jbs
Time: 04:55:31
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report vur7t4SumQ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
E-Banking Fraud 5
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 12
Public IPs 13
Private 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\ProgramData\Microsoft\Network\Downloader\edb.chk 15
C:\ProgramData\Microsoft\Network\Downloader\edb.log 15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db 15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\Report.wer 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp.xml 17
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 17
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Rich Headers 20
Data Directories 20
Sections 20
Resources 21
Imports 21
Exports 21
Possible Origin 21
Network Behavior 21
TCP Packets 21
HTTP Request Dependency Graph 22
HTTPS Proxied Packets 22
Statistics 22
Behavior 22
System Behavior 23
Analysis Process: loaddll64.exePID: 6328, Parent PID: 2912 23
General 23

File Activities 23
Analysis Process: cmd.exePID: 6348, Parent PID: 6328 23
General 23
File Activities 23
Analysis Process: regsvr32.exePID: 6356, Parent PID: 6328 23
General 23
File Activities 24
File Deleted 24
Analysis Process: rundll32.exePID: 6368, Parent PID: 6348 24
General 24
File Activities 24
Analysis Process: rundll32.exePID: 6376, Parent PID: 6328 24
General 24
File Activities 25
Analysis Process: svchost.exePID: 6424, Parent PID: 568 25
General 25
Analysis Process: rundll32.exePID: 6444, Parent PID: 6328 25
General 25
Analysis Process: regsvr32.exePID: 6512, Parent PID: 6356 26
General 26
Analysis Process: svchost.exePID: 6536, Parent PID: 568 26
General 26
File Activities 26
Registry Activities 26
Analysis Process: svchost.exePID: 6632, Parent PID: 568 27
General 27
Registry Activities 27
Analysis Process: WerFault.exePID: 6652, Parent PID: 6444 27
General 27
File Activities 27
File Created 27
File Deleted 28
File Written 28
Registry Activities 46
Key Created 46
Key Value Created 46
Key Value Modified 47
Analysis Process: svchost.exePID: 6696, Parent PID: 568 48
General 48
Analysis Process: SgrmBroker.exePID: 6908, Parent PID: 568 48
General 48
Analysis Process: svchost.exePID: 6960, Parent PID: 568 48
General 48
File Activities 49
Registry Activities 49
Analysis Process: svchost.exePID: 6988, Parent PID: 568 49
General 49
Registry Activities 49
Analysis Process: svchost.exePID: 6328, Parent PID: 568 49
General 49
File Activities 50
Analysis Process: svchost.exePID: 5608, Parent PID: 568 50
General 50
File Activities 50
Registry Activities 50
Analysis Process: MpCmdRun.exePID: 6856, Parent PID: 6988 50
General 50
File Activities 51
File Written 51
Analysis Process: conhost.exePID: 6956, Parent PID: 6856 52
General 52
Analysis Process: svchost.exePID: 5324, Parent PID: 568 52
General 52
File Activities 53
Analysis Process: svchost.exePID: 6056, Parent PID: 568 53
General 53
File Activities 53
Analysis Process: svchost.exePID: 6568, Parent PID: 568 53
General 53
File Activities 53
Disassembly 53

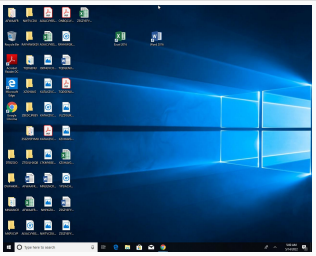
Windows Analysis Report

vur7t4SumQ

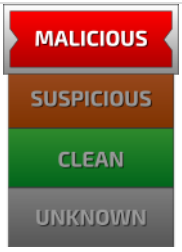
Overview

General Information

Sample Name:	vur7t4SumQ (renamed file extension from none to dll)
Analysis ID:	626495
MD5:	b4f74ea581aba7..
SHA1:	eec25f21b828ae..
SHA256:	91808c38624d6b..
Tags:	exe trojan
Infos:	



Detection



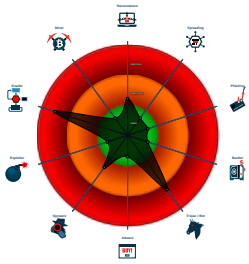
Emotet

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Query firmware table information (lik…
- Changes security center settings (n…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6328 cmdline: loaddll64.exe "C:\Users\user\Desktop\vur7t4SumQ.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6348 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\vur7t4SumQ.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6368 cmdline: rundll32.exe "C:\Users\user\Desktop\vur7t4SumQ.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6356 cmdline: regsvr32.exe /s C:\Users\user\Desktop\vur7t4SumQ.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6512 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JZAnomWmMqlc\LxifZH.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6376 cmdline: rundll32.exe C:\Users\user\Desktop\vur7t4SumQ.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6444 cmdline: rundll32.exe C:\Users\user\Desktop\vur7t4SumQ.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 6652 cmdline: C:\Windows\system32\WerFault.exe -u -p 6444 -s 316 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 6424 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6536 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6632 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6696 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6908 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6960 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6988 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6856 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6328 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5608 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5324 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6056 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6568 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.304486161.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.301657565.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.301080454.0000000000C20000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000000.305654507.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.330907798.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.2c00000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.0.rundll32.exe.1cc60a20000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.2c00000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.0.rundll32.exe.1cc60a20000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1c078260000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

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)

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

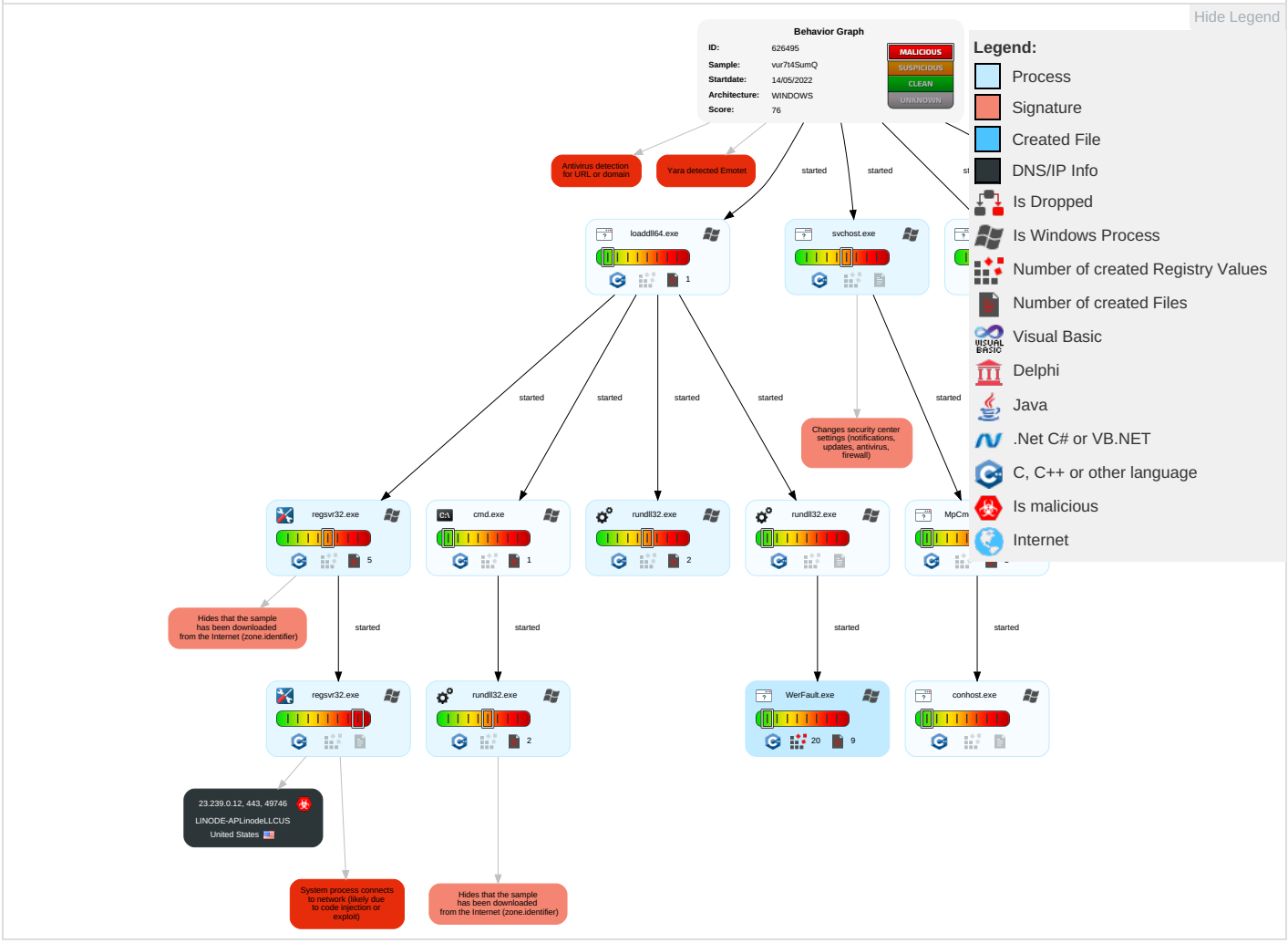
Yara detected Emotet

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 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 5 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	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 3 Virtualization/Sandbox Evasion	Security Account Manager	1 3 Virtualization/Sandbox Evasion	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	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	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 Remote System 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	2 File and Directory 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 Regsvr32	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	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 DLL Side-Loading	/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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

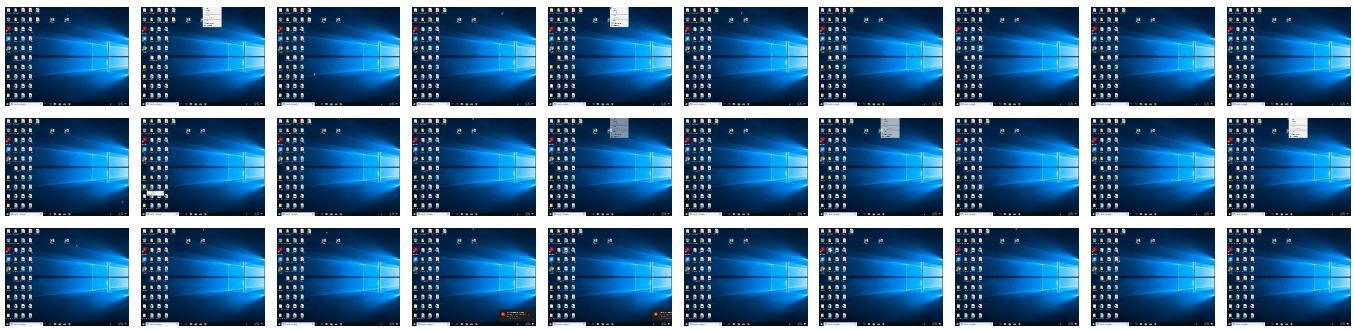
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.regsvr32.exe.2c00000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.0.rundll32.exe.1cc60a20000.4.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.1c078260000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.regsvr32.exe.c20000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.1bfbc3f0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.rundll32.exe.1cc60a20000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.0.rundll32.exe.1cc60a20000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://23.239.0.12/:	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	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://23.239.0.12/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

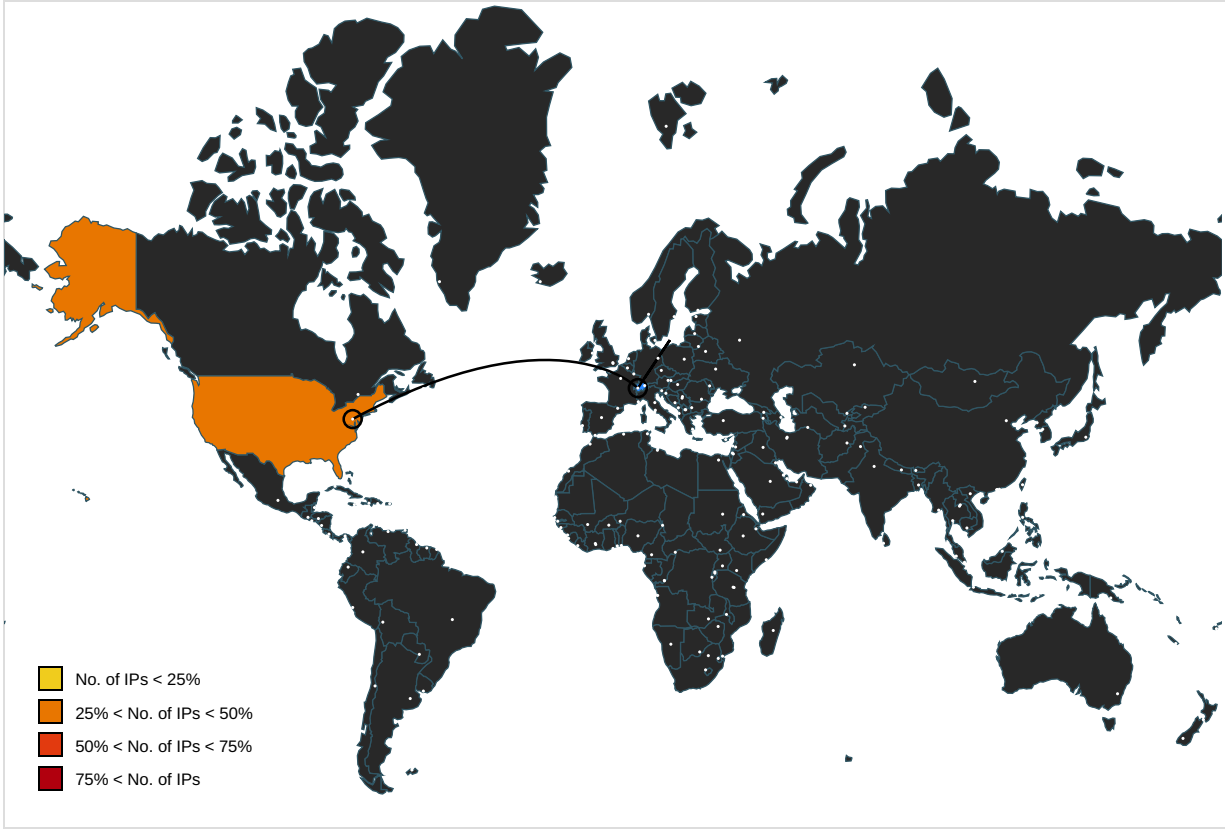
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000023.00000003.633872389.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.634106837.000001848C386000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000C.00000003.346793373.0000016408A56000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000C.00000002.347418598.0000016408A3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000C.00000002.347418598.0000016408A3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000C.00000003.346598052.0000016408A66000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.347465625.0000016408A69000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000C.00000002.347441463.0000016408A4D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346706686.0000016408A40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346778814.0000016408A46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/:	regsvr32.exe, 00000007.00000002.808671751.00000000012C3000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.372331150.00000000012C3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000C.00000002.347418598.0000016408A3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000C.00000003.310357279.0000016408A30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000C.00000003.346793373.0000016408A56000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000017.00000002.810883943.0000019E150DB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000C.00000002.347451088.0000016408A5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346643614.0000016408A5A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346706686.0000016408A40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000023.00000003.640164563.000001848C380000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.640328742.000001848C386000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.639176766.000001848C380000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.637766051.000001848C3B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.637802769.000001848C39A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.637784693.000001848C3B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.637820246.000001848C802000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000C.00000002.347418598.0000016408A3C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.347391430.0000016408A13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000C.00000002.347434165.0000016408A42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346706686.0000016408A40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346800723.0000016408A41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000009.00000002.808797308.0000020801644000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000C.00000003.310357279.0000016408A30000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000023.00000003.628872502.000001848C803000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628812103.000001848C802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628793828.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628775497.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628914924.000001848C386000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628985199.000001848C819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628947800.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000C.00000003.346643614.0000016408A5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000C.00000003.310357279.0000016408A30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000C.00000003.346643614.0000016408A5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000023.00000003.633872389.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.634106837.000001848C386000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000C.00000003.310357279.0000016408A30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000C.00000002.347434165.0000016408A42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346706686.0000016408A40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346800723.0000016408A41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000C.00000003.346793373.0000016408A56000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000023.00000003.628872502.000001848C803000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628812103.000001848C802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628793828.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628775497.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628914924.000001848C386000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628985199.000001848C819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628947800.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 00000023.00000003.628872502.000001848C803000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628812103.000001848C802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628793828.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628775497.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628914924.000001848C386000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628985199.000001848C819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.628947800.000001848C3A8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000023.00000003.633872389.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.634106837.000001848C386000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000C.00000003.310357279.0000016408A30000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.347406380.0000016408A29000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000C.00000002.347451088.0000016408A5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.346643614.0000016408A5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000009.00000002.808797308.0000020801644000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000C.00000002.347391430.0000016408A13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000C.00000003.346617620.0000016408A60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000023.00000003.633872389.000001848C398000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000023.00000003.634106837.000001848C386000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000C.00000002.347418598.0000016408A3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000009.00000002.808797308.0000020801644000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000C.00000003.346643614.0000016408A5A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.239.0.12	unknown	United States		63949	LINODE-APLinodeLLCUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626495
Start date and time: 14/05/202204:55:31	2022-05-14 04:55:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vur7t4SumQ (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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal76.troj.evad.winDLL@29/10@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 23.211.4.86, 51.104.136.2, 20.49.150.241, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdwus17.westus.cloudapp.azure.com, settings-prod-neu-2.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, ris.api.iris.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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.
- VT rate limit hit for: vur7t4SumQ.dll

Simulations

Behavior and APIs

Time	Type	Description
04:57:13	API Interceptor	1x Sleep call for process: WerFault.exe modified
04:57:14	API Interceptor	12x Sleep call for process: svchost.exe modified
04:58:16	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):	0.24935827104772523
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4Y:BJiRdwfu2SRU4Y
MD5:	65BA543731154E262BEBDA498C036A24
SHA1:	A5B0CDA7D5A43B87CE18383BE2332354AB405330
SHA-256:	F0A82DF3B3130C1DBD1C370AB18BDBF6C60EE1A940D22896E7CBD5410D77D160
SHA-512:	0C0737DAF84F655BFED9BD7E7C1E588F027E8FEED59EC4CBEA3457BEA49D443C603DAC03E5C6D6F048332AEDA4D0F5E2CC5F6991F79188CAC337583AE587E E31
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 0x26183b80, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505187084050976
Encrypted:	false
SSDEEP:	384:6br+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:6boSB2nSB2RSjlK/+mLesOj1J2
MD5:	5C23803EFC1E47189D12D1C421B0F22D
SHA1:	12702A4D5E7C3F5DED9F0F20B2C46569BEC9B1BE
SHA-256:	1A1994B86D5CC159BE5B8B8130F1CF777ABE6468E6AAB86D10BF69BCDAADE2C2
SHA-512:	A95D995F15C6177B50901AA29309D11C2C4946488C731C5C003DFEAEEBDBEA8536E048A3A321169BFEEBA9142F11190C2FE61C2E7177EBCF0492F93986E4477
Malicious:	false
Preview:	&.;.... .....e.f.3...w.....).....zA..9...z9.h.(.....zA...).....3...w.....B.....@..... ....=D=.....zA.....&.....zA..... .....

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

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

Size (bytes):	16384
Entropy (8bit):	0.07265747756488242
Encrypted:	false
SSDEEP:	3:n/lT7vrfraGpraeltlDlaAnBpolltld9laGltloll3VkttlmlnI:nZrTZavVlXT9laP3
MD5:	BA436A2D222DA4F542BCEDB02A12C6E8
SHA1:	0E97FDB6CD0E86FD2A9A7611314ECCA2F9B41C31
SHA-256:	436B148B10088042EB9FC0F481EA624D9AE2219136750CF6E1F3C986C8357315
SHA-512:	D2BBFFA71B22EC81C8D1FCDD8F6B92C5F88CAC395755A3D476B52CF9259A0D4F58B165728EFB1F8127D21D6A7C04D4C1407319AFA3DA812B6845FD6D5BE6AAB
Malicious:	false
Preview:	.....3...w...9...z9.....zA.....zA.....zA...|.....z.q.....&.....zA.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.785195610488955
Encrypted:	false
SSDEEP:	192:MPuiCJKAHK7gPri4jn9/u7s+S274ltl8:UuisKoK7gPri4j9/u7s+X4ltl8
MD5:	0AD5FC12C7D92E5D50F943425B4FFCF4
SHA1:	2BABCA8B3F44CAD959C144CB240C2723FAA21BD9
SHA-256:	3594824B9CB2403929E62A1C84B22B78E2585363AB322916B9DF5F54E00B03AD
SHA-512:	CFB9A9AC5AA63761A150E1C7ACB86E85450382E1B85075D5CC11D533AA46D4002BB252872A690B416DDEFDF9BB892998A9F48BD2D3CA694C5E3A5A9B0D902B73
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.0.0.3.0.2.4.5.2.2.0.4.4.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.0.0.3.0.3.1.6.3.1.3.9.6.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.0.d.2.a.8.9.4.-.c.7.6.2.-.4.a.5.d.-.b.9.e.e.-.c.c.a.b.8.a.3.7.8.5.8.d...I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.4.9.8.8.d.f.d.-.c.3.1.c.-.4.9.4.d.-.b.d.9.e.-.f.9.4.4.a.8.e.3.3.2.5.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.v.u.r.7.t.4.S.u.m.Q...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.2.c.-.0.0.0.1.-.0.0.1.d.-.c.1.3.e.-.b.4.b.5.8.9.6.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat May 14 11:57:05 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64474
Entropy (8bit):	2.2832062846864454
Encrypted:	false
SSDEEP:	384:1CgvroVDtgC+CyXdsIMyq7QEPryN48UNRwVC:1m/gCbysxyeNPryNYgV
MD5:	2E82CF8DFCC5A496806156DA213B18B2
SHA1:	5A93DE659A169E9ECFDF2D3967E42CEBDEFDB611
SHA-256:	86D97881EDA76878D65FD39ED97A73FF1CA080009449110D93A039857443BB76
SHA-512:	B0881E3FB5500B99AA26AB2510AAD7C700ECCE4059E7EACC41ED24AEBF92DC09E5A53D16E380137A8F3648D4C4C9349D09D77A6FC79CECEAB6FA838ADC46CEC8
Malicious:	false
Preview:	MDMP..... .....b.....|...8.....T...L;.....`.....8.....T.....".....$.....U.....B.....8%...Lw.....K.5...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...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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6664
Entropy (8bit):	3.7174259137072356

Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/pzinWcYViS0ZCprk89bhb25fp7jm:RrlsNiRzinWcYViS0AhbAfV6
MD5:	6BB0765B9553D593C72FF8A23CB23027
SHA1:	907E2DDE7ECE44164084A62989DEDC1D9B7A6553
SHA-256:	CB9902456BF80CFF1E8193187AE1476BE6E60F504F9E7B1CB2F1C24D5B474693
SHA-512:	B3ABB0ABB2B73EB785133393A4404BAC65CCE91DC2EB87D284C1290059B058B0125BFB90B53745AD7487AF2E7FB68550CD33A00E2D0B6FB8E0115FFE066548 E
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.>.6.4.4. 4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4892
Entropy (8bit):	4.49727789882082
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtBI9qk7Wgc8sqYjB8fm8M4JCLCSanF7yq8vhSa8ZESC5SVd:uITf9kkKgrsqYSJJWAVvVd
MD5:	7EE5B93B0903EC80B1131A4B14C7DBEA
SHA1:	10FED88E39C10847CFBD3DE4698B09527DD37B55
SHA-256:	0E48E34D48DF3EB7C8D9038C67129BFC4FD42323774342C3CEB8ABE70836C27B
SHA-512:	9DC223927FE94F487D760B895486305ACE57E2F7EBD7BCAD84857843C2C79ADF1D2AAD1BA9CF84B6E439707029D1D0A03C7EF278B49810008D62A6EB262645 B
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="1514707" />.. <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:\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):	3.164443212982886
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zO+J:j+s+v+b+P+m+0+Q+q+V+J
MD5:	0C045FFD84BAF7C76601574D4A25CE35
SHA1:	9E4CA8D58DE1BC64FE0106E9AD671410FA2EF104
SHA-256:	0F4F0FB3F81B23B82E1E9CFB4B16761CB8CE20C874D03C38E092D0F308098FFB

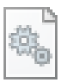
SHA-512:	765BAE3CCC841BFC6C461AB81B206D61D17A5B0950E4689149EF8DE9C249529F3917803911778F800E2B630BBA72D40BDC8DCA1D45627CA27AF410A66F2F59AF
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.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.....-.............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.482102345282002
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	vur7t4SumQ.dll
File size:	545280
MD5:	b4f74ea581aba7c9e44b4a0053d20bfe
SHA1:	eec25f21b828ae3aa2cb49dcd418855e98993ad7
SHA256:	91808c38624d6b8a14a9d86ce4e7fa9815ae08b359748873507db505255c2efe
SHA512:	92c058cccbd01738d562880f3abbb3876875918f3fd67d9339c611956bab47af35c36cc68bcfbd7cf31774896dff86abcf80b6f69a7c246ed3882ef0f76b9327
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZWHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVS
TLSH:	D4C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......2.H.v.&.v.&.v.&.h...o.&.h...2.&.h.....&.Q6].s.&.v.'.9.&.h...w.&.h...w.&.h...w.&.h...w.&.Richv.&.........PE..d.....}b.........."

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800423a8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627D8598 [Thu May 12 22:09:28 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	b268dbaa2e6eb6acd16e04d482356598

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx

Instruction
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007F95DCB65C57h
call 00007F95DCB67DE4h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F95DCB65B00h
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00014D05h]
call dword ptr [0000FC7Fh]
dec esp
mov ebx, dword ptr [00014DF0h]
dec esp
mov dword ptr [esp+58h], ebx
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007F95DCB747DAh
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F95DCB65C93h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax

Instruction
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [00014CB0h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007F95DCB74788h
jmp 00007F95DCB65C74h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [EXP] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x55cf0	0x6f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5544c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x2dffc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x59000	0xe1c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x1d8	.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	0x52000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355279737903	data	5.39248898629	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x5a0a0	0x2de00	data	English	United States
RT_MANIFEST	0x87ea0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	ExitProcess, VirtualAlloc, CompareStringW, CompareStringA, GetTimeZoneInformation, GetLocaleInfoW, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, EncodePointer, DecodePointer, TlsAlloc, FlsGetValue, FlsFree, SetLastError, GetLastError, GetCurrentThread, FlsAlloc, HeapFree, Sleep, GetModuleHandleW, GetProcAddress, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, HeapCreate, HeapDestroy, RtlUnwindEx, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, HeapAlloc, HeapReAlloc, WriteFile, SetConsoleCtrlHandler, FreeLibrary, LoadLibraryA, InitializeCriticalSectionAndSpinCount, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetDateFormatA, GetTimeFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, HeapSize, SetEnvironmentVariableA
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:57:31.352828979 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:31.352888107 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:31.353003979 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:31.378452063 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:31.378474951 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:31.922461987 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:31.922614098 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:32.444144964 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:32.444190025 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:32.444628000 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:32.444740057 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:32.449533939 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:32.492506981 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:33.298507929 CEST	443	49746	23.239.0.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:57:33.298602104 CEST	443	49746	23.239.0.12	192.168.2.3
May 14, 2022 04:57:33.298671961 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:33.298717976 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:33.299304008 CEST	49746	443	192.168.2.3	23.239.0.12
May 14, 2022 04:57:33.299326897 CEST	443	49746	23.239.0.12	192.168.2.3

HTTP Request Dependency Graph

- 23.239.0.12

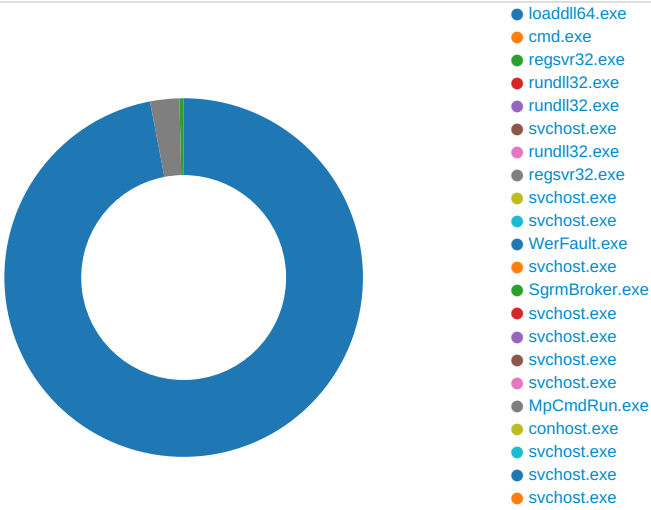
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:57:32 UTC	0	OUT	GET / HTTP/1.1 Cookie: KiooWzMPcOfXY=fouM8Yzji/kWWOstw7ufZfLJVZNbKgAu0/rg1O1uYBIrCdC0Hn0buz3E0IAaKdmkiYMT npxuvuKZurmhslkdzqEo/WOGiaNpRqNGTDnS3NWjmAbRgIb5eYQZk2UR9uqL4TgdvxDweS86PrebjaVImcCon40DEn EEUIMVNTxuR0f8VmRgDyeEw8icmXpZGcn38zfUHFU4HwEY/1nYky2xAGqbEg5n0AAhINzUsF1/jz4cRhxUGMYyFym9 LgWGo4l9QiEz7SPpIitn5mu29JhPUVmTUmQZU555T2rU8XxTaoIJZzh1p6w= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:57:33 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:57:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:57:33 UTC	0	IN	Data Raw: 31 63 63 0d 0a e0 9a a4 19 f3 0f 28 8d 91 6b be 1f 5d 3e ab e8 54 40 c4 5e 06 fa fc 2e bb 46 a8 45 12 84 a1 2e df 74 27 2a 38 07 ab 59 a5 f1 f0 45 f1 cb ab 30 35 09 41 2e b6 76 01 84 77 3a d1 a8 28 2b 69 77 c4 75 05 8f 09 f1 95 4c da 54 59 7c cd 6d 83 68 9a 78 82 04 bf 52 a3 87 59 9c 4d de 51 61 2b d3 95 c8 22 00 a5 b1 60 66 7a 0a f9 53 b3 69 55 f3 13 40 b8 e1 de 43 dd 0d d3 39 98 1e a4 ca 89 85 16 1a aa 87 b9 ff 35 b5 9c ae ba 7a 39 40 04 a5 82 dc 39 f9 01 67 96 67 d3 2d 66 f3 16 27 c1 ba 1a 79 42 e3 4e fa e8 92 d6 18 23 de f6 c4 ee 45 4a 2d df d4 32 9e c4 68 66 bd c5 db 1c 40 db e2 1e a9 09 c0 24 02 97 ab e2 68 cf a9 cc 7f 97 c2 30 f9 50 18 d6 97 4e 25 01 27 7a 24 96 45 ef 39 76 3b 16 b5 7a a1 4f 79 0a c3 d1 d4 40 ad bb 22 6f 5f 02 fe e3 9f 9e 9f 54 8f Data Ascii: 1cc(k]>T@^.FE.t'*8YE05A.vw:(+iwuLTY|mhxRYMQa+"`fzSiU@C95z9@9gg-f'yBN#EJ-2hf@$h0PN%'z$E9v ;zOy@"o_T

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6328, Parent PID: 2912

General

Target ID:	0
Start time:	04:56:51
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\vur7t4SumQ.dll"
Imagebase:	0x7ff625430000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: cmd.exe PID: 6348, Parent PID: 6328

General

Target ID:	1
Start time:	04:56:51
Start date:	14/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\vur7t4SumQ.dll",#1
Imagebase:	0x7ff63f7f0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: regsvr32.exe PID: 6356, Parent PID: 6328

General

Target ID:	2
Start time:	04:56:52
Start date:	14/05/2022

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\vur7t4SumQ.dll
Imagebase:	0x7ff6916b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.301657565.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.301080454.0000000000C20000.00000040.00001000.00020000.00000000.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\System32\JZAnomWmMqlc\LxifZH.dll:Zone.Identifier	success or wait	1	180009356	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6368, Parent PID: 6348

General

Target ID:	3
Start time:	04:56:52
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\vur7t4SumQ.dll",#1
Imagebase:	0x7ff685400000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.298675842.000001BFBC3F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.298420747.0000000180001000.00000020.00001000.00020000.00000000.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6376, Parent PID: 6328

General

Target ID:	4

Start time:	04:56:52
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\vur7t4SumQ.dll,DllRegisterServer
Imagebase:	0x7ff685400000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.298460675.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.298751504.000001C078260000.00000040.00001000.00020000.00000000.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6424**, Parent PID: **568**

General

Target ID:	5
Start time:	04:56:55
Start date:	14/05/2022
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: rundll32.exe PID: **6444**, Parent PID: **6328**

General

Target ID:	6
Start time:	04:56:56
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\vur7t4SumQ.dll,DllUnregisterServer
Imagebase:	0x7ff685400000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.304486161.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.305654507.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.330907798.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.304665909.000001CC60A20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.306126418.000001CC60A20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.331438414.000001CC60A20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6512**, Parent PID: **6356**

General

Target ID:	7
Start time:	04:56:59
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JZAnomWmMqlc\LxifZH.dll"
Imagebase:	0x7ff6916b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.808923967.0000000002C00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.810121562.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **6536**, Parent PID: **568**

General

Target ID:	9
Start time:	04:57:01
Start date:	14/05/2022
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

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: svchost.exe PID: **6632**, Parent PID: **568**

General

Target ID:	10
Start time:	04:57:02
Start date:	14/05/2022
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

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: **6652**, Parent PID: **6444**

General

Target ID:	11
Start time:	04:57:03
Start date:	14/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6444 -s 316
Imagebase:	0x7ff6c7fd0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
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	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F04.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F34.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 11 fd 7f 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	9528	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 38 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 4b fd 35 02 00 00 54 05 00 00 fd 03 00 00 2c 19 00 00 08 fd 7f 62 00 00 00 00 00 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 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 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 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 00	UB8%LwK5T,b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	10252	1232	16 02 14 00 00 00 00 00 fd 0b fd 60 fd 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 00 fd 02 00 00 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 02 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd fd 47 fd fd 00 00 00 40 fd 47 fd fd 00 00 00 16 02 14 00 00 00 00 00 00 00 00 00 00 00 00 00 32 5b fd 60 fd 01 00 00 0a 00 00 00 00 00 00 00 10 04 fd fd 0f 00 00 fd fd fd fd fd fd fd fd 5a fd 60 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 10 fd 60 fd 01 00 00 00 00 00 00 00 00 00	`_3++S++XG@G2[`Z`8`	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	1632	168	30 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 04 00 00 0c 28 00 00	0(	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	15180	20	55 00 00 00 00 fd 02 fd 01 00 00 00 2e 00 00 00 fd 40 00 00	U.@	success or wait	85	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	16544	46	01 1d 08 00 1d 64 15 00 1d 34 14 00 1d fd 13 fd 11 70 10 50 01 1f 0b 00 1f fd 1d 00 1f 74 1c 00 1f 64 1b 00 1f 34 1a 00 1f 01 18 00 14 50	d4pPtd4P	success or wait	84	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	51226	8192	00 00 00 00 00 00 00 00 00 00 58 fd fd 00 00 00 00 40 57 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d fd fd 00 00 00 00 00 00 00 00 00 00 00 2c 19 00 00 00 00 00 00 40 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	X@W-,@,	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	11484	1232	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 47 fd fd 00 00 00 fd fd fd fd fd fd fd fd fd 47 fd fd 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 68 fd 47 fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 47 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	3++S++FGGhGGh	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	1900	48	40 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 2d fd fd 00 00 00 18 fd 57 fd fd 00 00 00 fd 05 00 00 3a 55 00 00 fd 04 00 00 7c 36 00 00	@ -W:U|6	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	9534	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	4556	4320	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b fd 27 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 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 51 01 00 00 04 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 fd 02 fd 01 00 00 00 28 59 63 fd fd 67 fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 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 00 00 00 00 00 00 51 01 00 00 00 00 00	<2|h+'BB?#`A pQuu(YcgQ	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	8884	644	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 fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 17 fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 45 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 17 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 42 06 00 00 00 00 00 2e 23 11 4d 00 00 00 00 fd 66 fd 19 00 00 00 00 df 27 20 00 00 00 00 fd 02 01 00 00 00 00 fd fd 00 00 4c 0c 01 00 4d fd 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 42 06 00 65 fd 33 00 fd fd 01 00 fd fd 13 00 00 00 00 00 17 54 21 00 6f 5e 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 01 00	Zb`E@B.#Mf' LMBe3T!o^+	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	59418	5056	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 00 50 00 61 00 63 00 6b 00 65 00 74 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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C4.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 7c 10 00 00 38 12 00 00 05 00 00 00 54 05 00 00 4c 3b 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 0c 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	|8TL;`8T"$	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6444</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1080	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 30 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11065</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1230	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1316	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1376	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1430	96	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 32 00 32 00 30 00 33 00 35 00 30 00 34 00 30 00 39 00 31 00 31 00 33 00 36 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>22035 04091136 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1536	80	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 32 00 32 00 30 00 33 00 34 00 30 00 38 00 34 00 33 00 37 00 32 00 34 00 38 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>2203408437248</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1626	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 32 00 36 00 33 00 32 00 38 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>26328</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1712	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 35 00 32 00 34 00 36 00 37 00 32 00 30 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>105246720</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1822	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 37 00 32 00 30 00 30 00 37 00 36 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>7200768</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	1912	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 31 00 30 00 36 00 37 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>106768</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2036	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 31 00 30 00 36 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>106568</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2144	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 32 00 31 00 35 00 34 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>21544</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2278	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 32 00 31 00 31 00 39 00 32 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>21192</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2396	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 38 00 31 00 34 00 35 00 32 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>1814528</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2482	96	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 30 00 31 00 34 00 36 00 32 00 30 00 31 00 36 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>101462016</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2588	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 38 00 31 00 34 00 35 00 32 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>1814528</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2668	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2720	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2768	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2814	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 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>BEX64</EventType>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2870	4	0d 00 0a 00		success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2874	2	09 00		success or wait	18	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	2878	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 76 00 75 00 72 00 37 00 74 00 34 00 53 00 75 00 6d 00 51 00 2e 00 64 00 6c 00 6c 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>rundll32.exe_vur7t4SumQ.dll</Parameter0>	success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3670	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3710	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3714	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3716	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	3762	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4322	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4368	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4406	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4410	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4414	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4516	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 64 00 79 00 63 00 6b 00 72 00 67 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>dyckrg, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4630	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 64 00 79 00 63 00 6b 00 72 00 67 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>dyckrg7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4734	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4862	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 35 00 39 00 36 00 35 00 30 00 34 00 36 00 39 00 37 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>1596504697</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	4952	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5054	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5058	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5062	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5136	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5182	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5224	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</UEFISecureBootEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5326	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5368	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5400	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5652	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5684	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 35 00 2d 00 31 00 34 00 54 00 31 00 31 00 3a 00 35 00 37 00 3a 00 30 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-14T11:57:07Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5784	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5788	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	5792	262	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 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 34 00 34 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 35 00 34 00 36 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 35 00 34 00 36 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 00 3d 00 22	<Process AsId="400" PID="6444" UptimeMS="4546" TimeSinceCreationMS="4546" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6054	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6058	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6064	182	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 35 00 32 00 39 00 36 00 30 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5529600" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6254	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6274	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6278	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6280	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6318	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6322	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6324	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6362	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6366	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6370	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 30 00 64 00 32 00 61 00 38 00 39 00 34 00 2d 00 63 00 37 00 36 00 32 00 2d 00 34 00 61 00 35 00 64 00 2d 00 62 00 39 00 65 00 65 00 2d 00 63 00 63 00 61 00 62 00 38 00 61 00 33 00 37 00 38 00 35 00 38 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>80d2a894-c762-4a5d-b9ee-ccab8a37858d</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6468	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6472	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6476	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 35 00 2d 00 31 00 34 00 54 00 31 00 31 00 3a 00 35 00 37 00 3a 00 30 00 37 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>2022-05-14T11:57:07Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6580	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6620	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BF0.tmp.WERInternalMetadata.xml	6624	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB24.tmp.xml	0	4892	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 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 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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\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	152	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_vur_4cd58e58b1e637f1367f31dafe24a2e5d883329_67e37b4c_19aab41b\Report.wer	9582	48	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 2d 00 31 00 34 00 39 00 39 00 33 00 39 00 30 00 38 00 36 00 39 00	MetadataHash=-1499390869	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC738DE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFC73901D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{716106eb-4c16-3a41-7175-039016bd5bee}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFC73901D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E AF DE FC 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC739007CB	RegSetValueExW

Analysis Process: svchost.exe PID: **6696**, Parent PID: **568**

General	
Target ID:	12
Start time:	04:57:04
Start date:	14/05/2022
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: **6908**, Parent PID: **568**

General	
Target ID:	13
Start time:	04:57:12
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7273c0000
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: **6960**, Parent PID: **568**

General	
Target ID:	14
Start time:	04:57:13
Start date:	14/05/2022

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

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: **6988**, Parent PID: **568**

General

Target ID:	15
Start time:	04:57:14
Start date:	14/05/2022
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: **6328**, Parent PID: **568**

General

Target ID:	19
Start time:	04:57:44
Start date:	14/05/2022
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: 5608, Parent PID: 568

General

Target ID:	23
Start time:	04:57:55
Start date:	14/05/2022
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

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 6856, Parent PID: 6988

General

Target ID:	25
Start time:	04:58:15
Start date:	14/05/2022
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
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 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 53 00 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 35 00 38 00 3a 00 31 00 36 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat May 14 2022 04:58 :16	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 53 00 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 35 00 38 00 3a 00 31 00 36 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 04:58:16	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 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **6956**, Parent PID: **6856**

General

Target ID:	26
Start time:	04:58:16
Start date:	14/05/2022
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: **5324**, Parent PID: **568**

General

Target ID:	27
Start time:	04:58:20
Start date:	14/05/2022
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: **6056**, Parent PID: **568**

General

Target ID:	31
Start time:	04:58:55
Start date:	14/05/2022
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: **6568**, Parent PID: **568**

General

Target ID:	35
Start time:	04:59:19
Start date:	14/05/2022
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