ID: 631916
Sample Name: 3vYbe1bYFd.dll
Cookbook: default.jbs
Time: 23:40:40
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

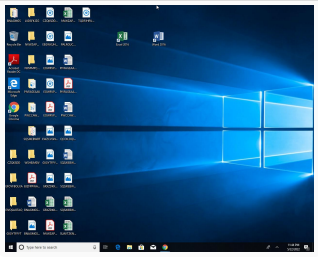
Windows Analysis Report

3vYbe1bYFd.dll

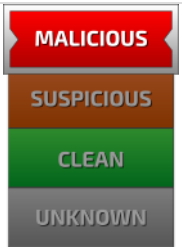
Overview

General Information

Sample Name:	3vYbe1bYFd.dll
Analysis ID:	631916
MD5:	bf2f633fde70f18…
SHA1:	b3aedb0275ec4f..
SHA256:	663127c151c319..
Tags:	exe
Infos:	



Detection



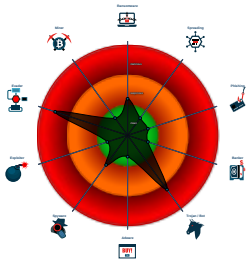
Emotet

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Multi AV Scanner detection for dom…
- Changes security center settings (n…
- Machine Learning detection for sam…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6316 cmdline: loaddll64.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6332 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6352 cmdline: rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6532 cmdline: C:\Windows\system32\WerFault.exe -u -p 6352 -s 324 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - regsvr32.exe (PID: 6340 cmdline: regsvr32.exe /s C:\Users\user\Desktop\3vYbe1bYFd.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 6452 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SyeNstLIaswClq\bXSPARJszx.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - rundll32.exe (PID: 6360 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6544 cmdline: C:\Windows\system32\WerFault.exe -u -p 6360 -s 316 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - rundll32.exe (PID: 6484 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6700 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 7044 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7088 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7124 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4780 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5084 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4264 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3808 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3756 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 2216 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6676 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.250134876.000001E8B52C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.634375590.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.634110300.0000000001290000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.261630591.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000000.249906990.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.1e8b52c0000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.1290000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.1e8b52c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.ee0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.1e8b52c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 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

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

E-Banking Fraud

Yara detected Emotet

Copyright Joe Security LLC 2022

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

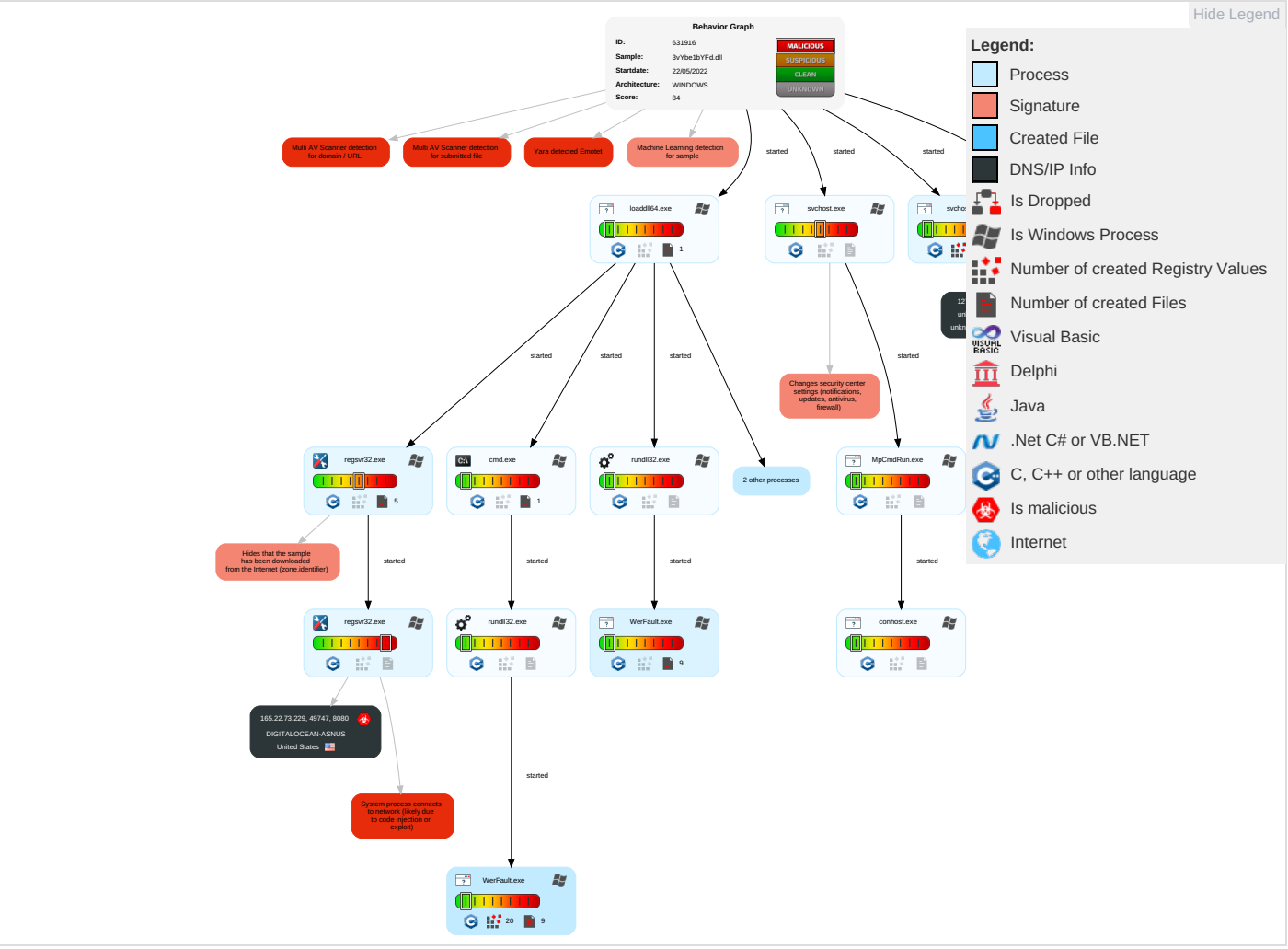
Mitre Att&ck Matrix

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 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	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	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	6 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	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	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	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 Hidden Files and Directories	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	2 Obfuscated Files or Information	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 Regsvr32	Proc Filesystem	2 5 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 Rundll32	/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 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph



Screenshots

Thumbnails

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

Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
3vYbe1bYFd.dll	38%	Virustotal		Browse
3vYbe1bYFd.dll	44%	ReversingLabs	Win64.Trojan.Emotet	
3vYbe1bYFd.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.ee0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.1ef360c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1e8b52c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.1e8b52c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.1ef360c0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.1ef360c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.1e8b52c0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.1290000.0.unpack	100%	Avira	HEUR/AGEN.1215461		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://165.22.73.229/	7%	Virustotal		Browse
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/tem	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://165.22.73.229/:	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/tg5	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

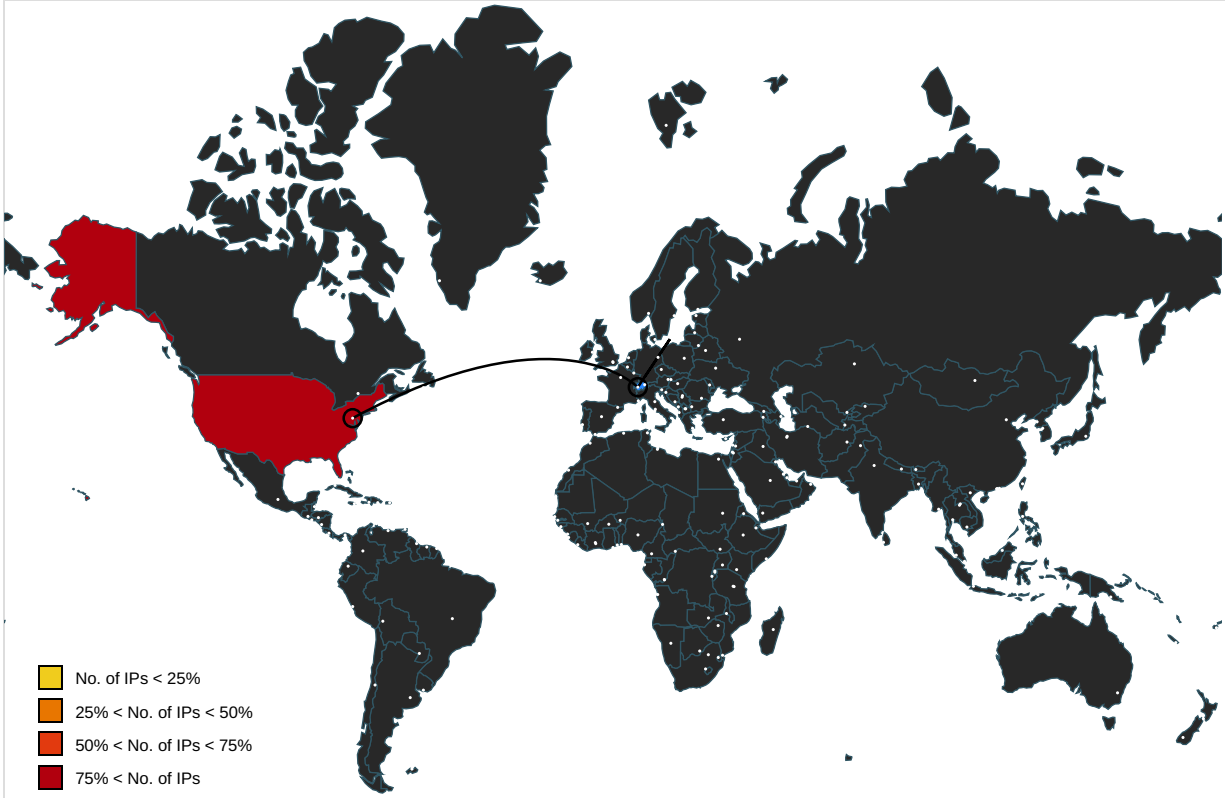
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001B.00000003.392520522.0000014C9BB8A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000013.00000003.318072301.0000024089045000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000013.00000002.318486937.000002408903D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000013.00000002.318486937.000002408903D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 00000013.00000003.317776474.0000024089067000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.318540112.0000024089069000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000013.00000002.318519840.0000024089056000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.317967284.000002408904D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318154497.0000024089050000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000013.00000002.318486937.000002408903D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000013.00000003.296155575.0000024089030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000013.00000003.318072301.0000024089045000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/	regsvr32.exe, 00000007.00000002.633798852.00000000010F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.539150633.00000000010F1000.00000004.00000020.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000018.00000002.603857311.0000029038E88000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000002.419979853.0000014C9B2EA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000013.00000002.318498118.000002408904B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318005723.0000024089049000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001B.00000003.400604746.0000014C9BBAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.400585855.0000014C9BBAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.400650100.0000014C9C002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.400622481.0000014C9BB88000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.400633517.0000014C9BB99000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000013.00000002.318442092.0000024089013000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.318486937.000002408903D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000013.00000002.318493323.0000024089042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318089937.0000024089041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000011.00000002.633990708.000001E86223F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000013.00000003.296155575.0000024089030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 0000001B.00000003.388278316.0000014C9C003000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388243624.0000014C9C002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388214343.0000014C9BB9A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388325169.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388305706.0000014C9BB88000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388351293.0000014C9C019000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388226079.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000013.00000003.318005723.0000024089049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000013.00000003.296155575.0000024089030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000013.00000002.318498118.000002408904B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318005723.0000024089049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001B.00000003.392520522.0000014C9BB8A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000013.00000003.296155575.0000024089030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000013.00000002.318493323.0000024089042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318089937.0000024089041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229:8080/tem	regsvr32.exe, 00000007.00000002.633798852.00000000010F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.539150633.00000000010F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 00000013.00000003.318036154.0000024089040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318089937.0000024089041000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229:8080/	regsvr32.exe, 00000007.00000002.633798852.00000000010F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.539150633.00000000010F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001B.00000003.388278316.0000014C9C003000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388243624.0000014C9C002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388214343.0000014C9BB9A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388325169.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388305706.0000014C9BB88000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388351293.0000014C9C019000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388226079.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001B.00000003.388278316.0000014C9C003000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388243624.0000014C9C002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388214343.0000014C9BB9A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388325169.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388305706.0000014C9BB88000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388351293.0000014C9C019000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.388226079.0000014C9BBAA000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001B.00000003.392520522.0000014C9BB8A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000013.00000002.318478368.0000024089039000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.296155575.0000024089030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/:	regsvr32.exe, 00000007.00000002.633798852.00000000010F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.539150633.00000000010F1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000013.00000002.318498118.000002408904B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.318005723.0000024089049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000011.00000002.633990708.000001E86223F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000013.00000002.318442092.0000024089013000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000013.00000003.317849654.0000024089061000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 0000001B.00000003.392520522.0000014C9BB8A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/tg5	regsvr32.exe, 00000007.00000002.633798852.00000000010F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.539150633.00000000010F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000013.00000002.318486937.000002408903D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000011.00000002.633990708.000001E86223F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000013.00000003.318005723.0000024089049000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.22.73.229	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631916
Start date and time: 22/05/202223:40:40	2022-05-22 23:40:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3vYbe1bYFd.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	37
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

Copyright Joe Security LLC 2022

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winDLL@30/16@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73% (good quality ratio 39.9%) • Quality average: 34.3% • Quality standard deviation: 37.7%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.20, 20.42.73.29, 8.238.85.126, 67.26.73.254, 8.241.126.249, 67.26.81.254, 8.252.5.126, 23.35.236.56, 20.223.24.244
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
23:42:19	API Interceptor	1x Sleep call for process: svchost.exe modified
23:43:08	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):	0.24942354822409118
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4o:BJiRdwfu2SRU4o
MD5:	E501EB118255C17E5564CECFF98437EF
SHA1:	324BB9C16249712A8EA1724E4D81F9CE8488A513
SHA-256:	72F4692B38408692F6F149F1569D763C5AAD19E1944C23DBDAF9CF87E5734B17
SHA-512:	B8741B19F4F62427AB0CC9E2FC64B988DAF4EA27C72E4096CCFDDF1DB83ED6C6F31A293BAF804499CE6A604ADC14CDD82FC407600EEB46017E65B99DA9A03 CFF
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 0x780aa5ad, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25065884597366206
Encrypted:	false
SSDEEP:	384:Pnc+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:PnDSB2nSB2RSjlK/+mLesOj1J2
MD5:	290F1FC77BF1F7667382431A8200BF72
SHA1:	A1617EB579E65E1239764245BD17022A28479168
SHA-256:	EC5017C8021670AF09AF3ABFAB223B3A6A14507754349E8AB337CA44AAE04577
SHA-512:	DDE2A30724832B25AB1A3E1F9E3AA77A695EEEA8B427C82588045F207BF6E948F6A436443B0FC1174DE267A2A93D6F3C82A7182C6677285A805F7886A1E39DC2
Malicious:	false
Preview:	x..... .....e.f.3...w.....).....,...zy..*...z..h.(.....,...zy...).....3...w.....B.....@..... ....?..._.,...zy.....T9.2.,...zy..... .....

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

Process:	C:\Windows\System32\svchost.exe

File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07711251262311615
Encrypted:	false
SSDEEP:	3:L/R7v2Pjs4bgOVbY///95JP+All3VkttlmlnI:DRr2blVVbYXF5J2A3
MD5:	2155A7A49770683AB923F0CF6BEEFAB4
SHA1:	15C5BEBFB3FE6E2BBC1961488B37470343515789
SHA-256:	6E16876658BEC2680303E129C742727CEEC82F9580A53E79CF7D2C3566652373
SHA-512:	CCFAAF7171DD2917EED561AD5DB0BC75B19E876446648DC973F27416924A6057B4859A592570F93B8CEF7A35CD6646767D51D31C2E8FE823926CF12DB10D4A7
Malicious:	false
Preview:	c.&.....3...w...*...z...,...zy.....,...zy..,...zy..\...,...z.....T9.2.,...zy..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185\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):	0.7850594562087836
Encrypted:	false
SSDEEP:	96:J4XFIAimvJPny5jD55oe7Rb6tpXIQcQZc6nfcEtcw3iXaXz+HbHgSQgJPb2IDV9e:sNimvJKiHXjf3UjI9/u7saS274ltSE
MD5:	20963099448C912BA8EDE45AE27F7FB4
SHA1:	162DCEC61D5B69AA0F516C6E6C64A1E696D02C17
SHA-256:	68A7CEBF8431BB9FB218963E6F328E4E1D4F25969B2BAE0F533A8C19F71B021B
SHA-512:	1B4500E6C306FB062EEFFAF4C45A3C64CE9CB4AE95BCE84468C8852DBDE90B477496C1CF6FDFF20B899DC38D84B2416660848C65A13C0A05E27616652332FCE
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.6.1.7.0.6.4.0.2.9.7.1.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.6.1.7.0.8.2.4.6.7.1.9.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.5.7.1.a.a.a.3.-.a.6.d.3.-.4.f.a.f.-.9.3.1.3.-.0.1.5.c.6.b.c.b.b.3.7.b...I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.1.c.8.0.8.c.5.-.8.8.5.4.-.4.8.1.7.-.8.4.a.5.-.a.e.0.8.2.6.f.b.5.2.2.1.....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._.3.v.Y.b.e.1.b.Y.F.d...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.d.8.-.0.0.0.1.-.0.0.1.d.-.d.e.a.a.-.f.4.2.8.7.0.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2\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):	0.7845313089953005
Encrypted:	false
SSDEEP:	96:DZF9AiGvJPny2jD55oe7Rb6tpXIQcQZc6nfcEtcw3iXaXz+HbHgSQgJPb2IDV9wi:IIiGvJK1HXjf3UjI9/u7saS274ltSEu
MD5:	3F21882C9BA803C2E1A4BAE32BF35D90
SHA1:	43911DE3E3B7873BD5071307B67DB062FA5A0646
SHA-256:	2B8507B5895390767EEABC7052F164F350DD2FF1715FCC9DB76F556556B8C7C3
SHA-512:	DD64518FA8030DBC8D687F4AD23B8CA2C914975AFCB50178EEBB5DD24EFE781DCBD1B890040DFB4BC9D34B90B7B1F31858FB466DB2EC8AE06363417D590B3DAB
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.6.1.7.0.6.3.5.2.6.6.9.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.6.1.7.0.8.0.0.8.9.1.1.3.....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.=.3.7.d.7.b.1.7.9.-.3.8.0.6.-.4.1.4.1.-.a.6.6.6.-.9.c.2.2.c.9.a.b.a.c.0.2...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.=.9.2.9.3.4.d.b.4.-.1.1.a.1.-.4.8.b.5.-.9.6.a.4.-.f.e.b.a.0.a.f.c.b.5.2.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.3.v.Y.b.e.1.b.Y.F.d...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.d.0.-.0.0.0.1.-.0.0.1.d.-.6.a.e.c.-.b.8.2.8.7.0.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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\WERD56F.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 06:41:46 2022, 0x1205a4 type

Category:	dropped
Size (bytes):	62968
Entropy (8bit):	2.34910603463446
Encrypted:	false
SSDEEP:	384:ci04cSe2YqH2JDRCx82cldYnK7ED6KspAyba:cifMqH2JlCP+h7ED8F
MD5:	0513F778BB2EAEEE790A6F85796599CB
SHA1:	4F1B67A579A8B829C89CA2EBBC57C221A95070A5
SHA-256:	9C64F6F41FB48FC9F9541D8B9AB910DDE3445E32BC33B20C640B9A9577CB5848
SHA-512:	C801C41C29FA4A2AFA7FDAA112277561C6CAA4AADEF0E67AA5584AE53B199E91639E7B737C7DB1D6CC574543E7AEBC4C54221064A29C9D55224B9AD5C9BB2759
Malicious:	false
Preview:	MDMP..... .....,.b.....8.....$...d;.....`.....8.....T.....0.....".....$.....U.....B.....P%... ...Lw.....T.....,.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 06:41:46 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64372
Entropy (8bit):	2.3058405441422507
Encrypted:	false
SSDEEP:	384:PGK04cSe2YqH2cHcQCZwZe0cldYn4yyaWMwg1xq5:eKfMqH2c8QC10+/Mw
MD5:	68E0A9DDAD26C7B237C1A0AA38D6B50E
SHA1:	1F3AEB340EBA49229136E10409626013F89EBDBB
SHA-256:	76D1C5762D752E1124ECD2AE536C14DAF10F0649111BF17DE4EC69B86BCEDB1A
SHA-512:	68F999FCDE6C98DF9C6B42E0DE68DF7096179ED2190DC39667658EEC7BB007A051331E046BEFCA1B741EC5E5D87B242218F273DDF4CD73349DAFFA132506A1CA
Malicious:	false
Preview:	MDMP..... .....,.b.....8.....4...d;.....`.....8.....T.....".....$.....U.....B.....P%... ...Lw.....@.....T.....,.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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):	8842
Entropy (8bit):	3.699804333734504
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiHI5UB8FT6YH3YgmfYMUS98uCprk89bUlUfecm:RrlsNio5UB8FT6YXYgmfYMUS983U2fc
MD5:	AEB61B0B220AEBD4CB5351F84DE37CE5
SHA1:	B712945BEACEFF038414BA620786E1746F39820D
SHA-256:	D6BD47F5C1E75A484C54F6E76CF5AEC2A2895D94D66DAF61584148495003896C
SHA-512:	DBDF4B24FCBA5ACD2DD3EBB432D803CEDC50510AC9025728BA52908535948A9C8BF826F5786D78AFA76107AED7BB3527F39A3810ED4E832F8FC5C568BA0FA2D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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):	8836
Entropy (8bit):	3.697670183455422

Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimArUB8TU6YLl4UgmfYMUS98uCpr289bULUfJcm:RrlsNiZrUB8TU6YZ5gmfYMUS98JUofH
MD5:	028FD7637582B07FAC3661961F5BA83F
SHA1:	A02ED00AF9AC0FAF01B743E60987F6D3DD8D14F0
SHA-256:	A9FF1B8D311E331AD88411D1623B191121E3276FBAE017B79F1AC33A200FA9CA
SHA-512:	F2411D803C0C8EE081F8E2352D46900A9372217147F6C4F58D9275C20F5899B8CA677E465528B13A09872CC8F92DA3AE377438F1263612715B69EC379856024D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.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):	4.499740395775507
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9gkkeWgc8sqYjgy8fm8M4JC6jC6KznFySyq8vh6KzGZESC5S6:uITflqkkfgrsqYknJ9BMWU1Vv0d
MD5:	9284B196B4D7881EB02493CCE769E1D5
SHA1:	E762F147CB2D3B01DB55AB9C067B6FC61E4F589C
SHA-256:	C63652EEEF2F2616E7B410DA507D2CB9C4991642F82815D90BD09EE8AFB490CE
SHA-512:	ECE062F2A8210F4DB4242757F6D184D4E0427E16D1AC494039A316B63627DA520B88B6578A4045A3BB187E292EB583AF4CCB24DEAE0CC8063EA1D9BBB33279(8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1527352" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.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):	4.498989978631906
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9gkkeWgc8sqYj3q8fm8M4JC6jC6KznFLRyq8vh6Kz3mZESC5E:uITflqkkfgrsqYjfJ9BkWUUmVvRd
MD5:	123495C5DE2E674665BD93ECC73D86E1
SHA1:	15B71D59E47A8A389E6C4214EF63D295D674F592
SHA-256:	7ADB19B8D55266DC12EEEBAD7B650B5776EBC017BF2BBBD4C4F5E85B0AB62E2F
SHA-512:	0D76A048F07EF1E7189DB508745A45FA62F03771FA0D2F0BC941199AE17693E8CF3F5077A8B3D64AABB61D184374FD6DF6280E799E88A9F1C3B0684AA4EC031(
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="1527352" />.. <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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3

<table>
<tr><td>SHA1:</td><td>4A3C330954F9F65A2F5FD7E55800E46CE228A3E2</td></tr>
<tr><td>SHA-256:</td><td>998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E</td></tr>
<tr><td>SHA-512:</td><td>D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994
76</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MSCF....(.......,...................I........y.........Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.......S..9.s.....3H.Mh......qV.=M6.=.4.F.....V:F..]......
B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.......Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A...<br>....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P ......|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9......sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:......
...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.......nP...2.Q8...O........M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9......^...CU......O....X.`........._.gU...*..V.{V6..m
..D.-|.Q.t.7.....9.~....[...I.<e...~$..>......s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@......2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.......I...</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\regsvr32.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>modified</td></tr>
<tr><td>Size (bytes):</td><td>330</td></tr>
<tr><td>Entropy (8bit):</td><td>3.0802324314549296</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6:kKN3oJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:l/kPlE99SNxAhUesE1</td></tr>
<tr><td>MD5:</td><td>11D24A43AC8D863CD6F2C610B245865B</td></tr>
<tr><td>SHA1:</td><td>3EADAA6EABE44351C09C1048EAA646F7215B0E72</td></tr>
<tr><td>SHA-256:</td><td>326EEB8F5D477856745027EA3AC50D977EEA4843ECC0EE5397BA93473A9B8BD4</td></tr>
<tr><td>SHA-512:</td><td>5B53FE39771F2B75BC78DC73EA0AF88C5B3E4C0E94352416BCA62E60FBF8480BADC58BFDA887D2D96E00A196C2A4FF5D144B5CA39D0B6A581E1CD2EEBF5A1
CCE</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>p...... ....:pn..(... ....3k/"[......(...........(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.
s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\svchost.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with no line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>55</td></tr>
<tr><td>Entropy (8bit):</td><td>4.306461250274409</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y</td></tr>
<tr><td>MD5:</td><td>DCA83F08D448911A14C22EBCACC5AD57</td></tr>
<tr><td>SHA1:</td><td>91270525521B7FE0D986DB19747F47D34B6318AD</td></tr>
<tr><td>SHA-256:</td><td>2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9</td></tr>
<tr><td>SHA-512:</td><td>96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA
CA</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Windows Defender\MpCmdRun.exe</td></tr>
<tr><td>File Type:</td><td>Little-endian UTF-16 Unicode text, with CRLF, CR line terminators</td></tr>
<tr><td>Category:</td><td>modified</td></tr>
<tr><td>Size (bytes):</td><td>9062</td></tr>
<tr><td>Entropy (8bit):</td><td>3.1633729363437952</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z7+Q:j+s+v+b+P+m+0+Q+q+c+Q</td></tr>
<tr><td>MD5:</td><td>ACA3ECDDF974F39302A739DDA63FF120</td></tr>
<tr><td>SHA1:</td><td>C8BFD13E7845908F4319BB3C61F19D99655BBCB9</td></tr>
<tr><td>SHA-256:</td><td>BABB566A83BDB3F727BB82D6B1779BC028508BABC308468DA30731B482E76CFD</td></tr>
<tr><td>SHA-512:</td><td>26E897355A68C15924722BFF0A7A6210836861A33833633517465B95306FE56205F98630FA789131D489C82BE1B0AF462E9C7BC5CF9A8BEB3C93CA346B5FCFE9</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.........-.....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.....-
.-............-.</td></tr>
</table>

Copyright Joe Security LLC 2022

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.152740840989443
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:	3vYbe1bYFd.dll
File size:	371200
MD5:	bf2f633fde70f181cc81fe6dffb048e7
SHA1:	b3aedb0275ec4f55f21a2e672e87c96b36f38959
SHA256:	663127c151c31915e66da770d7e2109306f1e2bf12acce04bb3defcb0de92134
SHA512:	c44fd444e946228a5892cead87ef9a79c2ab6f0b47205ca6bd34728b561920e805330f9c6d2ccc8917555e6deb2e785c1615f0427fa78001326260b53bef883e
SSDEEP:	6144:hlNuuXQASByX7RxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7jy/BJ7rGTK/V3
TLSH:	D9848E46F7F551E5E8F7C13889A23267F9317C948B38A7CB8A44466A4F70BA0E93D701
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik...k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d....{.b....."

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180003580
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:	0x62877BF5 [Fri May 20 11:31:01 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:	ad5c5b0f3e2e211c551f3b5059e614d7

Entrypoint Preview

Instruction
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 28h
cmp dword ptr [esp+38h], 01h
jne 00007F7FDD045407h

Instruction
call 00007F7FDD04A767h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007F7FDD045414h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 48h
mov dword ptr [esp+20h], 00000001h
cmp dword ptr [esp+58h], 00000000h
jne 00007F7FDD045412h
cmp dword ptr [00028DE8h], 00000000h
jne 00007F7FDD045409h
xor eax, eax
jmp 00007F7FDD045524h
cmp dword ptr [esp+58h], 01h
je 00007F7FDD045409h
cmp dword ptr [esp+58h], 02h
jne 00007F7FDD045450h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007F7FDD04541Ah
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call dword ptr [0001ED83h]
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
je 00007F7FDD045419h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007F7FDD04516Ah
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007F7FDD045409h

Instruction
xor eax, eax

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [EXP] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2aab0	0x84	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a1e4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x2e9fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x294	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x298	.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	0x203fa	0x20400	False	0.405439983043	zlib compressed data	5.75409030586	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x8b34	0x8c00	False	0.275474330357	data	4.41578795519	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x3798	0x1400	False	0.161328125	data	2.21550179132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.5048828125	data	5.08183440168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2e9fc	0x2ea00	False	0.887011980563	data	7.85049584102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x6fc	0x800	False	0.21435546875	data	2.34217115221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_FONTDIR	0x300a0	0x2e800	data	English	United States
RT_MANIFEST	0x5e8a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

Copyright Joe Security LLC 2022

DLL	Import
KERNEL32.dll	GetTimeFormatA, GetDateFormatA, GetThreadLocale, FileTimeToSystemTime, VirtualAlloc, ExitProcess, CloseHandle, CreateFileW, SetStdHandle, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, RtlUnwindEx, EncodePointer, FlsGetValue, FlsAlloc, FlsFree, SetLastError, GetLastError, HeapSize, HeapValidate, IsBadReadPtr, DecodePointer, GetProcAddress, GetModuleHandleW, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, GetStartupInfoW, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, GetVersion, HeapCreate, HeapDestroy, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, EnterCriticalSection, LeaveCriticalSection, GetACP, GetOEMCP, GetCPInfo, IsValidCodePage, HeapAlloc, GetModuleFileNameW, HeapReAlloc, HeapQueryInformation, HeapFree, WriteFile, LoadLibraryW, LCMapStringW, MultiByteToWideChar, GetStringTypeW, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, RaiseException, RtlPcToFileHeader, SetFilePointer, GetConsoleCP, GetConsoleMode, FlushFileBuffers
USER32.dll	MessageBoxA
ole32.dll	CoTaskMemFree, CoTaskMemAlloc, CoLoadLibrary

Exports

Name	Ordinal	Address
AddIn_FileTime	1	0x180001140
AddIn_SystemTime	2	0x1800010b0
DllRegisterServer	3	0x180003110

Possible Origin

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

Network Behavior

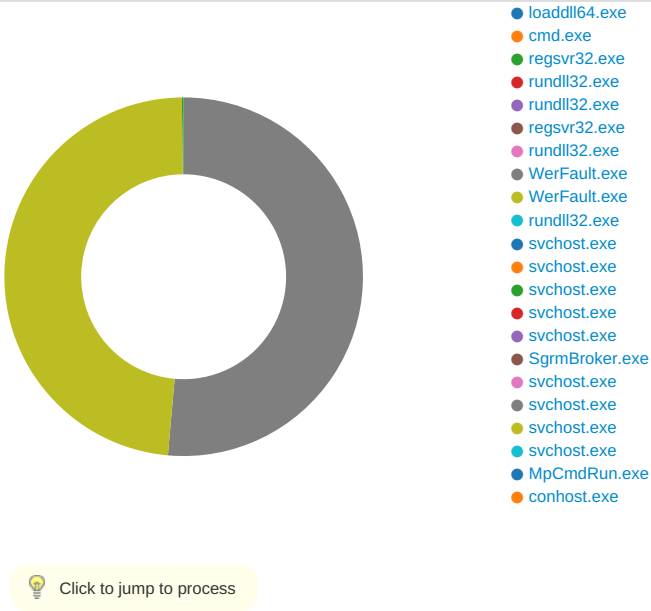
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 23:42:09.319221973 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:09.361620903 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:09.361771107 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:09.378669024 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:09.421169996 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:09.430986881 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:09.431035995 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:09.431132078 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:09.431164980 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:11.646833897 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:11.689599037 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:11.692980051 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:11.695926905 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:11.779875994 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:11.946090937 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:11.949352980 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:14.944626093 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:14.944693089 CEST	8080	49747	165.22.73.229	192.168.2.3
May 22, 2022 23:42:14.944951057 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:42:14.945008039 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:43:59.459301949 CEST	49747	8080	192.168.2.3	165.22.73.229
May 22, 2022 23:43:59.459351063 CEST	49747	8080	192.168.2.3	165.22.73.229

Copyright Joe Security LLC 2022

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6316**, Parent PID: **612**

General

Target ID:	0
Start time:	23:41:39
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll"
Imagebase:	0x7ff6fd790000
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: **6332**, Parent PID: **6316**

General

Target ID:	1
Start time:	23:41:40
Start date:	22/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1
Imagebase:	0x7ff7072e0000

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: 6340, Parent PID: 6316

General

Target ID:	2
Start time:	23:41:40
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\3vYbe1bYFd.dll
Imagebase:	0x7ff6b2260000
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: 00000002.00000002.250685839.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250530772.0000000000EE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\SyeNstLIaswClq\bXSPARJszx.dll:Zone.Identifier	success or wait	1	18002C502	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: 6352, Parent PID: 6332

General

Target ID:	3
Start time:	23:41:40
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1
Imagebase:	0x7ff756220000
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: 00000003.00000000.250134876.000001E8B52C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.261630591.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.249906990.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.248944138.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.261749514.000001E8B52C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.249070931.000001E8B52C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6360**, Parent PID: **6316**

General

Target ID:	4
Start time:	23:41:41
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_FileTime
Imagebase:	0x7ff756220000
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: 00000004.00000000.250231200.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.249310347.000001EF360C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.249207974.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.261251343.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.261348422.000001EF360C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.250432192.000001EF360C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6452**, Parent PID: **6340**

General

Target ID:	7
Start time:	23:41:43
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SyeNstLIaswClq\bXSPARJszx.dll"
Imagebase:	0x7ff6b2260000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.634375590.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.634110300.0000000001290000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6484**, Parent PID: **6316**

General

Target ID:	8
Start time:	23:41:44
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_SystemTime
Imagebase:	0x7ff756220000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **6532**, Parent PID: **6352**

General

Target ID:	10
Start time:	23:41:45
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6352 -s 324
Imagebase:	0x7ff6c7fd0000
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	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3CA.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3EA.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2c fd 62 fd 05 12 00 00 00 00 00	MDMP ,b	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.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 50 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 7f 2f 02 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 fd 2c fd 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBP%LwT,b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	10276	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 22 56 fd 7f 00 00 40 14 fd fd fd 7f 00 00 20 33 fd fd fd 01 00 00 7d 45 0e fd fd 7f 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 2d fd fd fd fd 6e 00 00 00 00 22 56 fd 7f 00 00 00 00 22 56 fd 7f 00 00 00 00 22 56 fd 7f 00 00 38 fd 17 10 fd 00 00 00 fd fd 17 10 fd 00 00 00 4e 02 06 00 00 00 00 00 08 fd 17 10 fd 00 00 00 74 04 fd fd fd 01 00 00 0a 00 00 00 00 00 00 00 28 22 cc fd 0f 00 00 fd fd fd fd fd fd fd 20 04 fd fd fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 7a fd fd fd 01 00 00 fd 00 00 00 00 00 00	"V@ 3}E_3++S++-n"V"V"V8Nt(" xz	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	15204	20	52 00 00 00 58 fd 47 10 fd 00 00 00 fd 03 00 00 fd 40 00 00	RXG@	success or wait	82	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	16520	936	76 fd 60 fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 61 fd fd 7f 00 00 10 00 00 00 00 00 00 00 fd fd 47 10 fd 00 00 00 fd fd 47 10 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 30 38 10 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 30 63 fd fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2f fd fd fd 01 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 58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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``2aGG080c/XX	success or wait	81	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	57796	8	fd fd 47 10 fd 00 00 00	G	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	11508	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 30 fd 17 10 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 17 10 fd 00 00 00 fd fd fd fd fd fd fd fd 38 fd 17 10 fd 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 17 10 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 38 fd 17 10 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	03++S++F888h	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 38 10 fd 00 00 00 58 fd 47 10 fd 00 00 00 fd 03 00 00 fd 40 00 00 fd 04 00 00 fd 36 00 00	8XG@6	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	9558	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	4556	4344	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 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 53 01 00 00 04 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 00 03 fd 01 00 00 00 fd fd 49 2a 70 6e 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 53 01 00 00 00 00 00	<2|h+(BB?#`A pSuuI*pnS	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	8908	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 50 fd 02 00 00 00 00 00 20 06 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 7a fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2a 1b 00 00 00 00 00 fd 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 45 00 00 00 00 fd 30 fd 19 00 00 00 00 0d 04 16 20 00 00 00 00 7e 5b 0a 01 00 00 00 00 fd fd 00 00 fd 0b 01 00 fd 00 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 fd 5e 2c 00 af 01 00 9b 12 00 00 00 00 00 fd fd 1a 00 fd 5a 04 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00	ZbP z*@E0 ~[^,Z	success or wait	1	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.tmp.dmp	57804	5164	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD56F.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 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 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 30 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	8$d;`8T0"$	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6352</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 34 00 39 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6499</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 33 00 38 00 30 00 30 00 33 00 32 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 03800320 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 31 00 37 00 31 00 30 00 30 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>220340817 1008</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 32 00 39 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>26293 </PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 30 00 31 00 33 00 32 00 34 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>105013248</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 30 00 35 00 33 00 33 00 31 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>7053312</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 34 00 34 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>106440</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 32 00 34 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>106240</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21440</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21088</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 32 00 37 00 32 00 30 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>1822720</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 36 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101462016</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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 32 00 37 00 32 00 30 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>1822720</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2720	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2760	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6332</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2854	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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>cmd.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2914	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2918	2	09 00		success or wait	4	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	2926	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 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3016	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3020	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3028	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6920</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3082	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3172	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3236	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3294	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 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22033 70262528 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3404	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 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 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>220337026 2528</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3498	72	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 37 00 39 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>793</ PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3584	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 32 00 38 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2 928640</P eakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3694	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 32 00 38 00 30 00 39 00 38 00 35 00 36 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>28098 56</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3788	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 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>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	3914	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 00 34 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>27664</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4024	122	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 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4150	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4160	106	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 33 00 36 00 36 00 34 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>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4280	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 32 00 39 00 39 00 38 00 32 00 37 00 32 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>2998272</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4370	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 35 00 37 00 32 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>3145728</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4476	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 32 00 39 00 39 00 38 00 32 00 37 00 32 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>2998272</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4560	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4616	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4666	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4704	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4752	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4798	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	4862	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 33 00 76 00 59 00 62 00 65 00 31 00 62 00 59 00 46 00 64 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_3vYbe 1bYFd.dll</Parameter0>	success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5652	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5654	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5694	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5698	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5700	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5738	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5742	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	5746	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6300	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6304	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6306	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6346	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6350	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6352	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6390	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6394	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6398	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6492	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6496	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6500	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 6d 00 63 00 78 00 67 00 6a 00 6f 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>mcxgjo, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6614	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 6d 00 63 00 78 00 67 00 6a 00 6f 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>mcxgjo7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6710	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6714	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6718	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6838	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6842	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6846	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 30 00 30 00 30 00 30 00 34 00 31 00 38 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1600004182</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	6936	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7046	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7120	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7160	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7164	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7166	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7208	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7304	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7308	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7310	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7346	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7350	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7352	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7376	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7380	2	09 00		success or wait	6	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7384	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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7630	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7634	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7636	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7668	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 32 00 33 00 54 00 30 00 36 00 3a 00 34 00 31 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T06:41:47Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7768	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7772	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	7776	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 35 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 32 00 36 00 38 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 32 00 36 00 38 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="403" PID="6352" UptimeMS="2687" TimeSinceCreationMS="2687" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	6	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8048	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 37 00 31 00 32 00 36 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="5771264" TimelineUnitShift="12" Timeline="11"/>	success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8424	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8428	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8432	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8452	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8456	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8458	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8496	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8500	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8502	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8540	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8544	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8548	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 37 00 64 00 37 00 62 00 31 00 37 00 39 00 2d 00 33 00 38 00 30 00 36 00 2d 00 34 00 31 00 34 00 31 00 2d 00 61 00 36 00 36 00 36 00 2d 00 39 00 63 00 32 00 32 00 63 00 39 00 61 00 62 00 61 00 63 00 30 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>37d7b179-3806-4141-a666-9c22c9abac02</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8646	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8650	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8654	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 32 00 33 00 54 00 30 00 36 00 3a 00 34 00 31 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T06:41:47Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8752	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8756	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8758	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8798	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85E.tmp.WERInternalMetadata.xml	8802	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA53.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19dde1f2\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 37 00 32 00 39 00 31 00 33 00 38 00 39 00 39 00	MetadataHash=-1072913899	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: 6544, Parent PID: 6360

General

Target ID:	11
Start time:	23:41:45
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6360 -s 316
Imagebase:	0x7ff6c7fd0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A6.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4B7.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2c fd 62 fd 05 12 00 00 00 00 00	MDMP ,b	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.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 50 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 40 fd fd 01 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 fd 2c fd 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBP%Lw@T,b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	10276	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 22 56 fd 7f 00 00 40 14 fd fd fd 7f 00 00 fd 2b fd 35 fd 01 00 00 7d 45 0e fd fd 7f 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 1d 5a fd fd fd 6e 00 00 00 00 22 56 fd 7f 00 00 00 00 22 56 fd 7f 00 00 00 00 22 56 fd 7f 00 00 fd fd 0c 3a fd 00 00 00 30 fd 0c 3a fd 00 00 00 3e 02 06 00 00 00 00 00 fd fd 0c 3a fd 00 00 00 28 5b fd 35 fd 01 00 00 0a 00 00 00 00 00 00 00 28 22 cc fd 0f 00 00 fd fd fd fd fd fd fd fd 5a fd 35 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 10 fd 35 fd 01 00 00 fd 00 00 00 00 00 00	"V@+5}E_3++S++Zn"V"V"V:0:>:([5("Z585	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	15204	20	53 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	S@	success or wait	83	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	16536	6	01 04 01 00 04 22	"	success or wait	82	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	59308	8	00 fd 1c 3a fd 00 00 00	:	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	11508	1232	fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 0c 3a fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0c 3a fd 00 00 00 fd fd fd fd fd fd fd fd fd 0c 3a 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 28 fd 0c 3a 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 0c 3a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	:3++S++F::(::h	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 23 3a fd 00 00 00 fd fd 1c 3a fd 00 00 00 38 06 00 00 fd 4a 00 00 fd 04 00 00 fd 36 00 00	#::8J6	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	9558	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	4556	4344	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 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 53 01 00 00 04 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 00 03 fd 01 00 00 00 47 fd 7d 2a 70 6e 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 00 00 53 01 00 00 00 00 00	<2|h+(BB?#`A pSuuG}*pnS	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	8908	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 20 06 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 5a fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2a 1b 00 00 00 00 00 60 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 45 00 00 00 00 14 fd fd 19 00 00 00 00 fd 03 17 20 00 00 00 00 06 7c 0a 01 00 00 00 00 07 fd 00 00 7f 0c 01 00 fd 01 06 00 2e fd 0a 00 60 fd 04 00 06 7f 15 00 fd fd 05 00 fd 7e 2c 00 6f 01 00 22 fd 12 00 00 00 00 00 1d fd 1a 00 fd 5a 04 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00	Zb@ Z*`@E |.`~,"Z	success or wait	1	7FFC738DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.tmp.dmp	59316	5056	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 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 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	(WaitCompletionPacketEventIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD59E.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 fd 10 00 00 38 12 00 00 05 00 00 00 34 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0c 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	84d;`8T"$	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6360</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 36 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6361</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 33 00 38 00 30 00 34 00 34 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03804416 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 31 00 37 00 31 00 30 00 30 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>220340817 1008</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 32 00 39 00 37 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>26297 </PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 30 00 31 00 33 00 32 00 34 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>105013248</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 30 00 35 00 37 00 34 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7057408</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 34 00 34 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>106440</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 32 00 34 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>106240</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21440</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21088</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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 36 00 36 00 31 00 31 00 32 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>101466112</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2720	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2760	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6316</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2854	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 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>loaddll64.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2926	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2930	2	09 00		success or wait	4	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	2938	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 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3028	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3032	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3040	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7505</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3094	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3184	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3248	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	5	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3306	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 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>4345114624</PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3410	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 31 00 31 00 34 00 39 00 36 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4341149696</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3498	72	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 36 00 34 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>643</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3584	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 31 00 34 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2314240</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3694	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 32 00 33 00 30 00 36 00 30 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2306048</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3788	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>28208</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	3914	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>20448</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4024	122	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 34 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4150	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4160	106	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 39 00 38 00 34 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>2984</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4280	74	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 34 00 37 00 39 00 32 00 33 00 32 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>479232</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4368	90	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 34 00 38 00 37 00 34 00 32 00 34 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>487424</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4472	70	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 34 00 37 00 39 00 32 00 33 00 32 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>479232</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4554	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4610	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4660	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4698	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4746	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4792	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4848	4	0d 00 0a 00		success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4852	2	09 00		success or wait	18	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	4856	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 33 00 76 00 59 00 62 00 65 00 31 00 62 00 59 00 46 00 64 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_3vYbe 1bYFd.dll</Parameter0>	success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5646	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5648	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5688	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5692	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5694	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5732	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5736	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	5740	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6300	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6346	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6384	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6388	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6392	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6486	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6490	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6494	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 6d 00 63 00 78 00 67 00 6a 00 6f 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>mcxgjo, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6608	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 6d 00 63 00 78 00 67 00 6a 00 6f 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>mcxgjo7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6712	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6840	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 30 00 30 00 30 00 30 00 34 00 31 00 38 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1600004182</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6926	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	6930	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7040	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7114	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7154	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7158	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7160	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7202	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7304	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7340	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7344	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7346	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7370	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7374	2	09 00		success or wait	6	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7378	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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7624	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7628	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7630	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7656	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7660	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7662	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 32 00 33 00 54 00 30 00 36 00 3a 00 34 00 31 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T06:41:47Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7762	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7766	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	7770	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 36 00 30 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 32 00 36 00 32 00 34 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 32 00 36 00 32 00 34 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="404" PID="6360" UptimeMS="2624" TimeSinceCreationMS="2624" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	6	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8042	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 37 00 31 00 32 00 36 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="5771264" TimelineUnitShift="12" Timeline="11"/>	success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8418	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8422	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8426	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8446	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8450	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8452	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8490	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8494	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8496	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8534	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8538	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8542	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 35 00 37 00 31 00 61 00 61 00 61 00 33 00 2d 00 61 00 36 00 64 00 33 00 2d 00 34 00 66 00 61 00 66 00 2d 00 39 00 33 00 31 00 33 00 2d 00 30 00 31 00 35 00 63 00 36 00 62 00 63 00 62 00 62 00 33 00 37 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8571aaa3-a6d3-4faf-9313-015c6bcbb37b</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8640	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8644	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8648	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 32 00 33 00 54 00 30 00 36 00 3a 00 34 00 31 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T06:41:47Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8746	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8750	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8752	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8792	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD929.tmp.WERInternalMetadata.xml	8796	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB1E.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f7c53a6fd35771ba6462da16e6bcb2581a34718_e0906090_19c9e185\Report.wer	9582	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 39 00 36 00 34 00 33 00 32 00 33 00 31 00 32 00 30 00	MetadataHash=1964323120	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d2d47f4e-2c78-4e3b-04cf-0166548cd667}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{d2d47f4e-2c78-4e3b-04cf-0166548cd667}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{d2d47f4e-2c78-4e3b-04cf-0166548cd667}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC738DE3FE	unknown

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

Analysis Process: rundll32.exe PID: **6700**, Parent PID: **6316**

General

Target ID:	13
Start time:	23:41:48
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,DllRegisterServer
Imagebase:	0x7ff756220000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7044**, Parent PID: **568**

General

Target ID:	15
Start time:	23:42:00
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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: svchost.exe PID: **7088**, Parent PID: **568**

General	
Target ID:	16
Start time:	23:42:03
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **7124**, Parent PID: **568**

General	
Target ID:	17
Start time:	23:42:04
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4780**, Parent PID: **568**

General	
Target ID:	18
Start time:	23:42:05
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Registry Activities

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

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

Analysis Process: svchost.exe PID: **5084**, Parent PID: **568**

General

Target ID:	19
Start time:	23:42:05
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **4264**, Parent PID: **568**

General

Target ID:	20
Start time:	23:42:06
Start date:	22/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff79ddd0000
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: **3808**, Parent PID: **568**

General

Target ID:	22
Start time:	23:42:07
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **2216**, Parent PID: **568**

General

Target ID:	23
Start time:	23:42:09
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6676**, Parent PID: **568**

General

Target ID:	24
Start time:	23:42:18
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7024, Parent PID: 568

General

Target ID:	27
Start time:	23:42:38
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 3756, Parent PID: 3808

General

Target ID:	32
Start time:	23:43:07
Start date:	22/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 244, Parent PID: 3756

General

Target ID:	33
Start time:	23:43:08
Start date:	22/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly