ID: 639646
Sample Name: cargo documents.pdf.exe
Cookbook: default.jbs
Time: 09:42:05
Date: 06/06/2022
Version: 35.0.0 Citrine

Table of Contents

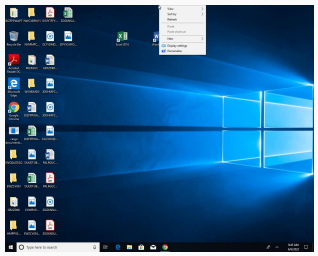
Windows Analysis Report

cargo documents.pdf.exe

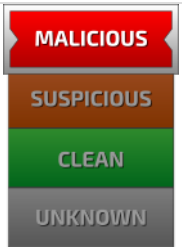
Overview

General Information

Sample Name:	cargo documents.pdf.exe
Analysis ID:	639646
MD5:	f0bec0deb10b8b..
SHA1:	452b936847f131..
SHA256:	b4b14f0512858e..
Tags:	exe warzonerat
Infos:	



Detection



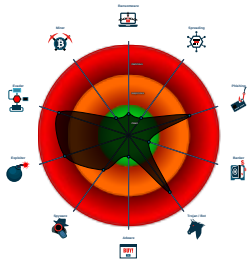
AveMaria, UACMe

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected UACMe UAC Bypass…
- Antivirus detection for URL or domain
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Initial sample is a PE file and has a…

Classification



Process Tree

- **System is w10x64**
- cargo documents.pdf.exe (PID: 6456 cmdline: "C:\Users\user\Desktop\cargo documents.pdf.exe" MD5: F0BEC0DEB10B8BC59A5B2D207B4CDEEF)
  - conhost.exe (PID: 6476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5936 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - images.exe (PID: 5700 cmdline: C:\ProgramData\images.exe MD5: F0BEC0DEB10B8BC59A5B2D207B4CDEEF)
    - powershell.exe (PID: 2040 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - cmd.exe (PID: 6052 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- images.exe (PID: 6224 cmdline: "C:\ProgramData\images.exe" MD5: F0BEC0DEB10B8BC59A5B2D207B4CDEEF)
  - conhost.exe (PID: 5732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WerFault.exe (PID: 1656 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6224 -s 620 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "udooiuyt.dynamic-dns.net",
  "port": 5200
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.wer	SUSP_WER_Suspicious_Crash_Directory	Detects a crashed application executed in a suspicious directory	Florian Roth	• 0x116:$a1: ReportIdentifier= • 0x198:$a1: ReportIdentifier= • 0x616:$a2: .Name=Fault Module Name • 0x193c:$a3: AppPath=

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x5028:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x5028:$c1: Elevation:Administrator!new:
0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x192c0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x192c0:$c1: Elevation:Administrator!new:

Click to see the 69 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.cargo documents.pdf.exe.7d6138.7.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.3.cargo documents.pdf.exe.7d6138.7.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2318:$c1: Elevation:Administrator!new:
0.3.cargo documents.pdf.exe.7d6138.7.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
0.3.cargo documents.pdf.exe.7d4450.9.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x5f8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.3.cargo documents.pdf.exe.7d4450.9.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x5f8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x5f8:$c1: Elevation:Administrator!new: • 0x3400:$c1: Elevation:Administrator!new:

Click to see the 193 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 45.137.22.163 −

Timestamp:	192.168.2.345.137.22.1634975752002036734 06/06/22-09:44:38.099241
SID:	2036734
Source Port:	49757
Destination Port:	5200
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 45.137.22.163 - Destination IP: 192.168.2.3 −

Timestamp:	45.137.22.163192.168.2.35200497572036735 06/06/22-09:44:37.664135

SID:	2036735
Source Port:	5200
Destination Port:	49757
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Yara detected AveMaria stealer
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Exploits

- Yara detected UACMe UAC Bypass tool

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected AveMaria stealer

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name
- Executable has a suspicious name (potential lure to open the executable)

Hooking and other Techniques for Hiding and Protection

- Contains functionality to hide user accounts
- Hides that the sample has been downloaded from the Internet (zone.identifier)
- Uses an obfuscated file name to hide its real file extension (double extension)

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- Allocates memory in foreign processes
- Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

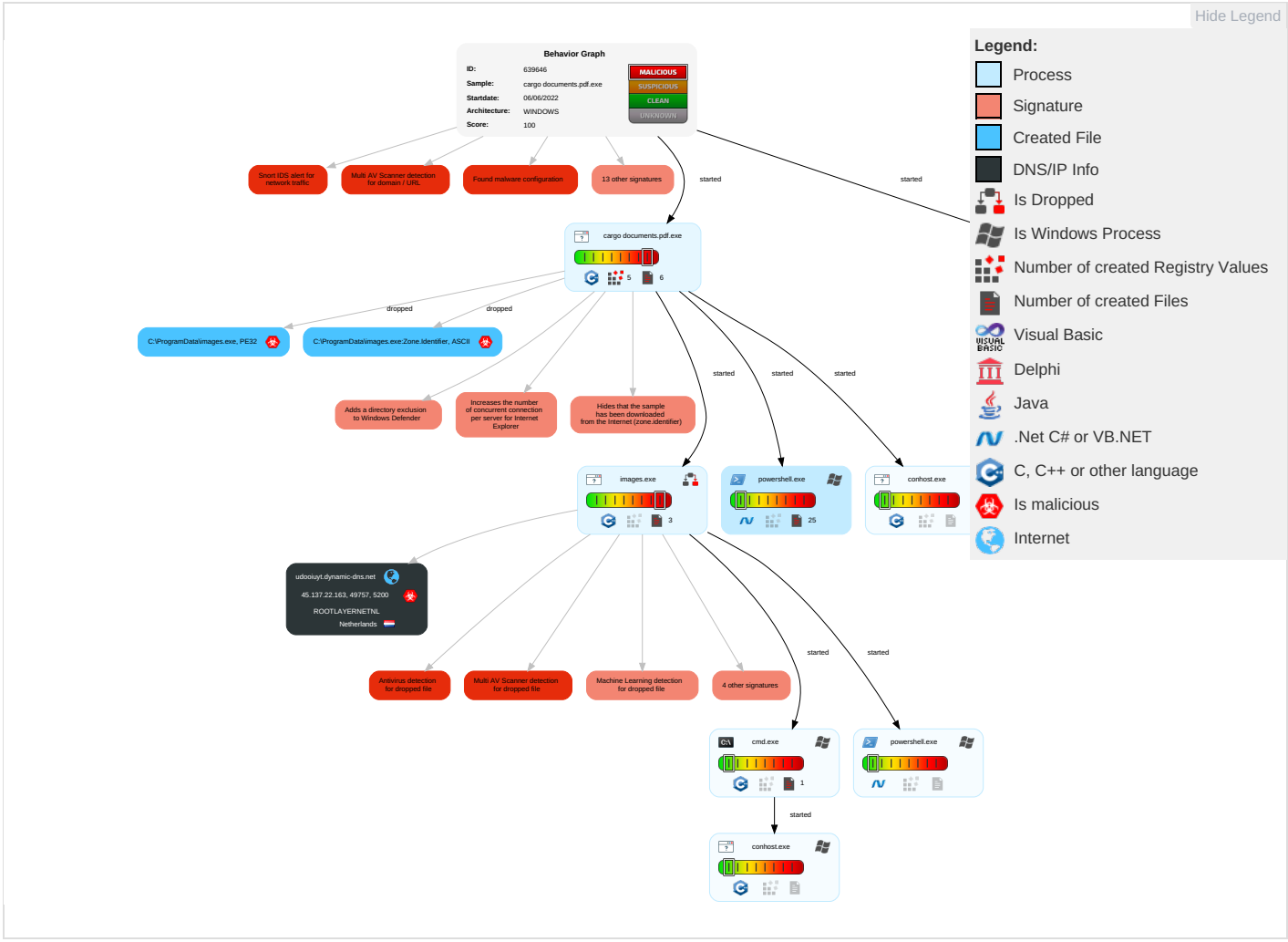
Remote Access Functionality

Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	3 2 Process Injection	1 3 Masquerading	2 1 Input Capture	1 System Time Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 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)	3 2 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 Application Window 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 Hidden Users	DCSync	1 Remote System 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 1 1 Obfuscated Files or Information	Proc Filesystem	1 File and Directory 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 1 Software Packing	/etc/passwd and /etc/shadow	1 3 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

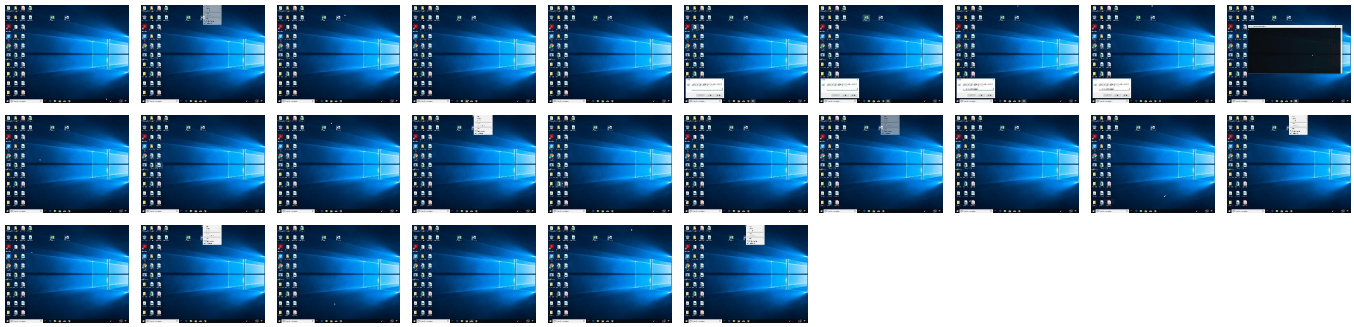
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cargo documents.pdf.exe	27%	Virustotal		Browse
cargo documents.pdf.exe	100%	Avira	HEUR/AGEN.1215358	
cargo documents.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\images.exe	100%	Avira	HEUR/AGEN.1215358	
C:\ProgramData\images.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	27%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.images.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
14.0.images.exe.22e053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
0.3.cargo documents.pdf.exe.7d4450.9.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File

Source	Detection	Scanner	Label	Link	Download
14.0.images.exe.22e053f.7.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
14.2.images.exe.22e053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
13.3.images.exe.801aa0.10.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
0.2.cargo documents.pdf.exe.b10000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
0.3.cargo documents.pdf.exe.7d4450.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
14.2.images.exe.2ce0000.3.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
0.0.cargo documents.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
13.3.images.exe.801aa0.5.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
0.2.cargo documents.pdf.exe.244053f.3.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
14.0.images.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1230764		Download File
13.3.images.exe.801aa0.13.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
13.2.images.exe.234053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
13.2.images.exe.2d40000.3.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
13.0.images.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
14.0.images.exe.2ce0000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
14.0.images.exe.2ce0000.9.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
13.3.images.exe.801aa0.4.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
13.0.images.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
13.0.images.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
udooiuyt.dynamic-dns.net	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.microsoft.c2J	0%	Avira URL Cloud	safe	
udooiuyt.dynamic-dns.net	13%	Virustotal		Browse
udooiuyt.dynamic-dns.net	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
udooiuyt.dynamic-dns.net	45.137.22.163	true	true	• 13%, Virustotal, Browse	unknown

Contacted URLs

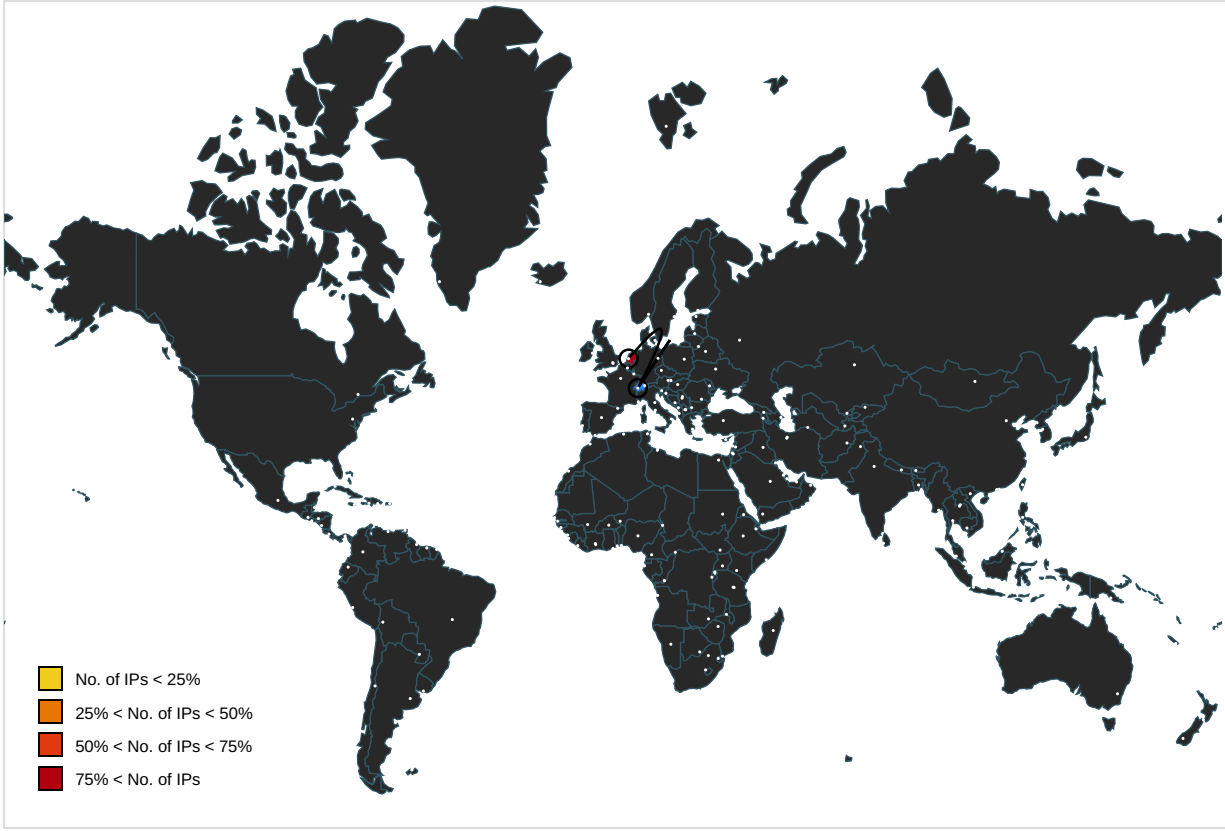
Name	Malicious	Antivirus Detection	Reputation
udooiuyt.dynamic-dns.net	true	• 13%, Virustotal, Browse • Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.microsoft.c2J	powershell.exe, 0000000C.00000003.463262262.00000000096AD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeperC:	cargo documents.pdf.exe, 00000000.00000003.328999945.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, cargo documents.pdf.exe, 00000000.00000003.329633013.00000000007BF000.00000004.00000020.00020000.00000000.sdmp, cargo documents.pdf.exe, 00000000.00000002.346161190.0000000000B24000.00000002.00001000.00020000.00000000.sdmp, cargo documents.pdf.exe, 00000000.00000002.346243872.0000000002440000.00000040.00001000.00020000.00000000.sdmp, cargo documents.pdf.exe, 00000000.00000003.329464338.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000D.00000003.424092042.0000000000815000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000D.00000003.424364363.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000D.00000002.533660136.0000000002340000.00000040.00001000.00020000.00000000.sdmp, images.exe, 0000000D.00000002.534137426.0000000002D5400.00000002.00001000.00020000.00000000.sdmp, images.exe, 0000000D.00000003.424337979.0000000000829000.00000004.00000020.00020000.00000000.sdmp, images.exe, 0000000E.00000002.473066946.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, images.exe, 0000000E.00000000.446138894.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000010.00000002.535162638.0000000004453000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000010.00000002.534474533.0000000004311000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/syohex/java-simple-mine-sweeper	cargo documents.pdf.exe, images.exe	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000010.00000002.535162638.0000000004453000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.163	udooiuyt.dynamic-dns.net	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	639646
Start date and time: 06/06/202209:42:05	2022-06-06 09:42:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cargo documents.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.expl.evad.winEXE@14/13@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 40.125.122.176, 20.54.89.106
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:43:51	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Images C:\ProgramData\images.exe
09:44:28	API Interceptor	60x Sleep call for process: powershell.exe modified
09:44:36	API Interceptor	352x Sleep call for process: cmd.exe modified
09:44:50	API Interceptor	1x Sleep call for process: WerFault.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\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.5715228937541381

Encrypted:	false
SSDEEP:	96:mfrFxp5V8QhMo/7JfkpXIQcQIc6GcE8cw3GZAXGng5FMTPSkvPkpXmTAzfnVXT5T:MrLp5VUHGCWL/u7s6S274ItQ
MD5:	C4791FAB7060F8F3029B262A4647E4A1
SHA1:	9ACE3950078225E7B76489E5D1C7D8B4F4A38692
SHA-256:	8C452C0CBB371B41190878FF6DDD465B4CE7D466B6FD1D6249EACD0FAA957797
SHA-512:	96A969E7BC2A68C01621FEFC96A7F7C11EFC64A28D79FB45DE14F5893C699A98E24036B71F38A9E3B12C6EE9A7BF3B2B363189A9CC45187D711B94528937294
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Suspicious_Crash_Directory, Description: Detects a crashed application executed in a suspicious directory, Source: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.we Author: Florian Roth
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.9.0.0.7.4.8.2.7.1.5.0.5.9.3.....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.=.1.3.2.9.9.0.0.7.4.8.9.3.2.4.4.7.0.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.3.d.1.9.0.6.7.-.3.8.f.e.-.4.9.7.1.-.b.5.8.1.-.f.6.9.f.5.8.e.e.7.8.a.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.0.b.5.3.2.1.e.-.b.c.5.9.-.4.5.8.0.-.b.4.1.4.-.c.0.d.8.1.a.6.7.e.f.4.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.b.a.d._.m.o.d.u.l.e._.i.n.f.o.....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.d.-.b.4.d.5.-.2.0.9.f.c.4.7.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.2.b.a.4.3.f.a.5.f.8.d.5.b.f.f.f.f.5.f.8.6.9.a.a.a.6.a.3.4.3.1.0.0.0.0.f.f.f.f.!.0.0.0.0.4.5.2.b.9.3.6.8.4.7.f.1.3.1.a.b.d.4.b.8.7.2.8.1.5.a.b.3.5.c.9.b.9.b.c.d.9.c.b.b.!.i.m.a.g.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8298
Entropy (8bit):	3.6893239628639813
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNinu686YWBSU1lhIgmfvSjCpD389b83sfa9Um:RrlsNiu686YQSU1bIgmfvSr88fM
MD5:	6D2CA85E7BC8C6794E8CA974F79261CD
SHA1:	09D8AFA6FC6267FDC4F46BAFAD6B1545F58A36B9
SHA-256:	4B8D7EE638CF427D63791D22C74755FD65EFD2540BEAC3B45C55888D5A18EAFF
SHA-512:	E4DB3EFF330BD8896ECC5128CCE6D18393EBB0A359793110E9B330AAE3F36C337C67D9CC8BA7933D76DCF7439DE4CAB34FE5D8FEBFD6D3493FF7FF49598BE427
Malicious:	false
Reputation:	low
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\WERF4D2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4554
Entropy (8bit):	4.437589986312388
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9H7rWgc8sqYjF8fm8M4JT8ZFW+q8iPvjVFYm/K+fd:uITfPgOgrsqY+J7tVjK+fd
MD5:	C778F196DE1FF6039AF1C742587E5AC2
SHA1:	AE93A10F29A5910603958B158A16775ACA279C66
SHA-256:	9E4670673E31FAB7B29147F273EEDF38FA9BFA4CF05F91E336826E2CB1E3F5D9
SHA-512:	A83CE0973EB77122E477222447E86AD16C567706036791BF350B58447BD47B65484CF149DF1E16A335B4D4CBE84AB0AE49FCB8AF6275206678568361E09139A1
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="1548115" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\images.exe

Process:	C:\Users\user\Desktop\cargo documents.pdf.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
Category:	dropped

Size (bytes):	187904
Entropy (8bit):	7.856698647812573
Encrypted:	false
SSDEEP:	3072:hFZRWMN2EyOdnHN/0f5B2gPcvTt728bZK3LyAw1HG7GMbcDK90XKgwcG2O5NCMLo:aMXHB0zlSTt728N5tuWXKVvPHq7
MD5:	F0BEC0DEB10B8BC59A5B2D207B4CDEEF
SHA1:	452B936847F131ABD4B872815AB35C9B9BCD9CBB
SHA-256:	B4B14F0512858ECD957152F6F21D06070AD3F371206568871D0F92D5A41ECD83
SHA-512:	A57437BBA1A5B9BB8CE2754290E80A5ED78ADB8A8017305FE30AC1A7A95C5480FD771A7B35CCD048D17DBA2409F74E8C407523A0F0AA61559392C4F0FC9516 E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 27%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....zB..zB..zB..yC..zB...C..zB..~C..zB..~C..zB..yC..zB...C..zB.. {C..zB..{B!.zB!.sC..zB!.B..zB!.xC..zBRich..zB.....PE..L...OO.b.....@...''...P...0....@.....@.....@.....@.....1..`....0.....<3.. (.....$.....$.....UPX0.....@.....UPX1.....P.....@....rsrc.....0.....@..... ....3.95.UPX!....

C:\ProgramData\images.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\cargo documents.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:wZvOdB8Ypib4JNXp59HopbjvwRjdvRlAYotiQ0HzAF8:UvOdB8YNNZjHopbjoRjdvRlAYotinHzr
MD5:	C5A56B913DEEDCF5AE01A2D4F8AA69CE
SHA1:	C91D19BFD666FDD02B0739893833D4E1C0316511
SHA-256:	1C5C865E5A98F33E277A81FCDADFBAB1367176BA14F8590022F7E5880161C00D
SHA-512:	1058802FCD54817359F84977DD26AD4399C572910E67114F70B024EBADDF4E35E6AFF6461F90356205228B4B860E69392ABC27D38E284176C699916039CFA5ED
Malicious:	false
Preview:	PSMODULECACHE.....#y;...Q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1.....Start-BitsTransfer.....Set-BitsTransfer .....Get-BitsTransfer.....Resume-BitsTransfer.....Add-BitsFile.....Suspend-BitsTransfer.....Complete-BitsTransfer.....Remove-BitsTransfer.....-.^(...[...C:\Win dows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1....#...Set-AppBackgroundTaskResourcePolicy.....Unregister-App BackgroundTask.....Get-AppBackgroundTask.....tid.....pfn.....iru....%...Enable-AppBackgroundTaskDiagnosticLog.....Start-AppBackgroundTask....&...Disable-Ap pBackgroundTaskDiagnosticLog.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1..... ..Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Pac kage.....Unins

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22164
Entropy (8bit):	5.600317935166761
Encrypted:	false

SSDEEP:	384:stCDhrueAYa+ZjX7gfi+RVKnyul1M7nvyMhsInEMA+ufmAV7OnWD+ZQvnI++WS:6ylX0f3Kyul1ch5PRyp6Z+i
MD5:	546C0C2814E471E7A806D8F8DF4A1D04
SHA1:	D202B08BB0C46F32A8A9213F12C625AD484AED8D
SHA-256:	E84441741EE5E4F09A625D9B5027500F9428552DAA1F5D70698C72E38E093014
SHA-512:	1EA82E518E52464F4F594F2DD07F48055A74F73EBA6E1F37BE5650CEDE640FE10AAC8B4C8ACD84B350560DA31D58058C5C8DBE8ED31B055CD593C87C8C8DC00
Malicious:	false
Preview:	@...e.....].....A.0.-.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\WERE271.tmp.WERDataCollectionStatus.txt

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4778
Entropy (8bit):	3.2530534973312633
Encrypted:	false
SSDEEP:	96:pwpIifkXkkXlkl7uWKH0Q40Qf0Qg30QXf0QX0QLi9gxXx9szeuzSzbxGQI5Pm1sD:pqlkQuPBtoeyOkNf
MD5:	54CDB6858C72CA844E7E7671F8E3056D
SHA1:	DE545E90C25C7DD1FE2E0D901906C8A17E5AAA15
SHA-256:	4AE5595CDBBE01B55DF729F1F09B787F2699C878A123555346FC29E265F2E7BF
SHA-512:	6E5B3EBEABD24A11F5005B9D883003C0A5A8B48A9D1007DA083FF040AF651B0D5764122C72D84544ADA2256982463D02DB7E0694C9002DC45CCC14C7A84CF9C
Malicious:	false
Preview:	.....S.n.a.p.s.h.o.t. .s.t.a.t.i.s.t.i.c.s.:.....-. .S.i.g.n.a.t.u.r.e. . . . . .:. .P.S.S.D.....-. .F.l.a.g.s./.C.a.p.t.u.r.e.F.l.a.g.s. . . . . .:. .0.0.0.0.0.0.0.1./.d.0.0.0.3.9.f.f.....-. .A.u.x. .p.a.g.e.s. . . . . .:. .1. .e.n.t.r.i.e.s. .l.o.n.g.....-. .V.A. .s.p.a.c.e. .s.t.r.e.a.m. . . . . .:. .4.5.6.4.8. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .H.a.n.d.l.e. .t.r.a.c.e. .s.t.r.e.a.m. . . . . .:. .0. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .H.a.n.d.l.e. .s.t.r.e.a.m. . . . . .:. .1.6.8.7.8. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .T.h.r.e.a.d.s. . . . . .:. .4. .t.h.r.e.a.d.s.....-. .T.h.r.e.a.d. .s.t.r.e.a.m. . . . . .:. .3.3.2.8. .b.y.t.e.s. .i.n. .s.i.z.e.....S.n.a.p.s.h.o.t. .p.e.r.f.o.r.m.a.n.c.e. .c.o.u.n.t.e.r.s.:.....-. .T.o.t.a.l.C.y.c. l.e.C.o.u.n.t. . . . . .:. .9.4.0.8.7.6.4.9. .c.y.c.l.e.s.....-. .V.a.C.l.o.n.e.C.y.c.l.e.C.o.u.n.t. . . .

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2s3ge4l4.jod.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q3fxmylt.3yr.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A

Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tchg0qr4.bxh.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wt4y1mqo.f1w.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\Documents\20220606\PowerShell_transcript.376483.VEQ2RUHw.20220606094353.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5048
Entropy (8bit):	5.3956121257690866
Encrypted:	false
SSDEEP:	96:BZqhxN5XqDo1ZVZ7uhxN5XqDo1ZBGM6UjZ+hxN5XqDo1ZbFEEVZG:EhMbaW
MD5:	50067B3E098A9B443322885859E46427
SHA1:	4947553A5DCE4C9DEA82DA357A3094106FEB1D3B
SHA-256:	62C16022FE950A6C4D62CA0A5C3F6F2748074DA4E88DFBB6A484F809E025D64D
SHA-512:	205190B1E791F158BE7C4FEA844DF909335A25C3B73BC8A3E47F34358F41F44F0201C6D356C38E6B8FC8FA3094DFE4093E3C0AB8DB6753B418029B894FF8022D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220606094418..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 5936..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220606094418..********** *****..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20220606094814..Username: computer\user. .RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.856698647812573
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • UPX compressed Win32 Executable (30571/9) 0.30% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	cargo documents.pdf.exe
File size:	187904
MD5:	f0bec0deb10b8bc59a5b2d207b4cdeef
SHA1:	452b936847f131abd4b872815ab35c9b9bcd9cbb
SHA256:	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83
SHA512:	a57437bba1a5b9bb8ce2754290e80a5ed78adb8a8017305fe30ac1a7a95c5480fd771a7b35ccd048d17dba2409f74e8c407523a0f0aa61559392c4f0fc95164e
SSDEEP:	3072:hFZRWMN2EyOdnHN/0f5B2gPcvTt728bZK3LyAw1HG7GMbcDK90XKgwcG2O5NCMLo:aMXHB0zlSTt728N5tuWXKVvPHq7
TLSH:	620412BB653F798BCA1C53794A9ECE3285AE924B0CDE117CA450F68B3EC2CD84B55350
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....zB..zB..zB..yC..zB...C..zB..~C..zB..~C..zB..yC..zB...C..zB..{C..zB..{B!.zB!.sC..zB!..B..zB!.xC..zBRich..zB.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5422b0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x629D4F4F [Mon Jun 6 00:50:23 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b89c0acb10e1bafbe56a95fb03ea7ddd

Entrypoint Preview

Instruction
pushad
mov esi, 00515000h
lea edi, dword ptr [esi-00114000h]
mov dword ptr [edi+0013C580h], B7169FEFh
push edi
jmp 00007F6954C40443h
nop
nop
nop
nop
nop
nop
nop
mov al, byte ptr [esi]
inc esi

Instruction
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F6954C4041Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F6954C4043Dh
jne 00007F6954C4045Ah
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F6954C40451h
dec eax
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
jmp 00007F6954C40406h
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jmp 00007F6954C40484h
xor ecx, ecx
sub eax, 03h
jc 00007F6954C40443h
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F6954C404A7h
sar eax, 1
mov ebp, eax
jmp 00007F6954C4043Dh
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F6954C403FEh
inc ecx
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh

Instruction
adc ebx, ebx
jc 00007F6954C403F0h
add ebx, ebx
jne 00007F6954C40439h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F6954C40421h
jne 00007F6954C4043Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F6954C40416h
add ecx, 02h
cmp ebp, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1431dc	0x160	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x143000	0x1dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x14333c	0x28	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x14249c	0x18	UPX1
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1424bc	0xbc	UPX1
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
UPX0	0x1000	0x114000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x115000	0x2e000	0x2d600	False	0.974238119835	data	7.86250939013	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x143000	0x1000	0x400	False	0.49609375	data	4.62013477766	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x14305c	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
ADVAPI32.dll	CopySid

DLL	Import
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
SHELL32.dll	SHGetFolderPathW
USER32.dll	IsWindow
VERSION.dll	VerQueryValueW

Possible Origin

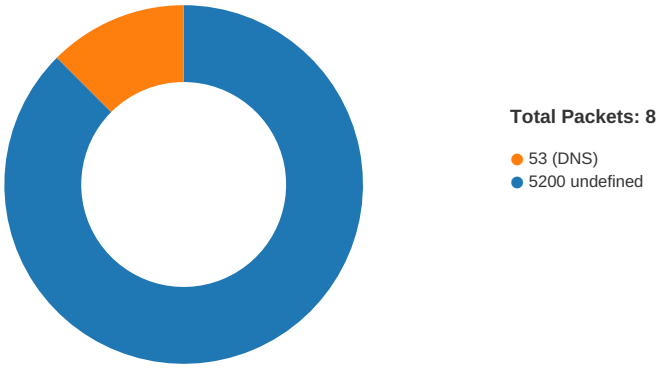
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.137.22.163 4975752002036734 06/06/22-09:44:38.099241	TCP	2036734	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin	49757	5200	192.168.2.3	45.137.22.163
45.137.22.163192.168.2.3 5200497572036735 06/06/22-09:44:37.664135	TCP	2036735	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	5200	49757	45.137.22.163	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2022 09:44:37.613935947 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:44:37.636133909 CEST	5200	49757	45.137.22.163	192.168.2.3
Jun 6, 2022 09:44:37.638196945 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:44:37.664134979 CEST	5200	49757	45.137.22.163	192.168.2.3
Jun 6, 2022 09:44:37.772237062 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:44:38.099241018 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:44:38.171850920 CEST	5200	49757	45.137.22.163	192.168.2.3
Jun 6, 2022 09:44:57.678237915 CEST	5200	49757	45.137.22.163	192.168.2.3
Jun 6, 2022 09:44:57.723774910 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:44:57.800843000 CEST	5200	49757	45.137.22.163	192.168.2.3
Jun 6, 2022 09:45:17.693059921 CEST	5200	49757	45.137.22.163	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2022 09:45:17.744366884 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:45:17.750114918 CEST	49757	5200	192.168.2.3	45.137.22.163
Jun 6, 2022 09:45:17.822278023 CEST	5200	49757	45.137.22.163	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2022 09:44:37.563575983 CEST	57421	53	192.168.2.3	8.8.8.8
Jun 6, 2022 09:44:37.584103107 CEST	53	57421	8.8.8.8	192.168.2.3

DNS Queries

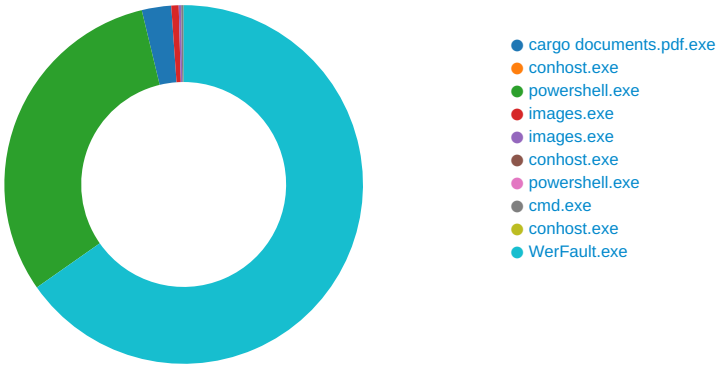
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 6, 2022 09:44:37.563575983 CEST	192.168.2.3	8.8.8.8	0xd3b	Standard query (0)	udooiuyt.dynamic-dns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 6, 2022 09:44:37.584103107 CEST	8.8.8.8	192.168.2.3	0xd3b	No error (0)	udooiuyt.dynamic-dns.net		45.137.22.163	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: cargo documents.pdf.exe PID: **6456**, Parent PID: **3692**

General

Target ID:	0
Start time:	09:43:13
Start date:	06/06/2022
Path:	C:\Users\user\Desktop\cargo documents.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cargo documents.pdf.exe"
Imagebase:	0x400000
File size:	187904 bytes
MD5 hash:	F0BEC0DEB10B8BC59A5B2D207B4CDEEF

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.328999945.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.328999945.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.328999945.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.329633013.00000000007BF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.329633013.00000000007BF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.329445075.00000000007D5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.329445075.00000000007D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.346161190.0000000000B24000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.346161190.0000000000B24000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.346220388.0000000000C5F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.346220388.0000000000C5F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.346243872.0000000002440000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.346243872.0000000002440000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.346243872.0000000002440000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.346243872.0000000002440000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.329464338.00000000007C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.329035116.00000000007D5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.329035116.00000000007D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	B2360F	CreateDirectoryW
C:\ProgramData\images.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	B211DD	CopyFileW
C:\ProgramData\images.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	B211DD	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe:Zone.Identifier	success or wait	1	B21482	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 14 11 fd fd 7a 42 fd fd 7a 42 fd fd 7a 42 fd fd 79 43 fd fd 7a 42 fd fd 7f 43 19 fd 7a 42 fd fd 7e 43 fd fd 7a 42 fd fd 7e 43 fd fd 7a 42 fd fd 79 43 fd fd 7a 42 fd fd 7f 43 fd fd 7a 42 fd fd 7b 43 fd fd 7a 42 fd fd 7b 42 21 fd 7a 42 21 fd 73 43 fd fd 7a 42 21 45 42 fd fd 7a 42 21 fd 78 43 fd fd 7a 42 52 69 63 68 fd fd 7a 42 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03	MZ@!L!This program cannot be run in DOS mode.$zBzBzByCzBCzB ~ CzB~CzByCzBCzB{CzB{ B!zB!sCzB!B zB!xCzBRichzBPEL	success or wait	2	B211DD	CopyFileW
C:\ProgramData\images.exe:Zone .Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	B211DD	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cargo documents.pdf.exe	unknown	187904	success or wait	1	B21E78	ReadFile

Registry Activities

Analysis Process: conhost.exe PID: **6476**, Parent PID: **6456**

General

Target ID:	1
Start time:	09:43:15
Start date:	06/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5936**, Parent PID: **6456**

General

Target ID:	12
Start time:	09:43:46
Start date:	06/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\

Imagebase:	0xe90000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA4CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wt4y1mqo.f1w.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tchg0qr4.bxh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0E1E60	CreateFileW
C:\Users\user\Documents\20220606	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0EBEFF	CreateDirectoryW
C:\Users\user\Documents\20220606\PowerShell_transcript.376483.VEQ2RUHw.20220606094353.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wt4y1mqo.f1w.ps1	success or wait	1	6C0E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tchg0qr4.bxh.psm1	success or wait	1	6C0E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C045B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wt4y1mqo.f1w.ps1	0	1	31	1	success or wait	1	6C0E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tchg0qr4.bxh.psm1	0	1	31	1	success or wait	1	6C0E1B4F	WriteFile
C:\Users\user\Documents\20220606\PowerShell_transcript.376483.VEQ2RUHw.20220606094353.txt	0	3	ff		success or wait	1	6C0E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220606\PowerShell_transcript.376483.VEQ2RUHw.20220606094353.txt	3	588	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 36 30 36 30 39 34 34 31 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 37 36 34 38 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220606094418Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 376483 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	6C0E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 fd 23 79 3b 9f fd 08 51 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 73 54 72 61 6e 73 66 65 72 5c 42 69 74 73 54 72 61 6e 73 66 65 72 2e 70 73 64 31 08 00 00 00 12 00 00 00 53 74 61 72 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 53 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 47 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 13 00 00 00 52 65 73 75 6d 65 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 0c 00 00 00 41 64 64 2d 42 69 74 73 46 69 6c 65 08 00 00 00 14 00 00 00 53 75 73 70 65 6e 64 2d 42 69 74 73 54 72 61	PSMODULECACHE#y;QC:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1Start-BitsTransferSet-BitsTransferGet-BitsTransferResume-BitsTransferAdd-BitsFileSuspend-BitsTra	success or wait	1	6C0E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 4c 6f 63 6b 65 72 5c 42 69 74 4c 6f 63 6b 65 72 2e 70 73 6d 31 28 00 00 00 20 00 00 00 41 64 64 2d 45 78 74 65 72 6e 61 6c 4b 65 79 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 19 00 00 00 43 6c 65 61 72 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 44 69 73 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 47 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1b 00 00 00 53 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 45 6e 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74	wsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1(Add-ExternalKeyProtectorInternalClear-BitLockerAutoUnlockDisable-BitLockerAutoUnlockGet-BitLockerVolumeInternalSet-BitLockerVolumeInternalEnable-BitLockerAut	success or wait	1	6C0E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	72 64 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 50 72 6f 63 65 73 73 08 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 49 74 65 6d 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 09 00 00 00 4a 6f 69 6e 2d 50 61 74 68 08 00 00 00 0c 00 00 00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 1a 00 00 00 54 65 73 74 2d 43 6f 6d 70 75 74 65 72 53 65 63 75 72 65 43 68 61 6e 6e 65 6c 08 00 00 00 0e 00 00 00 4c 69 6d 69 74 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 10 00 00 00 49 6e 76 6f 6b 65 2d 57 6d 69 4d 65 74 68 6f 64 08 00 00 00 10 00 00 00 47 65 74 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0b 00 00 00 4e 65	rdStart-ProcessInvoke-ItemStop-ComputerGet-HotFixJoin-PathStop-ProcessTest-ComputerSecureChannelLimit-EventLogInvoke-WmiMethodGet-ItemPropertyRemove-ComputerNe	success or wait	1	6C0E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	2446	3b 9f fd 08 71 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 00 08 00 00 00 47 65 74 2d 44 61 74 65 08 00 00 00 0e 00 00 00 43 6c 65 61 72 2d 56 61 72 69 61 62 6c 65 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0a 00 00 00 49 6d 70 6f 72 74 2d 43 73 76 08 00 00 00 0c 00 00 00 47 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0c 00 00 00 4e 65 77 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f	;qC:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mGet-DateClear-VariableGet-EventSubscriberImport-CsvGet-VariableNew-VariableCo	success or wait	1	6C0E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 5d 14 00 00 19 00 00 00 fd 0b fd 04 41 07 30 07 2d 07 00 00 00 00 fd 00 0d 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e]A0-@	success or wait	1	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DD176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DD176FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 29 40 01 fd 29 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 23 29 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 09 06 fd 00 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 45 4d 40 01 fd 71 40	T@>@)@)@@V@H@X @[@NT@HT@S@S@h T@ S@S@S@\@T@T@@X @? X@T@S@S@T@T@xT @#)@zT@T@=M@DM @:M@"M@ M@\d@Zd@ [d@!M@;M@D@D@@M @<M@$M@8M@? M@Xd @Vd@*@EM@q@	success or wait	11	6DD176FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA2CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA25705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DA31F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DA3203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C0E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA25705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	13	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C0E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6C0E1B4F	ReadFile

Analysis Process: images.exe PID: **5700**, Parent PID: **6456**

General

Target ID:	13
Start time:	09:43:50
Start date:	06/06/2022
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x400000
File size:	187904 bytes
MD5 hash:	F0BEC0DEB10B8BC59A5B2D207B4CDEEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.423633743.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.423583171.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000003.424092042.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000003.424092042.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.424092042.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.424092042.0000000000815000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.424364363.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.424364363.00000000007EF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000002.533660136.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000002.533660136.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.533660136.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000002.533660136.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.534137426.0000000002D54000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000002.534137426.0000000002D54000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000003.424337979.0000000000829000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000003.424337979.0000000000829000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000003.424337979.0000000000829000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000D.00000003.424337979.0000000000829000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000D.00000002.534228937.0000000002E8F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000D.00000002.534228937.0000000002E8F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 27%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2D5360F	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	unknown	187904	success or wait	1	2D51E78	ReadFile
C:\ProgramData\images.exe	unknown	187904	success or wait	1	2D51E78	ReadFile

Analysis Process: images.exe PID: 6224, Parent PID: 3968

General

Target ID:	14
Start time:	09:43:59
Start date:	06/06/2022

Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\images.exe"
Imagebase:	0x400000
File size:	187904 bytes
MD5 hash:	F0BEC0DEB10B8BC59A5B2D207B4CDEEF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000002.473066946.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000002.473066946.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.473066946.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000002.473066946.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000000.446217093.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000000.446217093.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.446138894.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000000.446138894.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000000.444579296.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000000.444579296.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000000.445828569.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000000.445828569.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.445828569.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000000.445828569.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.473541698.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000002.473541698.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000002.473733362.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000002.473733362.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000E.00000000.444162816.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000E.00000000.444162816.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.444162816.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000000.444162816.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.444484040.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000E.00000000.444484040.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	unknown	187904	success or wait	1	2CF1E78	ReadFile

Analysis Process: conhost.exe PID: **5732**, Parent PID: **6224**

General

Target ID:	15
Start time:	09:44:00
Start date:	06/06/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **2040**, Parent PID: **5700**

General

Target ID:	16
Start time:	09:44:31
Start date:	06/06/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0xe90000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: cmd.exe PID: **6052**, Parent PID: **5700**

General

Target ID:	17
Start time:	09:44:32
Start date:	06/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	unknown	187904	success or wait	1	310026F	ReadFile

Analysis Process: conhost.exe PID: **1892**, Parent PID: **6052**

General

Target ID:	18

Start time:	09:44:33
Start date:	06/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **1656**, Parent PID: **6224**

General

Target ID:	23
Start time:	09:44:41
Start date:	06/06/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6224 -s 620
Imagebase:	0x3e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
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	6B091717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE241.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE241.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\Users\user\AppData\Local\Temp\WERE271.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\Users\user\AppData\Local\Temp\WERE271.tmp.WERDataCollectionStatus.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B08497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE241.tmp	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE241.tmp.dmp	success or wait	1	6B08497A	unknown
C:\Users\user\AppData\Local\Temp\WERE271.tmp	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D2.tmp	success or wait	1	6B08497A	unknown
C:\Users\user\AppData\Local\Temp\WERE271.tmp.WERDataCollectionStatus.txt	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D2.tmp.xml	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF57B.tmp.csv	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8D7.tmp.txt	success or wait	1	6B08497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\WERE271.tmp.WERDataCollectionStatus.txt	0	2	fd fd		success or wait	1	6B08497A	unknown
C:\Users\user\AppData\Local\Temp\WERE271.tmp.WERDataCollectionStatus.txt	2	4776	0d 00 0a 00 53 00 6e 00 61 00 70 00 73 00 68 00 6f 00 74 00 20 00 73 00 74 00 61 00 74 00 69 00 73 00 74 00 69 00 63 00 73 00 3a 00 0d 00 0a 00 2d 00 20 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 50 00 53 00 53 00 44 00 2e 00 0d 00 0a 00 2d 00 20 00 46 00 6c 00 61 00 67 00 73 00 2f 00 43 00 61 00 70 00 74 00 75 00 72 00 65 00 46 00 6c 00 61 00 67 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 3a 00 20 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 31 00 2f 00 64 00 30 00 30 00 30 00 33 00 39 00 66 00 66 00 2e 00 0d 00 0a 00 2d 00 20 00 41 00 75 00 78 00 20 00 70 00 61 00 67 00 65 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20	Snapshot statistics:- Signature : PSSD.- Flags/CaptureFlags : 00000001/d00039ff.- Aux pages	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1002	66	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 69 00 6d 00 61 00 67 00 65 00 73 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>images.exe</ImageName>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1068	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1072	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1076	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1166	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1170	2	09 00		success or wait	2	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1174	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 33 00 30 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>47303</Uptime>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1430	88	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 31 00 31 00 36 00 31 00 35 00 34 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>116154368</PeakVirtualSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1528	72	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 31 00 31 00 34 00 37 00 32 00 34 00 38 00 36 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>114724864</VirtualSize>	success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 37 00 35 00 31 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>6751</PageFaultCount>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1694	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 35 00 38 00 37 00 34 00 34 00 33 00 32 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>25874432</PeakWorkingSetSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1802	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 35 00 38 00 36 00 36 00 36 00 32 00 34 00 30 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>25866240</WorkingSetSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	1894	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 39 00 31 00 30 00 31 00 36 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>191016</QuotaPeakPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2008	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2012	2	09 00		success or wait	3	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2018	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 39 00 30 00 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>190096</QuotaPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2116	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2120	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2126	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 34 00 31 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>41112</QuotaPeakNonPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2260	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 34 00 30 00 39 00 37 00 36 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>40976</QuotaNonPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2368	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2372	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2378	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 38 00 35 00 36 00 36 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>19185664</PagefileUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2466	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 34 00 37 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>19472384</PeakPagefileUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2560	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2564	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2570	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 38 00 35 00 36 00 36 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>19185664</PrivateUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2644	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2648	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2652	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2698	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2702	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2706	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2736	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2740	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2746	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2798	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2828	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2832	2	09 00		success or wait	4	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2840	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2910	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2914	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	2922	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3012	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3016	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3024	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 34 00 30 00 31 00 38 00 38 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7401888</Uptime>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3084	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3162	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3166	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3174	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3238	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	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3282	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3286	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3296	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3386	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3390	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3400	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3474	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3478	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3488	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 37 00 32 00 36 00 34 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>57264</PageFaultCount>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3578	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 34 00 38 00 35 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>104853504</PeakWorkingSetSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3692	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>104251392</WorkingSetSize>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3790	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 35 00 33 00 37 00 36 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>965376</QuotaPeakPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	3918	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 38 00 38 00 35 00 32 00 33 00 32 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>885232</QuotaPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4030	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 38 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>73832</QuotaPeakNonPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4154	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4158	2	09 00		success or wait	5	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4168	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 36 00 38 00 39 00 33 00 36 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>68936</QuotaNonPagedPoolUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4276	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4280	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4290	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 30 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34902016</PagefileUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4382	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 30 00 30 00 37 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35700736</PeakPagefileUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4490	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 30 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34902016</PrivateUsage>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4576	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4632	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4682	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4720	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4768	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4814	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4876	4	0d 00 0a 00		success or wait	8	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4880	2	09 00		success or wait	16	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	4884	80	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 62 00 61 00 64 00 5f 00 6d 00 6f 00 64 00 75 00 6c 00 65 00 5f 00 69 00 6e 00 66 00 6f 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>bad_module_info</Parameter0>	success or wait	8	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5486	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5490	2	09 00		success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5492	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5538	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	6	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	12	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	5584	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6138	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6142	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6144	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6190	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6236	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	2	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6338	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 75 00 6f 00 6b 00 6b 00 61 00 63 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>uokkac, Inc.</SystemManufacturer>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6444	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6448	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6452	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 75 00 6f 00 6b 00 6b 00 61 00 63 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>uokkac7,1</SystemProductName>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6548	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6552	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6556	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6676	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6680	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6684	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 36 00 32 00 35 00 30 00 34 00 33 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1606250432</OSInstallDate>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6766	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6770	2	09 00		success or wait	2	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6774	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6876	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6880	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6884	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6952	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6956	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6958	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7004	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7046	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7148	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	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7184	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7188	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7190	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	6	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7222	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7468	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7472	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7474	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7500	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7504	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7506	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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 34 00 34 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-06-06T16:44:47Z">	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7606	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7610	2	09 00		success or wait	2	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7614	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 30 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 33 00 38 00 38 00 32 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 33 00 38 00 38 00 32 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	<Process AsId="410" PID="6224" UptimeMS="38828" TimeSinceCreationMS="38828" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7880	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7884	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7888	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7914	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7958	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	7996	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8000	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8004	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 33 00 64 00 31 00 39 00 30 00 36 00 37 00 2d 00 33 00 38 00 66 00 65 00 2d 00 34 00 39 00 37 00 31 00 2d 00 62 00 35 00 38 00 31 00 2d 00 66 00 36 00 39 00 66 00 35 00 38 00 65 00 65 00 37 00 38 00 61 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>03d19067-38fe-4971-b581-f69f58ee78ad</Guid>	success or wait	1	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8102	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8106	2	09 00		success or wait	2	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8110	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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 34 00 34 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-06-06T16:44:47Z</CreationTime>	success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8212	2	09 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8214	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8254	4	0d 00 0a 00		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF31B.tmp.WERInternalMetadata.xml	8258	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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D2.tmp.xml	0	4554	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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.wer	0	2	fd fd		success or wait	1	6B08497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\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	124	6B08497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bad_module_info_31b4b99a83ed1b21aef14a886e70751296652b_85207d7d_0609777c\Report.wer	6692	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 33 00 38 00 35 00 37 00 30 00 32 00 35 00 38 00	MetadataHash=-338570258	success or wait	1	6B08497A	unknown

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

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

Disassembly

No disassembly