ID: 652387
Sample Name: fleW7NKwt9.exe
Cookbook: default.jbs
Time: 09:34:41
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

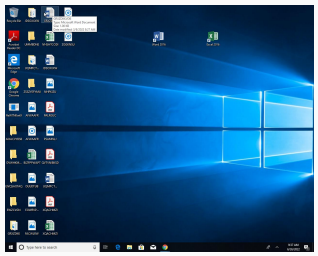
Windows Analysis Report

fleW7NKwt9.exe

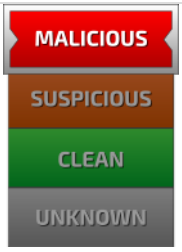
Overview

General Information

Sample Name:	fleW7NKwt9.exe
Analysis ID:	652387
MD5:	07edca391e6f40..
SHA1:	c64b12430fb6b2..
SHA256:	d30687d6d06df3..
Tags:	exe SnakeKeylogger
Infos:	



Detection



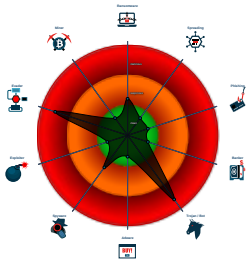
Snake Keylogger

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- May check the online IP address of…
- .NET source code contains potentia…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- fleW7NKwt9.exe (PID: 6476 cmdline: "C:\Users\user\Desktop\fleW7NKwt9.exe" MD5: 07EDCA391E6F402F748CB369540E7073)
  - fleW7NKwt9.exe (PID: 1316 cmdline: C:\Users\user\Desktop\fleW7NKwt9.exe MD5: 07EDCA391E6F402F748CB369540E7073)
    - WerFault.exe (PID: 6644 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1316 -s 1528 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "Username": "myreportlog@valete.buzz",
  "Password": "7213575aceACE@#$",
  "Host": "cp5ua.hyperhost.ua",
  "Port": "myreport@valete.buzz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x173b0:$x1: $%SMTPDV$ • 0x173c6:$x2: $#TheHashHere%& • 0x18760:$x3: %FTPDV$ • 0x18828:$x4: $%TelegramDv$ • 0x14cf7:$x5: KeyLoggerEventArgs • 0x1508d:$x5: KeyLoggerEventArgs • 0x187d0:$m1: \| Snake Keylogger • 0x18888:$m1: | Snake Keylogger • 0x189dc:$m1: \| Snake Keylogger • 0x18b02:$m1: | Snake Keylogger • 0x18c5c:$m1: \| Snake Keylogger • 0x18784:$m2: Clipboard Logs ID • 0x18992:$m2: Screenshot Logs ID • 0x18aa6:$m2: keystroke Logs ID • 0x18c92:$m3: SnakePW • 0x1896a:$m4: \SnakeKeylogger\
00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.fleW7NKwt9.exe.400000.14.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b2e6:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a4cf:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1a916:$a4: \Orbitum\User Data\Default\Login Data • 0x1ba97:$a5: \Kometa\User Data\Default\Login Data
3.0.fleW7NKwt9.exe.400000.14.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
3.0.fleW7NKwt9.exe.400000.14.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
3.0.fleW7NKwt9.exe.400000.14.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
3.0.fleW7NKwt9.exe.400000.14.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 76 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.6 - Destination IP: 132.226.8.169

Timestamp:	192.168.2.6132.226.8.16949769802842536 06/26/22-09:36:21.815879
SID:	2842536
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected Snake Keylogger

Yara detected Telegram RAT

Remote Access Functionality

Yara detected Snake Keylogger

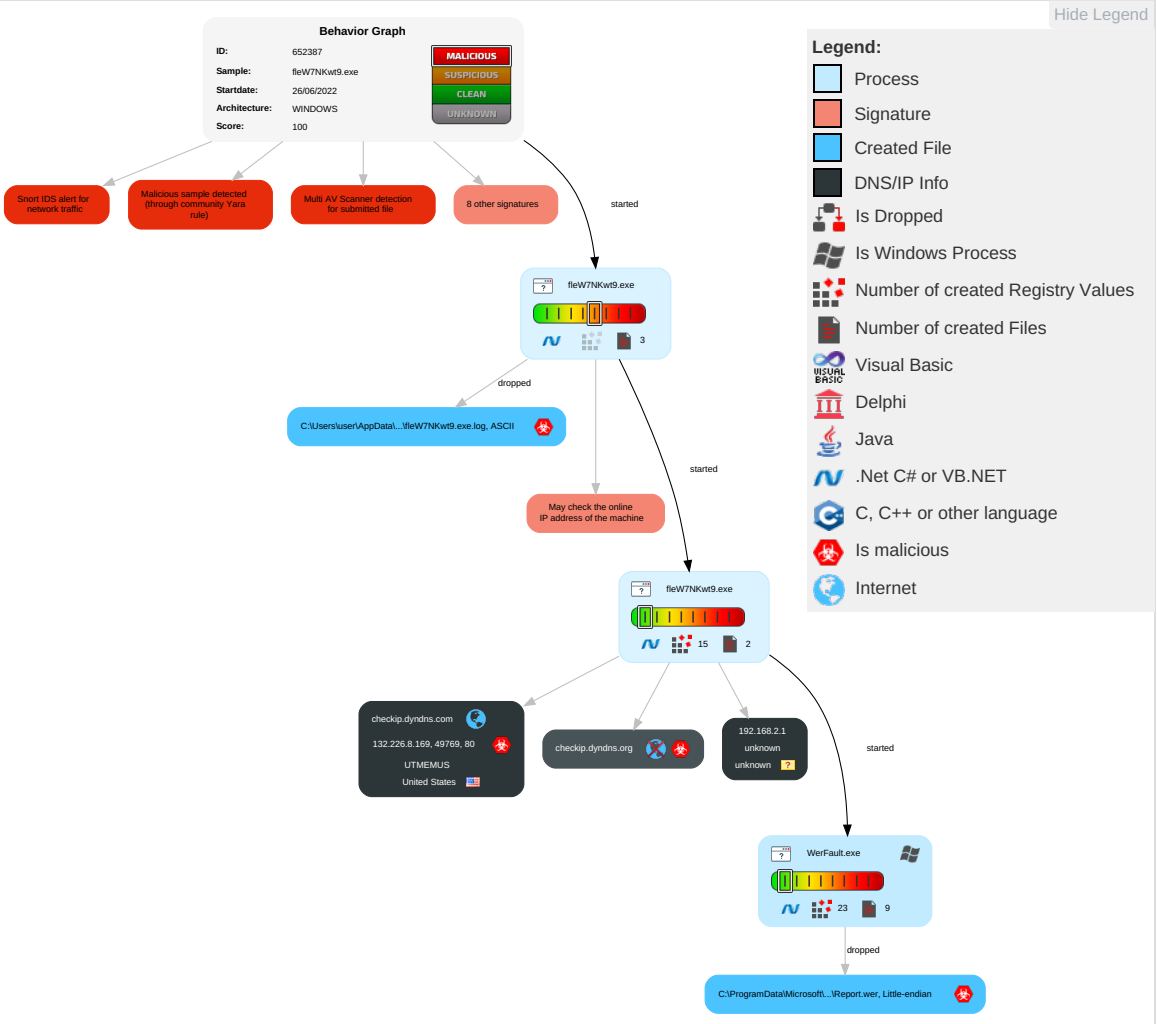
Yara detected Telegram RAT

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
Valid Accounts	1 Native API	Path Interception	1 1 Process Injection	1 Masquerading	1 Input Capture	1 1 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	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 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

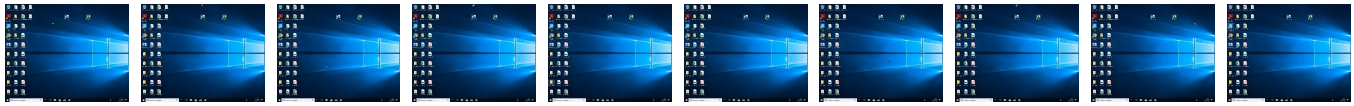
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
fleW7NKwt9.exe	33%	Virustotal		Browse
fleW7NKwt9.exe	54%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	
fleW7NKwt9.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.fleW7NKwt9.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.fleW7NKwt9.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.0.fleW7NKwt9.exe.400000.14.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.0.fleW7NKwt9.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.0.fleW7NKwt9.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.0.fleW7NKwt9.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.0.fleW7NKwt9.exe.400000.16.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
3.2.fleW7NKwt9.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	132.226.8.169	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

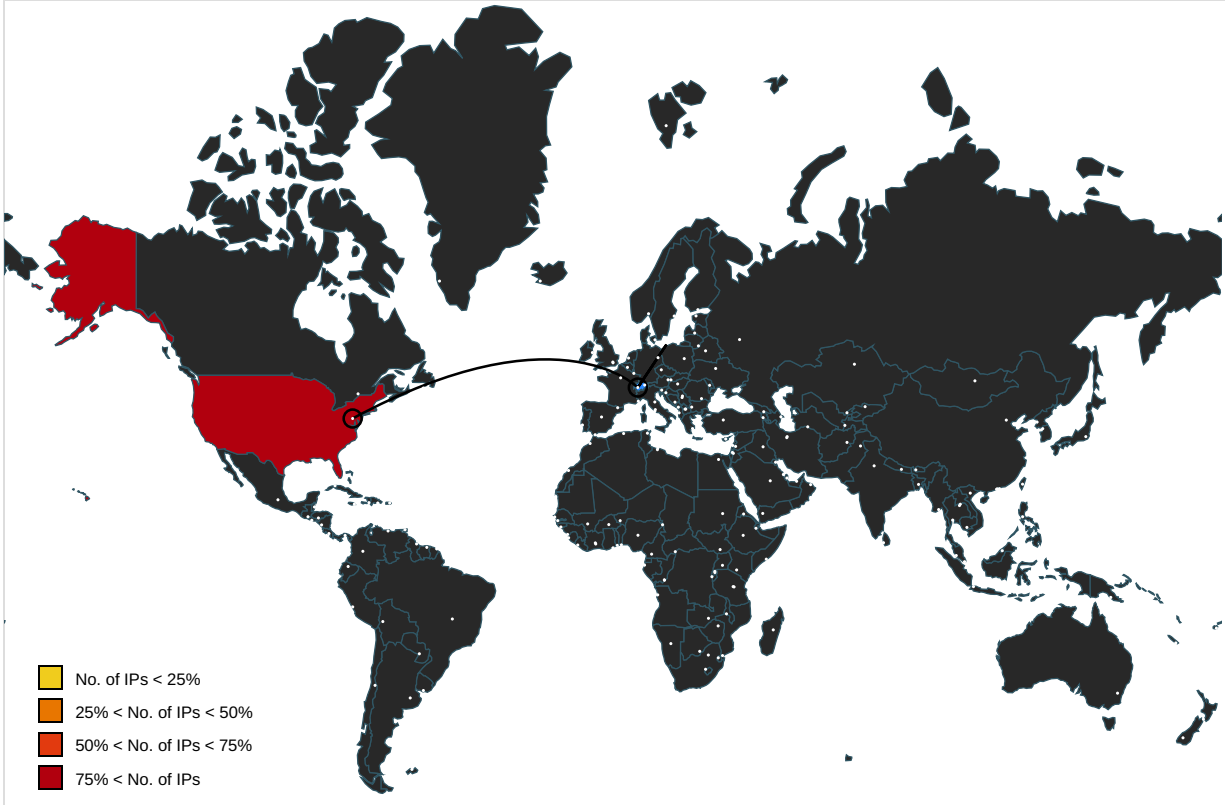
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	fleW7NKwt9.exe, 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, fleW7NKwt9.exe, 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp, fleW7NKwt9.exe, 00000000.00000003.385930269.0000000000AAC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org	fleW7NKwt9.exe, 00000003.00000002.467045157.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, fleW7NKwt9.exe, 00000003.00000002.467289457.0000000002BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4	fleW7NKwt9.exe, 00000003.00000002.467045157.0000000002B41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://checkip.dyndns.org/q	fleW7NKwt9.exe, 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, fleW7NKwt9.exe, 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	fleW7NKwt9.exe, 00000003.00000002.467289457.0000000002BE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	fleW7NKwt9.exe, 00000003.00000002.467045157.0000000002B41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	fleW7NKwt9.exe, 00000000.00000002.432034031.00000000065E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: 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:	35.0.0 Citrine
Analysis ID:	652387
Start date and time: 26/06/202209:34:41	2022-06-26 09:34:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fleW7NKwt9.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/5@2/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 8.8% (good quality ratio 1.6%) • Quality average: 9.6% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 95% • 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, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, blob collector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Execution Graph export aborted for target fleW7NKwt9.exe, PID 1316 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory 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
09:36:14	API Interceptor	1x Sleep call for process: fleW7NKwt9.exe modified
09:36:37	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_fleW7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4\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):	1.0892268191931285
Encrypted:	false
SSDEEP:	192:9hdxxiHHBUZMXSaPbqwiPZ/u7sgS274lt1hV:Ldxx8BUZMXSaIPZ/u7sgX4lt1h
MD5:	3008CD39A6E428CBC8182E96BB8D61DA
SHA1:	72B8BEA106B60C14F15E408FC5C63605FF31C370
SHA-256:	153CD6C41C776F7EF9FB1BEDCEA5609BF15B008819F178F4BA1E1B7310DAF58A
SHA-512:	2C7EA0ED563468204752299137E79E969F0F286D11A82EE93D6361B050CCA6F53EE9DB55E617EBDA879D928776D00E1B246D7DA9218E4F77FC6F18B459806E4E
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.0.7.3.4.9.9.2.6.1.4.4.4.2.9.....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.=.1.3.3.0.0.7.3.4.9.9.6.6.1.4.4.3.1.2.....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.=.d.c.4.2.4.9.3.e.-.8.e.1.2.-.4.f.0.1.-.a.7.7.f.-.f.1.5.7.c.c.9.c.8.9.5.0.....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.=.3.2.5.b.5.8.0.c.-.2.e.f.f.-.4.7.c.1.-.a.7.1.c.-.9.7.b.2.0.a.4.7.2.5.5.8.....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.=.f.l.e.W.7.N.K.w.t.9...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.a.n.g.e.M.a.n.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.2.4.-.0.0.0.1.-.0.0.1.8.-.b.0.6.8.-.a.9.d.a.7.a.8.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.5.8.1.e.9.b.9.5.2.5.c.7.d.c.2.9.7.3.f.8.9.5.1.2.d.c.3.e.7.8.e.0.0.0.0.0.0.0.0.!.0.0.0.0.c.6.4.b.1.2.4.3.0.f.b.6.b.2.d.c.5.b.5.5.5.1.b.c.0.e.e.2.a.e.a.0.3.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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):	6310
Entropy (8bit):	3.7252179392238407
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMy67pYYE4x8SxCprW89bWJsfuym:RrlsNix6KYE42SGWifS
MD5:	60ED62A168EA97B1E685892E43E9B060
SHA1:	7F1D438937BD70B766F7AFCF48878FCD9F8EB6F6
SHA-256:	2FAEB348F061732352DD991CBC52DF2DBE00C4AC3F01CB77EFCCE946A9709175
SHA-512:	BDDAA542A1E276FFD78D7FB3EAA8B8EAEC9C1D64F9645661C55EF713E303BF9B80ACB6A99D14FC222C68D9F75961B45F821E8770DBAD2803059ECE488C22BF6F
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.>.1.3.1.6.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4637
Entropy (8bit):	4.478963845178849
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9l5Wgc8sqYjX8fm8M4JijFv+q8MWMUhBBrd:uITffKIgrsqY4Jk2MUhBxd
MD5:	3D3B3361CA85356FCE4A8478ED063D94
SHA1:	E38F977589DC40B06EBD66D593B958FB96716F56
SHA-256:	9705FD9CF7ACFCD3FC973A4796D64280696AD194739AAA0989CAF6D89E632FDD
SHA-512:	AD0F937E63ADA5DF7B780D58BB4D384FED49907986ED74A72B7C40C2F87CECF8E7ADE08D2F3AB122E17CEFEB0C5CB6F19C1AA54A65E857B9E14021623708C585
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="1576907" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Jun 26 16:36:34 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	265423
Entropy (8bit):	3.704350522574553
Encrypted:	false
SSDEEP:	3072:ZC9gIOgF5YqbA0KaF0g5UCgUU67iAsnJFoe0bjd+pnBAnAlwW:o9RpD/bA0PXTj5iXnP0kpnBU
MD5:	5447FC246EA9C53CE81DD32877ABDACA
SHA1:	7FE5EBE3A4AC71C6659E7EDB1DD6ACCBEE1A9DB6
SHA-256:	E424DF006EBC1B1D7C0B351E1AE1935A850A11F53D8987AD5FAA304EACD2E8C3
SHA-512:	A14166E3D023738CD069467C39F52C8ECBD259B4FA89F2469693E32B3631DA7B4BDE4B4C6E5826DF94705203223E58123274ABFD841E33AA6C00F26DF00A852
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....b.....D.....X.....<....#.....%...Q.....`.....8.....T.....<.....T#.....@%.....U.....B.....%.....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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fleW7NKwt9.exe.log

Process:	C:\Users\user\Desktop\fleW7NKwt9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9231620193463135
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:	fleW7NKwt9.exe
File size:	751616
MD5:	07edca391e6f402f748cb369540e7073
SHA1:	c64b12430fb6b2dc5b5551bc0ee2aea033aeae4f
SHA256:	d30687d6d06df3a60501b077b6dcfa82e3ba0c0efea48f17126e2607ce140a37
SHA512:	b2140eb59723b167954d3f652a3e28c0d73429c44b4966802bdcf43e55df61e554070dc54453993c977cd78ef43d12d59742b7557791ae15c463ded883d70773
SSDEEP:	12288:1sH2iN1kPRxliW11pyidNa+YPMjpwD1cJrl1ivBk542eIKFIe/u1KL:W13kPRrhbv6MyirlWm5eGa
TLSH:	CFF41286E3680DDDD1C357F51CACD1442A57F38A80ECC61AB9BA758EE5723E250A3D07
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..p..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b8fde
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62B71CEE [Sat Jun 25 14:34:22 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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]
dec eax
push edx

Instruction
dec eax
inc ecx
xor eax, 45373434h
cmp byte ptr [3534564Eh], dh
xor eax, 4F373751h
push esp
inc ecx
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb8f8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbc000	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	0xb6ffc	0xb7000	False	0.921841647455601	data	7.928642532152079	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xba000	0x3a0	0x400	False	0.376953125	data	2.9217575746193245	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xba058	0x344	data		

Imports

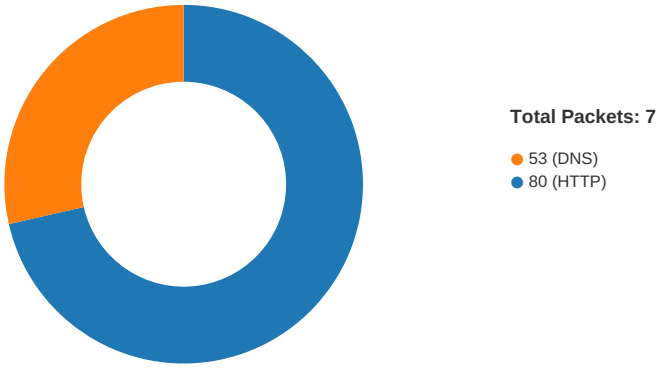
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6132.226.8.16949769802842536 06/26/22-09:36:21.815879	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49769	80	192.168.2.6	132.226.8.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:36:21.549525023 CEST	49769	80	192.168.2.6	132.226.8.169
Jun 26, 2022 09:36:21.814925909 CEST	80	49769	132.226.8.169	192.168.2.6
Jun 26, 2022 09:36:21.815366983 CEST	49769	80	192.168.2.6	132.226.8.169
Jun 26, 2022 09:36:21.815879107 CEST	49769	80	192.168.2.6	132.226.8.169
Jun 26, 2022 09:36:22.086443901 CEST	80	49769	132.226.8.169	192.168.2.6
Jun 26, 2022 09:36:25.083626986 CEST	80	49769	132.226.8.169	192.168.2.6
Jun 26, 2022 09:36:25.238773108 CEST	49769	80	192.168.2.6	132.226.8.169
Jun 26, 2022 09:36:40.110644102 CEST	49769	80	192.168.2.6	132.226.8.169

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:36:21.452459097 CEST	51748	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:36:21.472434998 CEST	53	51748	8.8.8.8	192.168.2.6
Jun 26, 2022 09:36:21.486792088 CEST	61116	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:36:21.505736113 CEST	53	61116	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:36:21.452459097 CEST	192.168.2.6	8.8.8.8	0xa9b8	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.486792088 CEST	192.168.2.6	8.8.8.8	0x8aab	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
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.472434998 CEST	8.8.8.8	192.168.2.6	0xa9b8	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:36:21.505736113 CEST	8.8.8.8	192.168.2.6	0x8aab	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

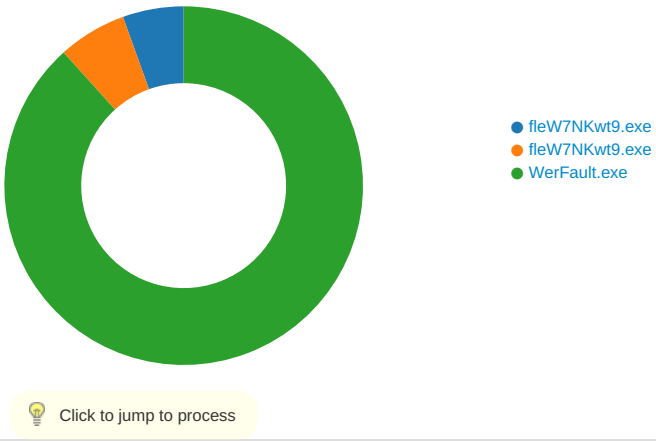
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49769	132.226.8.169	80	C:\Users\user\Desktop\fleW7NKwt9.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:36:21.815879107 CEST	1149	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
Jun 26, 2022 09:36:25.083626986 CEST	1150	IN	HTTP/1.1 504 Gateway Time-out Date: Sun, 26 Jun 2022 07:36:24 GMT Content-Type: text/html Content-Length: 557 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 35 30 34 20 47 61 74 65 77 61 79 20 54 69 6d 65 2d 6f 75 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 34 20 47 61 74 65 77 61 79 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>504 Gateway Time-out</title></head><body><center> 504 Gateway Time-out </center><hr><center></center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: fleW7NKwt9.exe PID: **6476**, Parent PID: **4876**

General

Target ID:	0
Start time:	09:35:53
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\fleW7NKwt9.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\fleW7NKwt9.exe"
Imagebase:	0xd0000
File size:	751616 bytes
MD5 hash:	07EDCA391E6F402F748CB369540E7073

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.428238748.0000000002451000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.430505969.00000000036B5000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.428503354.00000000024FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D9DCF06	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	6D9DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fleW7NKwt9.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DCEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fleW7NKwt9.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DCEC907	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	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile

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	6D9BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile

Analysis Process: fleW7NKwt9.exe PID: **1316**, Parent PID: **6476**

General

Target ID:	3
Start time:	09:36:15
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\fleW7NKwt9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\fleW7NKwt9.exe
Imagebase:	0x650000
File size:	751616 bytes
MD5 hash:	07EDCA391E6F402F748CB369540E7073
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: 00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.423560430.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.438756101.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000000.421990847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.421990847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.421990847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.421990847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000000.444529103.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.444529103.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.444529103.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.444529103.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000000.421362580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.421362580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.421362580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.421362580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000002.466292475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000002.466292475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.466292475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000002.466292475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000003.00000000.422724141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.422724141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.422724141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.422724141.0000000000402000.00000040.00000400.00020000.00000000.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	6D9DCF06	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	6D9DCF06	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	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D99D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D99D72F	unknown
C:\Users\user\Desktop\fleW7NKwt9.exe	unknown	4096	success or wait	1	6D99D72F	unknown
C:\Users\user\Desktop\fleW7NKwt9.exe	unknown	512	success or wait	1	6D99D72F	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **6644**, Parent PID: **1316**

General

Target ID:	10
Start time:	09:36:31
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1316 -s 1528
Imagebase:	0x1310000
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	6AE61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_flew7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_flew7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AE5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp.xml	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1C09.tmp.csv	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E2D.tmp.txt	success or wait	1	6AE5497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 12 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	9688	6	00 00 00 00 00 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.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 fd 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 24 05 00 00 fd fd fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00	UB%GenuineIntelWT$b0Pacific Standard TimePacific Daylight Time	success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	11628	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 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 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 fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 fd fd 00 05 00 00 00 00 00 00 00 00 05 00 00 00 08 fd 00 64 fd 00 22 fd fd 73 23 00 00 00 12 02 00 00 08 fd 00 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 fd fd fd	+S++d"s#+	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	1632	168	fd 04 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 73 00 00 00 00 05 00 00 00 00 00 00 00 34 15 13 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 00 00 00 00 00 00 00 00 50 72 fd 00 00 00 00 00 4c fd 00 00 00 00 00 01 00 00 00 00 00 00 00 1c fd 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 00 00 00 00 00 fd 76 fd 6d 00 00 00 00 fd 72 fd 00 00 00 00 00 fd 58 fd 00 00 00 00 00 fd 02 00 00 6c 2d 00 00	RCC"s4mPrLvmrXl-	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	20936	20	5b 02 00 00 6c 11 fd 00 00 00 00 00 08 00 00 00 7c 77 00 00	[l|w	success or wait	603	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	30588	8	fd 56 fd 02 fd 56 fd 02	VV	success or wait	602	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	240861	4	18 fd 04 01		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	1800	4	0c 00 00 00		success or wait	12	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	12344	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 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 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 fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 20 af 00 fd fd 2f 77 23 00 00 00 16 02 00 00 fd 2f 00 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 fd fd fd fd fd	?+S++ /w#+	success or wait	12	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	2332	48	3c 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 64 fd fd 05 00 00 00 00 fd 0c 00 00 6d fd 02 00 fd 02 00 00 fd 4e 00 00	< @dmN	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	2392	4	3d 00 00 00	=	success or wait	61	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	9694	34	1c 00 00 00 66 00 6c 00 65 00 57 00 37 00 4e 00 4b 00 77 00 74 00 39 00 2e 00 65 00 78 00 65 00 00 00	fleW7NKwt9.exe	success or wait	61	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	8876	120	00 00 fd 6a 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a fd 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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	j`Z,?)@A	success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	11538	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6OnDemandConnRouteHelper.dll	success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	9020	668	00 00 fd 72 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 4e 2d 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 50 fd 02 00 00 00 00 00 60 01 03 00 00 00 00 fd 4d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 5a 07 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 06 51 05 00 00 00 00 00 16 1e 31 7c 00 00 00 00 fd 5f fd 21 00 00 00 00 58 7d 3c 21 00 00 00 00 0d 6b 43 01 00 00 00 00 fd 37 01 00 2b 16 01 00 7d fd 06 00 fd fd 0a 00 5a 07 05 00 06 7f 15 00 06 51 05 00 fd 52 00 43 fd 01 00 77 14 1c 00 00 00 00 00 3b 58 39 00 fd fd 04	r*,N-ZbP`MZ@Q1|_!X}<!kC7+}ZQRCw;X9	success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	240865	24558	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4.tmp.dmp	32	120	03 00 00 00 44 02 00 00 08 07 00 00 04 00 00 00 fd 19 00 00 58 09 00 00 0e 00 00 00 3c 00 00 00 18 23 00 00 05 00 00 00 fd 25 00 00 fd 51 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 3c 00 00 fd fd 03 00 15 00 00 00 fd 01 00 00 54 23 00 00 16 00 00 00 fd 00 00 00 40 25 00 00	DX<#%Q`8T<T#@%	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1316</Pid>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 6c 00 65 00 57 00 37 00 4e 00 4b 00 77 00 74 00 39 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>fleW7NKwt9.exe</ImageName>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 37 00 31 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19710</Uptime>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1234	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1324	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1384	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1438	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 30 00 33 00 37 00 30 00 32 00 32 00 37 00 32 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>203702272</PeakVirtualSize>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1536	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 33 00 36 00 39 00 34 00 30 00 38 00 30 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>203694080</VirtualSize>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 38 00 30 00 30 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>7801</PageFaultCount>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 37 00 30 00 32 00 31 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>27021312</PeakWorkingSetSize>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 37 00 30 00 32 00 31 00 33 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>27021312</WorkingSetSize>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	1902	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 31 00 33 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>313408</QuotaPeakPagedPoolUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2026	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 34 00 30 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>313408</QuotaPagedPoolUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2134	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 36 00 31 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>61152</QuotaPeakNonPagedPoolUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2268	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 30 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>60800</QuotaNonPagedPoolUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2386	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 33 00 37 00 30 00 35 00 32 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>13705216</PagefileUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2464	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2468	2	09 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2474	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 33 00 37 00 31 00 33 00 34 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>13713408</PeakPagefileUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2568	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2572	2	09 00		success or wait	3	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2578	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 33 00 37 00 30 00 35 00 32 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>13705216</PrivateUsage>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2652	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2656	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2660	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2706	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2710	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2712	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2754	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2758	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2760	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2806	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2868	4	0d 00 0a 00		success or wait	8	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2872	2	09 00		success or wait	16	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	2876	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 6c 00 65 00 57 00 37 00 4e 00 4b 00 77 00 74 00 39 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>fleW7NKwt9.exe</Parameter0>	success or wait	8	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3496	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3536	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3540	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3542	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3580	4	0d 00 0a 00		success or wait	6	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3584	2	09 00		success or wait	12	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	3588	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4148	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4188	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4192	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4194	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4240	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4334	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4338	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4342	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 71 00 70 00 62 00 6e 00 65 00 6c 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>qpbnel, Inc.</SystemManufacturer>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4448	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4452	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4456	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 71 00 70 00 62 00 6e 00 65 00 6c 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>qpbnel7,1</SystemProductName>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4560	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4680	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4684	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4688	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 39 00 30 00 38 00 39 00 32 00 33 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1599089232</OSInstallDate>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	2	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4778	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4880	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4884	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4888	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4956	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4960	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	4962	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5002	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5006	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5008	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5042	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5046	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5050	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5146	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5150	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5152	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	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5188	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5192	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5194	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5218	4	0d 00 0a 00		success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5222	2	09 00		success or wait	6	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5226	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5490	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5522	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 36 00 2d 00 32 00 36 00 54 00 31 00 36 00 3a 00 33 00 36 00 3a 00 33 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-06-26T16:36:35Z">	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5622	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5626	2	09 00		success or wait	2	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5630	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 33 00 31 00 36 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 38 00 39 00 35 00 33 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 38 00 39 00 35 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="411" PID="1316" UptimeMS="8953" TimeSinceCreationMS="8953" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5892	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5896	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5900	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5920	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5924	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5926	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5964	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5968	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	5970	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6008	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6012	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6016	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 63 00 34 00 32 00 34 00 39 00 33 00 65 00 2d 00 38 00 65 00 31 00 32 00 2d 00 34 00 66 00 30 00 31 00 2d 00 61 00 37 00 37 00 66 00 2d 00 66 00 31 00 35 00 37 00 63 00 63 00 39 00 63 00 38 00 39 00 35 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>dc42493e-8e12-4f01-a77f-f157cc9c8950</Guid>	success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6114	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6118	2	09 00		success or wait	2	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6122	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 36 00 2d 00 32 00 36 00 54 00 31 00 36 00 3a 00 33 00 36 00 3a 00 33 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-06-26T16:36 :35Z</CreationTime>	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6226	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19F7.tmp.WERInternalMetadata.xml	6270	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	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B31.tmp.xml	0	4637	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_fleW7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4\Report.wer	0	2	fd fd		success or wait	1	6AE5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_fleW7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4\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	6AE5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_flew7NKwt9.exe_22b6db12ffaf2d73473ec2207b1b61d0d71c9b_42e88d20_19a524b4\Report.wer	14076	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 38 00 30 00 34 00 33 00 35 00 30 00 34 00 37 00 38 00	MetadataHash=-1804350478	success or wait	1	6AE5497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	success or wait	1	6AE736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6AE71FB2	RegCreateKeyExW
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AE543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	ProgramId	unicode	00066581e9b9525c7dc2973f89512dc3e78e00000000	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	FileId	unicode	0000c64b12430fb6b2dc5b5551bc0ee2aea033aeae4f	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	LowerCaseLongPath	unicode	c:\users\user\desktop\flew7nkwt9.exe	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	LongPathHash	unicode	flew7nkwt9.exe\57b5df95	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	Name	unicode	flew7nkwt9.exe	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	Publisher	unicode		success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	Version	unicode	1.0.0.0	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	BinFileVersion	unicode	1.0.0.0	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	BinaryType	unicode	pe32_clr_32	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	ProductName	unicode	homework interface	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	ProductVersion	unicode	1.0.0.0	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	LinkDate	unicode	06/25/2022 14:34:22	success or wait	1	6AE736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	BinProductVersion	unicode	1.0.0.0	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	Size	B	00 78 0B 00 00 00 00 00	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	Language	dword	0	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	IsPeFile	dword	1	success or wait	1	6AE736BF	unknown
\REGISTRY\A\{cf31a1b0-8150-3cfa-89f7-ac200f3746d3}\Root\InventoryApplicationFile\flew7nkwt9.exe\57b5df95	IsOsComponent	dword	0	success or wait	1	6AE736BF	unknown
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 C7 73 05 00 00 00 34 15 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 84 6D 00 00 00 00 50 72 E7 00 4C E9 AF 00 01 00 00 00 1C E9 AF 00 D8 E8 AF 00 D0 E8 AF 00 F4 76 85 6D 98 72 E8 00 90 58 CB 00	success or wait	1	6AE71FE8	RegSetValueExW

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

Disassembly

No disassembly