ID: 632544
Sample Name:
RFQ__637456464647.exe
Cookbook: default.jbs
Time: 18:58:49
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

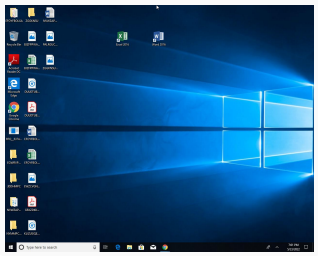
Windows Analysis Report

RFQ__6374564646647.exe

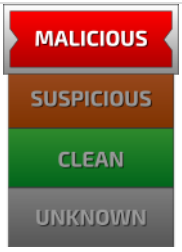
Overview

General Information

Sample Name:	RFQ__637456464647.exe
Analysis ID:	632544
MD5:	b4bc907e8d48e8..
SHA1:	592a814a428c8a..
SHA256:	7f7804a5460695..
Tags:	exe SnakeKeylogger
Infos:	



Detection



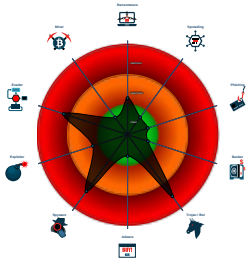
Snake Keylogger

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- RFQ__637456464647.exe (PID: 6312 cmdline: "C:\Users\user\Desktop\RFQ__637456464647.exe" MD5: B4BC907E8D48E8F09B4D9FDD8D416599)
  - RFQ__637456464647.exe (PID: 6400 cmdline: C:\Users\user\Desktop\RFQ__637456464647.exe MD5: B4BC907E8D48E8F09B4D9FDD8D416599)
  - chrome.exe (PID: 6672 cmdline: "C:\Users\user\AppData\Local\Temp\chrome.exe" MD5: 7F916511A313837EFCDE9E4112A64E5B)
  - WerFault.exe (PID: 7124 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6312 -s 1296 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "Telegram",
  "Telegram Token": "Null!",
  "Telegram ID": "5164987354:AAFbwY5baNRyoCilWU25jL6nSQnU8yn8vuc"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x185d0:$x1: $%SMTPDV$ • 0x17292:$x2: $#TheHashHere%& • 0x18578:$x3: %FTPDV$ • 0x17274:$x4: $%TelegramDv$ • 0x14ba3:$x5: KeyLoggerEventArgs • 0x14f39:$x5: KeyLoggerEventArgs • 0x185fc:$m1: \| Snake Keylogger • 0x186a2:$m1: | Snake Keylogger • 0x187f6:$m1: \| Snake Keylogger • 0x1891c:$m1: | Snake Keylogger • 0x18a76:$m1: \| Snake Keylogger • 0x1859c:$m2: Clipboard Logs ID • 0x187ac:$m2: Screenshot Logs ID • 0x188c0:$m2: keystroke Logs ID • 0x18aac:$m3: SnakePW • 0x18784:$m4: \SnakeKeylogger\
00000001.00000000.266228380.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 57 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.RFQ__637456464647.exe.400000.6.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b0d0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a2b9:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1a700:$a4: \Orbitum\User Data\Default\Login Data • 0x1b881:$a5: \Kometa\User Data\Default\Login Data
1.0.RFQ__637456464647.exe.400000.6.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
1.0.RFQ__637456464647.exe.400000.6.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
1.0.RFQ__637456464647.exe.400000.6.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
1.0.RFQ__637456464647.exe.400000.6.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 109 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.3 - Destination IP: 132.226.8.169

Timestamp:	192.168.2.3132.226.8.16949740802842536 05/23/22-19:00:12.710166
SID:	2842536
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Snake Keylogger

Yara detected Telegram RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

Yara detected Snake Keylogger

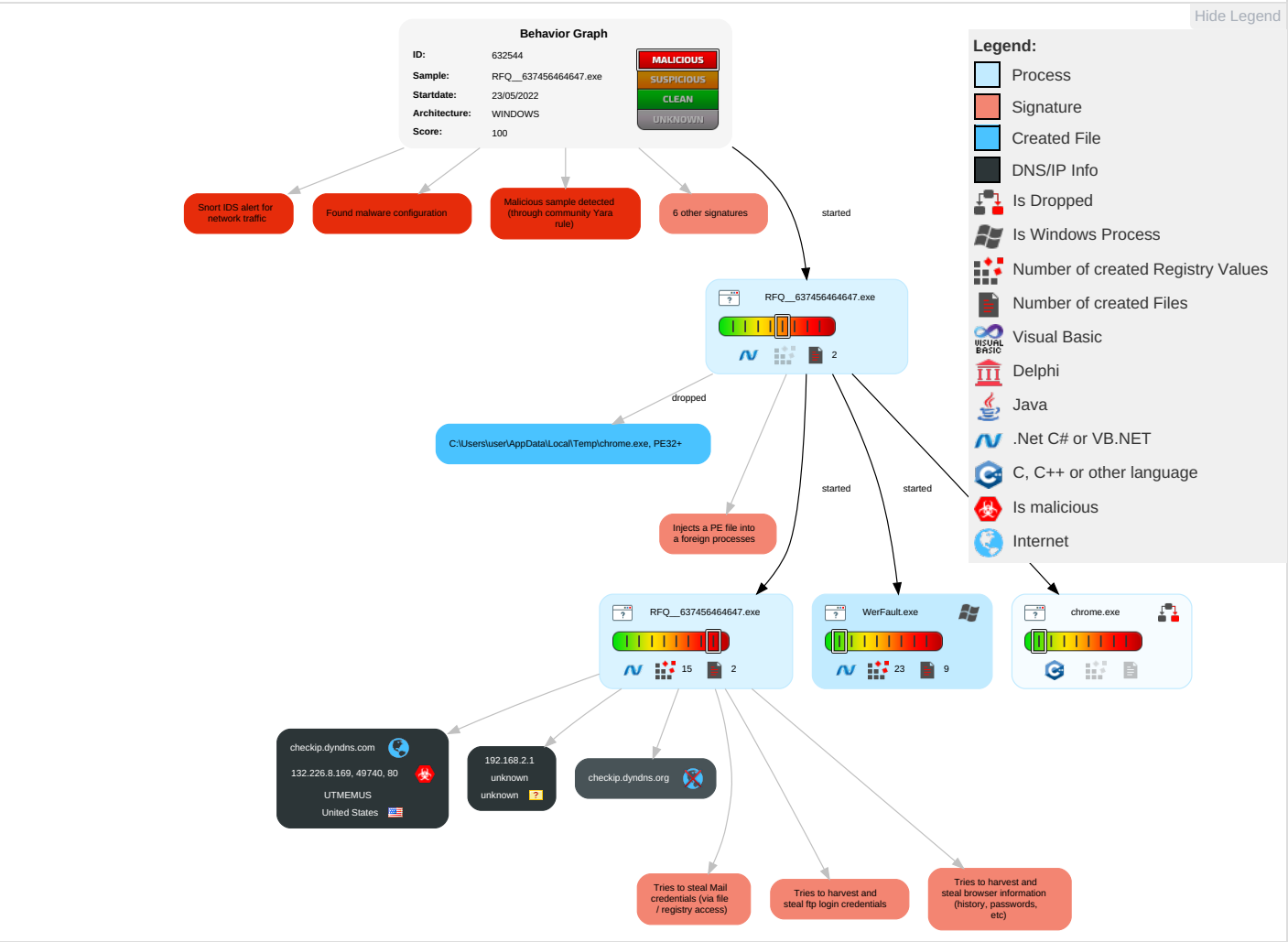
Yara detected Telegram RAT

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
1 Valid Accounts	2 Command and Scripting Interpreter	1 Valid Accounts	1 Valid Accounts	1 Valid Accounts	2 OS Credential Dumping	1 1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Access Token Manipulation	1 Input Capture	2 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 2 Process Injection	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Disable or Modify Tools	NTDS	1 Process Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 2 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

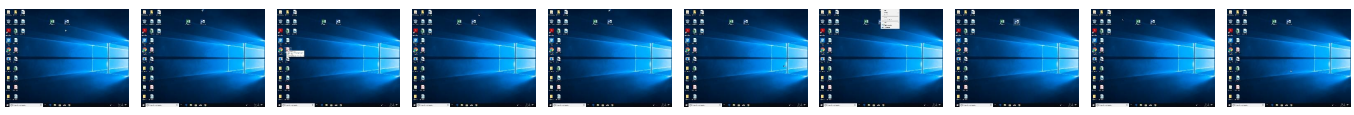
Behavior Graph

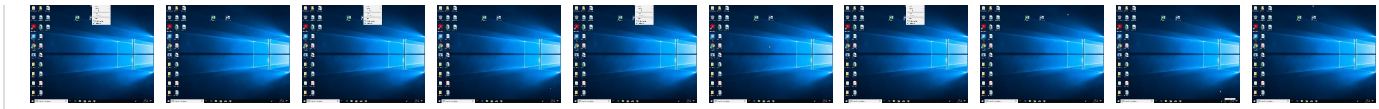


Screenshots

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
RFQ__637456464647.exe	46%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
RFQ__637456464647.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\chrome.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\chrome.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.RFQ__637456464647.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.RFQ__637456464647.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.0.RFQ__637456464647.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.0.RFQ__637456464647.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.0.RFQ__637456464647.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.0.RFQ__637456464647.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dsssdsa.fa)Uri	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/Reporting/UploadReport2	0%	URL Reputation	safe	
http://https://dsssdsa.fa	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/Reporting/	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/UploadReportLogin/	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/UploadReportLogin/GetServerURL	0%	URL Reputation	safe	
http://checkip.dyndns.org4Jk	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	132.226.8.169	true	true		unknown
checkip.dyndns.org	unknown	unknown	false		unknown

Contacted URLs

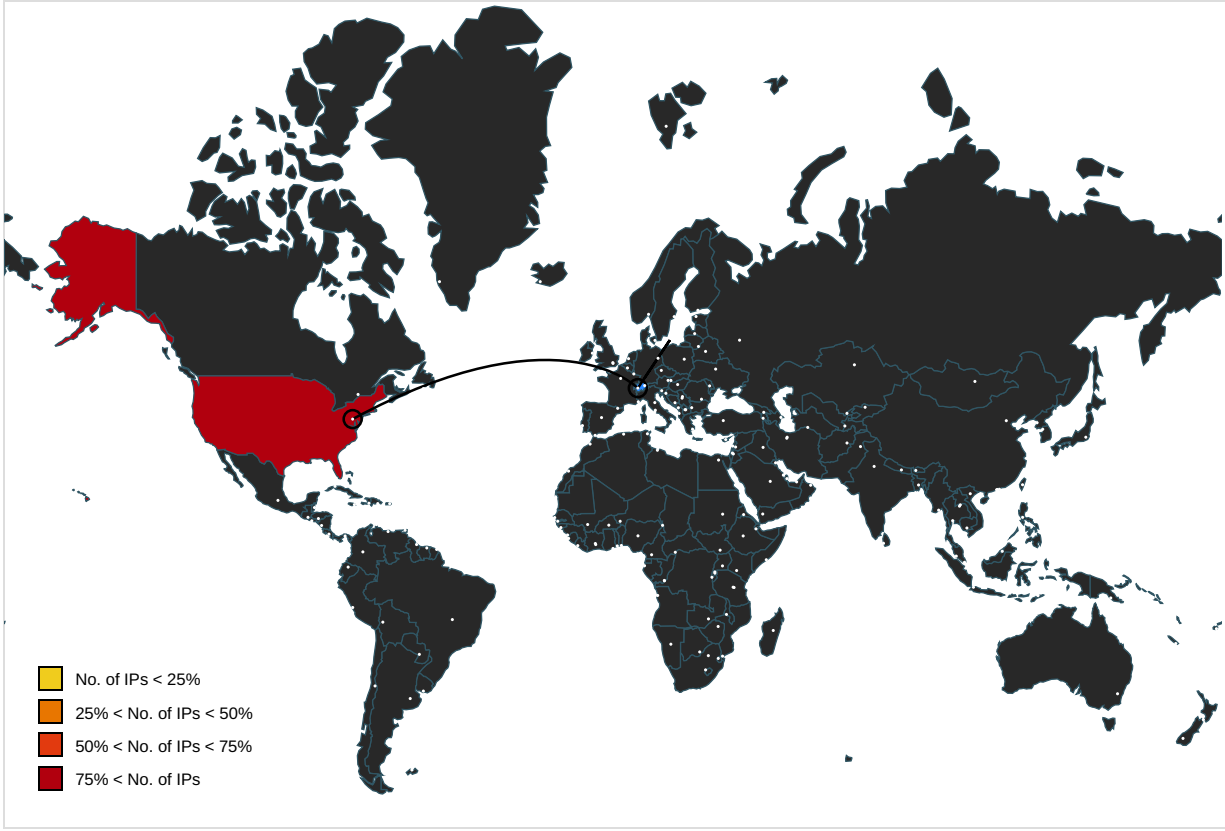
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dsssdsa.fa)Uri	RFQ__637456464647.exe	false	• Avira URL Cloud: safe	low
http://https://crashpad.chromium.org/	RFQ__637456464647.exe, 00000000.00000002.317423148.00000000044C2000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000002.318083841.0000000004762000.00000004.00000800.00020000.00000000.sdmp, chrome.exe, chrome.exe, 00000005.00000000.281746338.00007FF7A8C4A000.00000002.00000001.01000000.00000006.sdmp, chrome.exe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	RFQ__637456464647.exe, 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000000.293530185.000000004504000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://crashpad.chromium.org/bug/new	RFQ__637456464647.exe, 00000000.00000002.317423148.00000000044C2000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000002.318083841.0000000004762000.00000004.00000800.00020000.00000000.sdmp, chrome.exe, chrome.exe, 00000005.00000000.281746338.00007FF7A8C4A000.00000002.00000001.01000000.00000006.sdmp, chrome.exe.0.dr	false		high
http://checkip.dyndns.org/q	RFQ__637456464647.exe, 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000000.293530185.000000004504000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sawebservice.red-gate.com/	RFQ__637456464647.exe	false		high
http://www.smartassembly.com/webservices/Reporting/UploadReport2	RFQ__637456464647.exe	false	• URL Reputation: safe	unknown
http://https://dsssdsa.fa	RFQ__637456464647.exe	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org	RFQ__637456464647.exe, 00000001.00000002.528823599.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000001.00000002.529500482.0000000002FF7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.smartassembly.com/webservices/Reporting/	RFQ__637456464647.exe	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	RFQ__637456464647.exe, 00000001.00000002.529500482.0000000002FF7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RFQ__637456464647.exe, 00000001.00000002.528823599.0000000002F51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://crashpad.chromium.org/https://crashpad.chromium.org/bug/new	RFQ__637456464647.exe, 00000000.00000002.317423148.00000000044C2000.00000004.00000800.00020000.00000000.sdmp, RFQ__637456464647.exe, 00000000.00000002.318083841.0000000004762000.00000004.00000800.00020000.00000000.sdmp, chrome.exe, 00000005.00000000.281746338.00007FF7A8C4A000.00000002.00000001.01000000.00000006.sdmp, chrome.exe.0.dr	false		high
http://www.smartassembly.com/webservices/UploadReportLogin/	RFQ__637456464647.exe	false	• URL Reputation: safe	unknown
http://www.smartassembly.com/webservices/UploadReportLogin/GetServerURL	RFQ__637456464647.exe	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4Jk	RFQ__637456464647.exe, 00000001.00000002.528823599.0000000002F51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.226.8.169	checkip.dyndns.com	United States		16989	UTMEMUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632544
Start date and time: 23/05/202218:58:49	2022-05-23 18:58:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ__637456464647.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:	29
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.troj.spyw.evad.winEXE@6/5@2/2

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 16.1% (good quality ratio 13%) • Quality average: 58.1% • Quality standard deviation: 37.6%
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, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.182.143.212
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Execution Graph export aborted for target chrome.exe, PID 6672 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:00:24	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_RFQ__637456464 64_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159\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):	1.0802804484479727
Encrypted:	false
SSDEEP:	192:WOyEvUsxHBUZMXSaKtXfW/u7s4S274Itw:ZyEvUSBUZMXSah/u7s4X4Itw
MD5:	E56BC667B3B678430631F7CE3B8BBD4C
SHA1:	EA08F52BDD81A1D5BD03C34A20802621A13A5E8C
SHA-256:	3C7F3BEF460243B93180F3CCBD3CBC10971A29097D21F53C4B57598568A8058C
SHA-512:	F0ED9A2F476CD8B0899F8234DF82D1FFE2480992EC4EAE7A3957214828AFE6A64B9DCF86399061B7889A108F69F41485A778C450FBDC86D64B8B15D2E69B33D
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.8.3.1.2.2.0.5.7.1.0.4.9.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.8.3.1.2.2.2.9.1.4.7.8.7.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.a.a.d.a.1.6.-.4.1.d.c.-.4.9.d.f.-.a.e.5.1.-.3.4.8.f.7.9.c.5.3.0.7.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.=.f.6.5.2.5.6.8.f.-.b.b.9.9.-.4.8.f.2.-.b.a.9.1.-.9.a.0.e.c.b.9.8.4.a.0.b.....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.=.R.F.Q._._.6.3.7.4.5.6.4.6.4.6.4.7...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.J.x.l.l.a.R.U.T.v.a.L.x.e.x.P.W.T.L.b.b.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.a.8.-.0.0.0.1.-.0.0.1.d.-.9.b.e.e.-.a.2.f.7.1.1.6.f.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.4.b.d.2.8.a.4.2.a.c.e.9.6.7.0.f.5.3.9.7.b.7.b.0.8.5.f.4.b.9.c.f.0.0.0.0.0.0.0.0.!.0.0.0.0.5.9.2.a.8.1.4.a.4.2.8.c.8.a.5.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 24 02:00:21 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	265529
Entropy (8bit):	3.312337303087705
Encrypted:	false
SSDEEP:	3072:rkHORSy0dv9UCgUnOw9gIOgF5xlH0DhmGndsTjd+pe:rkkTcTjP9RpDxt0AGFp
MD5:	7973C58C32915FBA6B5E4EEE9BF12854
SHA1:	8FBE6CBECD95C5CE84DC87F9A6399D06FD2BDBBC
SHA-256:	0583DBAE1CBBF287351119BDE87703268E64DA8D430F9D3C33A9D99C185432B2
SHA-512:	16E6182D38A8D0AB550B3FA310E6FC81E84E8AEEF686015B9050A2F8CB1A74D6C406CEFBC0A830E496F8655DEADB904F7444CA7835083ECBF4B1235098380E9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....5<.b.....t.....T...p"..... T..... `.....8.....T.....A..)..... "..... $..... U..... B.....H%... ...GenuineIntelW..... T..... <.b..... 0..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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):	8422
Entropy (8bit):	3.6962392631754497
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicG6yVG6YWhSUvlCvGgmfZF3S3Cprz89bphsfSYjm:RrlsNi16yVG6YgSUvlzgmf73S7pafSx
MD5:	DB6D045DBC6C75AE674930E621C24D0C
SHA1:	EC5D9E89F492C938C6B45FD7948D6D7E630575C0
SHA-256:	6763D58AA2DA5B1C0DB34B2CD54ABF3DEA1334933A99F235945CFDD3CD6B445A
SHA-512:	27D6CDA8DA201F33BCEFFBD510B010C421FD95B0D2871636315AA63C3147B43E11CB310388FB9AD143452D723651EFF61E9350C20A72AD7EB47BF5352048A18A
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.>.6.3.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4794
Entropy (8bit):	4.506229802328503
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9AGWgc8sqYj68fm8M4JKOwO7FnHno+q8vrOwOsUPOY4TsK3QE:uITf9nHgrsqYbJ7wcIKawyPO1Y1ud
MD5:	10BD2D57F1961B27D477C05A55D89E59
SHA1:	1ABFAD5821C4BC61962184488F33565531BB59F9
SHA-256:	40DBD1A60D73AA328FAB8171384B79764B1A0F1A934FB1038CC0BE506F2CEB11
SHA-512:	D8A24722E437F15B220AF4A2AC6BB5DA80E8F6B90C25CA69C3FCE203329D755953F8F9B739039FC3EE766DFB9D7273A9790535D741CBB8856F02A386D36C828
Malicious:	false
Reputation:	low
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="1528511" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\chrome.exe

Process:	C:\Users\user\Desktop\RFQ__637456464647.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2622352
Entropy (8bit):	6.584925607886023
Encrypted:	false
SSDEEP:	49152:ZkwWDBRk5Swp1oFSFb8XUK+3crWECSP/cESM0RCZ/Sf8peUTbVkyC:2TX79FXCaSMHpC
MD5:	7F916511A313837EFCDE9E4112A64E5B
SHA1:	6A2A2427CF1D888CB40A18527478C84DEDF1DB61
SHA-256:	F342AF2B1E3DD9BA90C10F643EC1F50459EFBB5912496E8AC553682C2B7A9F6E
SHA-512:	A2F92AE37D6ECD16D7B4312EA2548F494D01BD386A439E05258073F4038FCFA60BD7D79FCB8CA5B285BAC121799826B87655EC594F7B4A9CCF5DA70CE3273EB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....\|b.....".....@.....(.....(...`.....u .....u .P.....#.P.....".....'..#....(..#...L .8.....XK .(....!..0.....} .....`f .`.....text...x..... ..`.rdata...#... ...$.....@..@.data....+...P!.....,!.....@....pdata.....".....!.....@..@.00cfg..(....`#.....".....@..@.retplne$....p#.....".....tls....9....#.....".....@...CPADinfo8.....#.....".....@..._RDATA.....#.....".....@..@.rsrc...P.....#.....".....@..@.reloc...#....(..$...'.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.991836040381107
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	RFQ__637456464647.exe
File size:	2844160
MD5:	b4bc907e8d48e8f09b4d9fdd8d416599
SHA1:	592a814a428c8a5de3f06245996fc775e8dc987f
SHA256:	7f7804a5460695dae61e378d733f0a613083e84c654ea6264a5276944b33f943
SHA512:	b74608846f9e494789e52b79e1aab9fd5fa7918b46441cc0cf2ee0d2883151c327180b4119bbeae6bd83360dcedc8c6142e6fab0b56650b818aa51a2527d6759
SSDEEP:	49152:oXJTCTSfReUawVjvGdhAD7E3lJ6daAQeFdjwCE1/02Xro9+83qpK:suoRZawVjvGdhGE3lJA/jwD82013q
TLSH:	A9D52383B38AA47AF0BC25B4DCC3EB834F65579C5665FCD62A8151AC38253BBE570213

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......b................Z+..........y+.. ....+...@.. ....+.......+...@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x6b791a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x628B062E [Mon May 23 03:57:34 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2b78d0	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2b8000	0x72a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2ba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2b5920	0x2b5a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x2b8000	0x72a	0x800	False	0.31591796875	data	4.48924436504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2ba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2b80b8	0x27c	data		
RT_MANIFEST	0x2b8334	0x1fa	XML 1.0 document, ASCII text, with very long lines, with no line terminators		
RT_MANIFEST	0x2b8530	0x1fa	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0

Description	Data
InternalName	JxIIaRUTvaLxexPWTLbbe.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	JxIIaRUTvaLxexPWTLbbe.exe

Possible Origin

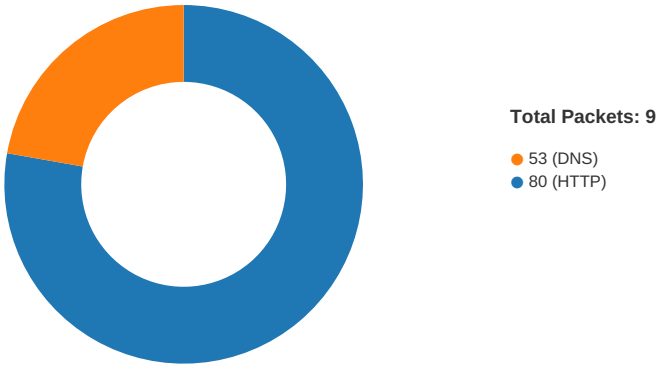
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3132.226.8.169 49740802842536 05/23/22-19:00:12.710166	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49740	80	192.168.2.3	132.226.8.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 19:00:09.422519922 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:00:12.433237076 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:00:12.709538937 CEST	80	49740	132.226.8.169	192.168.2.3
May 23, 2022 19:00:12.709647894 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:00:12.710165977 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:00:12.986522913 CEST	80	49740	132.226.8.169	192.168.2.3
May 23, 2022 19:00:13.988107920 CEST	80	49740	132.226.8.169	192.168.2.3
May 23, 2022 19:00:14.126456022 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:01:18.987670898 CEST	80	49740	132.226.8.169	192.168.2.3
May 23, 2022 19:01:18.987759113 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:01:54.057121992 CEST	49740	80	192.168.2.3	132.226.8.169
May 23, 2022 19:01:54.333545923 CEST	80	49740	132.226.8.169	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 19:00:09.279763937 CEST	64851	53	192.168.2.3	8.8.8.8
May 23, 2022 19:00:09.298605919 CEST	53	64851	8.8.8.8	192.168.2.3
May 23, 2022 19:00:09.312563896 CEST	49316	53	192.168.2.3	8.8.8.8
May 23, 2022 19:00:09.331444979 CEST	53	49316	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 19:00:09.279763937 CEST	192.168.2.3	8.8.8.8	0xc5ee	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.312563896 CEST	192.168.2.3	8.8.8.8	0x2cce	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.298605919 CEST	8.8.8.8	192.168.2.3	0xc5ee	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
May 23, 2022 19:00:09.331444979 CEST	8.8.8.8	192.168.2.3	0x2cce	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

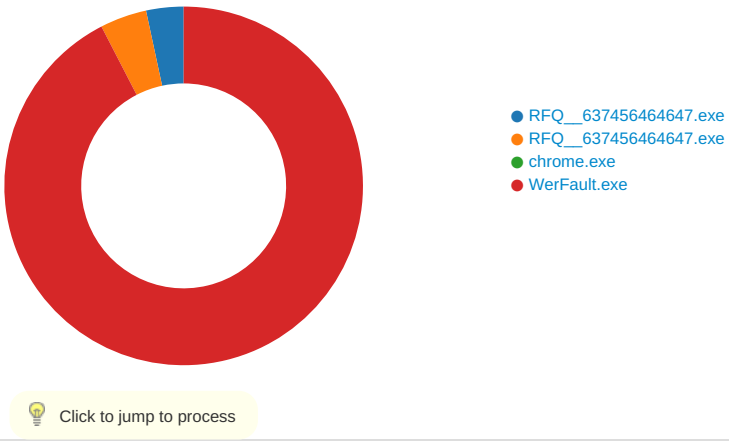
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49740	132.226.8.169	80	C:\Users\user\Desktop\RFQ__637456464647.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 19:00:12.710165977 CEST	1139	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 19:00:13.988107920 CEST	1139	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 17:00:13 GMT Content-Type: text/html Content-Length: 103 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 31 39 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.19</body></html>

Statistics

Behavior



System Behavior

Analysis Process: RFQ__637456464647.exe PID: 6312, Parent PID: 4684

General

Target ID:	0
Start time:	18:59:56
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\RFQ__637456464647.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ__637456464647.exe"
Imagebase:	0xd20000
File size:	2844160 bytes
MD5 hash:	B4BC907E8D48E8F09B4D9FDD8D416599
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.295208630.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.300985988.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.300985988.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.300985988.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.300985988.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.318129181.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.318129181.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.318129181.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.318129181.00000000047A4000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.293530185.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.293530185.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.293530185.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.293530185.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.292477124.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.292477124.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.292477124.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.292477124.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.300121250.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.300121250.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.300121250.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.300121250.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.317016109.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.317478170.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.317478170.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.317478170.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.317478170.0000000004504000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.299489390.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.299489390.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.299489390.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.299489390.00000000042C9000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrome.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0D1E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrome.exe	0	2622352	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 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 24 00 00 50 45 00 00 64 fd 0b 00 1e 07 7c 62 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 04 1c 00 00 fd 0b 00 00 00 00 00 30 11 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 28 00 00 04 00 00 fd fd 28 00 02 00 60 fd 00 00 fd 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEd|b"@((`	success or wait	1	6C0D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DBCD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DBCD72F	unknown
C:\Users\user\Desktop\RFQ__637456464647.exe	unknown	4096	success or wait	1	6DBCD72F	unknown
C:\Users\user\Desktop\RFQ__637456464647.exe	unknown	512	success or wait	1	6DBCD72F	unknown

Analysis Process: RFQ__637456464647.exe PID: **6400**, Parent PID: **6312**

General

Target ID:	1
Start time:	18:59:58
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\RFQ__637456464647.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ__637456464647.exe
Imagebase:	0x8f0000
File size:	2844160 bytes
MD5 hash:	B4BC907E8D48E8F09B4D9FDD8D416599
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000000.267692324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000000.266228380.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000000.266228380.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.266228380.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000000.266228380.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000002.525677202.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.525677202.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.525677202.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000002.525677202.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000000.270358708.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000000.270358708.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.270358708.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000000.270358708.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000000.268966946.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000000.268966946.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.268966946.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000000.268966946.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

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	6DC0CF06	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	6DC0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C0D1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6672**, Parent PID: **6312**

General

Target ID:	5
Start time:	19:00:08
Start date:	23/05/2022
Path:	C:\Users\user\AppData\Local\Temp\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\chrome.exe"
Imagebase:	0x7ff7a8a70000
File size:	2622352 bytes
MD5 hash:	7F916511A313837EFCDE9E4112A64E5B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

Analysis Process: WerFault.exe PID: **7124**, Parent PID: **6312**

General

Target ID:	13
Start time:	19:00:19
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6312 -s 1296
Imagebase:	0xf40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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\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	68FD1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ__63745646464_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ__63745646464_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	68FC497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp.xml	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34C6.tmp.csv	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34D6.tmp.txt	success or wait	1	68FC497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 35 3c fd 62 fd 05 12 00 00 00 00 00	MDMP 5<b	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	9544	6	00 00 00 00 00 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 48 25 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 1c 3c fd 62 00 00 00 00 02 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBH%GenuineIntelWT<b 0Pacific Standard TimePacific Daylight T ime	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	11506	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 fd fd 36 01 05 00 00 00 00 00 00 00 05 00 00 00 30 fd 36 01 fd fd 36 01 22 fd fd 75 23 00 00 00 16 02 00 00 30 fd 36 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++6066"u#06+	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 22 fd fd 75 00 00 00 00 05 00 00 00 00 00 00 00 05 40 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6d 00 00 00 00 fd 0f 77 01 00 00 00 00 44 fd 36 01 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 28 10 77 01 00 00 00 00 fd fd 36 01 00 00 00 00 fd 5f fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 30 11 fd 6b 00 00 00 00 50 fd 36 01 00 00 00 00 fd 02 00 00 fd 2c 00 00	RCC"u@mwD6(w6_m0k P6,	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	21530	20	fd 01 00 00 30 fd 7d 6d 00 00 00 00 fd 0b 00 00 fd 71 00 00	0}mq	success or wait	474	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	29118	2980	00 00 fd fd fd 43 fd 10 fd fd fd 24 fd fd 4d 0a fd 60 28 fd 73 fd d5 2e 2a 6c 54 02 fd fd 53 fd fd 10 fd fd 00 0a 4a fd fd fd 5c fd fd 09 0c 54 66 74 fd 22 04 20 05 fd 18 fd 02 fd 51 fd 49 2a 54 66 28 30 53 fd fd 33 22 08 7b 30 0c fd fd fd 12 fd fd 70 fd 11 fd 68 44 23 1a 48 46 34 fd 11 fd 68 44 23 1a 48 36 4c 2a 7c 48 15 41 fd fd 03 22 05 63 fd 0c 0c 0c 57 fd 46 68 fd fd 48 2a fd 1c 30 fd 5c 45 62 fd 34 fd 26 fd 69 1a 72 3f 14 fd fd fd fd fd 6a 64 fd 40 39 fd 56 2a fd 62 b9 fd 16 fd 72 2a 17 12 a0 54 fd 48 fd fd fd 18 50 4f fd 65 fd fd fd 76 14 fd 15 fd fd 49 25 43 fd 15 fd 10 4f 51 fd 52 01 fd 19 0f fd 4c 43 fd 7e 04 24 5a 70 fd 64 49 fd 11 34 fd fd fd fd 0a 3b 18 fd 38 41 61 2a fd fd 17 56 fd 50 4b fd fd 2a fd 20 fd	C$M`.*lTSJ\Tft"QI*Tf(0S3"{0phD#F4hD#6L*\|HA"cWFhH*0\Eb4&ir?jd@9V*br*THPOevI%COQRLC~$ZpdI4;Aa*VPK*	success or wait	473	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	239543	100	00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 34 22 12 6c 00 00 00 00 30 fd 13 00 00 00 00 00 00 00 00 00 01 21 00 00 04 00 00 00 1d 01 30 00 01 00 00 00 04 00 00 00 00 fd 00 00 00 00 00 00 fd 00 00 00 fd 00 02 00 00 00 00 00 fd 00 02 00 00 00 00 00 fd 00 02 00 00 00 00 00 fd 00 02 00 00 00 00 00	4"l0!0	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	1800	4	0d 00 00 00		success or wait	13	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	12222	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 48 fd 36 01 fd fd 4c 77 23 00 00 00 06 02 00 00 fd fd 36 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++H6Lw#6+	success or wait	13	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	2380	48	0c 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 13 01 00 00 00 00 40 fd fd 06 00 00 00 00 fd 06 00 00 fd fd 02 00 fd 02 00 00 4e 51 00 00	@NQ	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	2440	4	3b 00 00 00	;	success or wait	59	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	9550	48	2a 00 00 00 52 00 46 00 51 00 5f 00 5f 00 36 00 33 00 37 00 34 00 35 00 36 00 34 00 36 00 34 00 36 00 34 00 37 00 2e 00 65 00 78 00 65 00 00 00	*RFQ__637456464647.exe	success or wait	59	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	8708	120	00 00 10 6b 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a 7a 2c 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 03 00 00 00	k`Zz,?)@A	success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	11424	24	12 00 00 00 70 00 73 00 61 00 70 00 69 00 2e 00 64 00 6c 00 6c 00 00 00	psapi.dll	success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	8876	668	00 00 fd 6f 00 00 00 00 00 fd 16 00 fd 69 17 00 08 fd fd 77 fd 2c 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd fd 02 00 00 00 00 00 fd 06 03 00 00 00 00 42 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 d6 03 00 00 00 00 00 9a 03 00 00 00 00 00 00 00 00 00 00 00 00 3c fd 1a 00 00 00 00 00 04 31 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 0e 48 47 00 00 00 00 1f 71 73 1b 00 00 00 00 2a fd 25 21 00 00 00 00 fd 7c 1f 01 00 00 00 00 fd fd 00 00 fd 15 01 00 61 fd 06 00 60 fd 0a 00 04 31 05 00 06 7f 15 00 fd fd 05 00 6b 5e 3f 00 79 fd 01 00 de 17 00 00 00 00 00 46 fd 29 00 66 79 04	oiw,ZbB<1@HGqs*%!|a`1k^?yF)fy	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	239643	25886	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7284.tmp.dmp	32	120	03 00 00 00 74 02 00 00 08 07 00 00 04 00 00 00 fd 18 00 00 fd 09 00 00 0e 00 00 00 54 00 00 00 70 22 00 00 05 00 00 00 fd 1d 00 00 1a 54 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 10 41 00 00 29 fd 03 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	tTp"T`8TA)"$	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6312</Pid>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1002	88	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 52 00 46 00 51 00 5f 00 5f 00 36 00 33 00 37 00 34 00 35 00 36 00 34 00 36 00 34 00 36 00 34 00 37 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>RFQ__637456464647.exe</ImageName>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1090	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1094	2	09 00		success or wait	2	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1098	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1188	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1192	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1196	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 35 00 34 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>25490</Uptime>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1240	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1244	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1248	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1330	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1334	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1338	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1390	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1394	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1398	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1442	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1446	2	09 00		success or wait	3	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1452	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 32 00 31 00 36 00 36 00 36 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>216662016</PeakVirtualSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1540	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1544	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1550	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 32 00 30 00 37 00 37 00 39 00 34 00 31 00 37 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>207794176</VirtualSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1622	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1626	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1632	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 31 00 30 00 31 00 33 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>10131</PageFaultCount>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1708	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1712	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1718	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 33 00 39 00 30 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>39047168</PeakWorkingSetSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1816	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1820	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1826	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 33 00 39 00 30 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>39047168</WorkingSetSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1908	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1912	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	1918	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 33 00 33 00 32 00 30 00 35 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>332056</QuotaPeakPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2032	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2036	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2042	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 33 00 31 00 33 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>313568</QuotaPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2140	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2144	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2150	126	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 31 00 30 00 30 00 30 00 31 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>100120</QuotaPeakNonPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2276	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2280	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2286	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 39 00 39 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>99768</QuotaNonPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2394	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2398	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2404	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 38 00 35 00 37 00 39 00 34 00 35 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>18579456</PagefileUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2482	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2486	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2492	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 38 00 35 00 39 00 31 00 37 00 34 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>18591744</PeakPagefileUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2586	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2590	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2596	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 38 00 35 00 37 00 39 00 34 00 35 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>18579456</PrivateUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2670	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2674	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2678	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2732	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2772	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	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2824	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2854	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2858	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2866	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2936	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2940	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	2948	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3038	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3042	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3050	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 39 00 30 00 33 00 37 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4290371</Uptime>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3098	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3102	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3110	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3188	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3192	2	09 00		success or wait	4	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3200	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3252	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3256	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3264	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3308	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3312	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3322	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3412	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3416	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3426	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3500	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3504	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3514	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 34 00 39 00 34 00 30 00 39 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>49409</PageFaultCount>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3590	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3594	2	09 00		success or wait	5	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3604	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 32 00 32 00 36 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102268928</PeakWorkingSetSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3704	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3708	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3718	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 31 00 38 00 35 00 35 00 32 00 33 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>101855232</WorkingSetSize>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3802	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3806	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3816	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 36 00 39 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>965696</QuotaPeakPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3930	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3934	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	3944	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 39 00 31 00 39 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>919360</QuotaPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4042	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4046	2	09 00		success or wait	5	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4056	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 30 00 36 00 35 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 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>70656</QuotaPeakNonPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4180	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4184	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4194	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 30 00 31 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>68016</QuotaNonPagedPoolUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4302	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4306	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4316	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 35 00 30 00 34 00 37 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34504704</PagefileUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4394	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4398	2	09 00		success or wait	5	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4408	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 33 00 31 00 39 00 38 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35319808</PeakPagefileUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4502	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4506	2	09 00		success or wait	5	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4516	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 35 00 30 00 34 00 37 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34504704</PrivateUsage>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4590	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4594	2	09 00		success or wait	4	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4602	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4648	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4652	2	09 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4658	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4708	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4746	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4794	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	2	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4840	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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>CLR20r3</EventType>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4900	4	0d 00 0a 00		success or wait	9	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4904	2	09 00		success or wait	18	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	4908	92	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 52 00 46 00 51 00 5f 00 5f 00 36 00 33 00 37 00 34 00 35 00 36 00 34 00 36 00 34 00 36 00 34 00 37 00 2e 00 65 00 78 00 65 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>RFQ__637456464647.exe</Parameter0>	success or wait	9	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5616	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5656	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5660	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5662	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5700	4	0d 00 0a 00		success or wait	6	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5704	2	09 00		success or wait	12	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	5708	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6268	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6308	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6312	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6314	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6352	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6356	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6360	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6454	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6458	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6462	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 76 00 6d 00 6f 00 70 00 79 00 72 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>vmopyr, Inc.</SystemManufacturer>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6568	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6572	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6576	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 76 00 6d 00 6f 00 70 00 79 00 72 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>vmopyr7,1</SystemProductName>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6672	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6676	2	09 00		success or wait	2	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6680	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6800	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6804	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6808	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 31 00 34 00 31 00 38 00 30 00 36 00 34 00 31 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>1614180641</OSInstallDate>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6890	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6894	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	6898	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7008	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7082	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7128	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7170	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7272	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7308	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7312	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7314	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7338	4	0d 00 0a 00		success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7342	2	09 00		success or wait	6	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7346	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7592	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7596	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7598	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7624	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7628	2	09 00		success or wait	1	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7630	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 34 00 54 00 30 00 32 00 3a 00 30 00 30 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-24T02:00:22Z">	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7730	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7734	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	7738	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 33 00 39 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 33 00 33 00 37 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 33 00 33 00 37 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="395" PID="6312" UptimeMS="13374" TimeSinceCreationMS="13374" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8012	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8038	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8076	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8080	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8082	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	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8120	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8124	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8128	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 35 00 61 00 61 00 64 00 61 00 31 00 36 00 2d 00 34 00 31 00 64 00 63 00 2d 00 34 00 39 00 64 00 66 00 2d 00 61 00 65 00 35 00 31 00 2d 00 33 00 34 00 38 00 66 00 37 00 39 00 63 00 35 00 33 00 30 00 37 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>75aada16-41dc-49df-ae51-348f79c5307d</Guid>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	2	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8234	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 34 00 54 00 30 00 32 00 3a 00 30 00 30 00 3a 00 32 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-24T02:00:22Z</CreationTime>	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8332	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8336	2	09 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8338	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	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8378	4	0d 00 0a 00		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78ED.tmp.WERInternalMetadata.xml	8382	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	68FC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A56.tmp.xml	0	4794	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ__63745646464_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159\Report.wer	0	2	fd fd		success or wait	1	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ__63745646464_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159\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	187	68FC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RFQ__63745646464_94dd9d68755d61cc97c9e42d0ec1b28c5989ec6_083b13b0_1b958159\Report.wer	13904	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 30 00 37 00 38 00 34 00 38 00 33 00 31 00 30 00	MetadataHash=1207848310	success or wait	1	68FC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__63745646464|983115d	success or wait	1	68FE36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	68FE1FB2	RegCreateKeyExW
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	68FC43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__63745646464|983115d	ProgramId	unicode	00064bd28a42ace9670f5397b7b085f4b9cf00000000	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__63745646464|983115d	FileId	unicode	0000592a814a428c8a5de3f06245996fc775e8dc987f	success or wait	1	68FE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	LowerCaseLongPath	unicode	c:\users\user\desktop\rfq__637 456464647.exe	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	LongPathHash	unicode	rfq__63745646464|983115d	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	Name	unicode	rfq__637456464647.exe	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	Publisher	unicode		success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	Version	unicode	0.0.0.0	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	BinFileVersion	unicode	0.0.0.0	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	BinaryType	unicode	pe32_clr_32	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	ProductName	unicode		success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	ProductVersion	unicode	0.0.0.0	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	LinkDate	unicode	05/23/2022 03:57:34	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	BinProductVersion	unicode	0.0.0.0	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	Size	B	00 66 2B 00 00 00 00 00	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	Language	dword	0	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	IsPeFile	dword	1	success or wait	1	68FE36BF	unknown
\REGISTRY\A\{8db74139-9b4a-e3e1-0313-53ba814e9f14}\Root\InventoryApplicationFile\rfq__6374 5646464|983115d	IsOsComponent	dword	0	success or wait	1	68FE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 F4 75 05 00 00 00 05 40 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A7 6D E8 0F 77 01 44 EF 36 01 01 00 00 00 03 00 00 00 28 10 77 01 84 EE 36 01 CA 5F A9 6D 00 00 00 00 30 11 C6 6B 50 EE 36 01	success or wait	1	68FE1FE8	RegSetValueExW

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

Disassembly

No disassembly