



ID: 756343
Sample Name:
PrWP76ejHO.exe
Cookbook: default.jbs
Time: 02:20:08
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PrWP76ejHO.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
System Summary 6
Persistence and Installation Behavior 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer 13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\Report.wer 13
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp 13
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp.xml 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.xml 15
C:\Users\user\AppData\Local\Temp\1x6VE38oK 15
C:\Users\user\AppData\Local\Temp\iscan.exe 16
C:\Users\user\AppData\Local\Temp\mmbedbm.jl 16
C:\Users\user\AppData\Local\Temp\nsx4EFE.tmp 16
C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c 17
C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe 17
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Rich Headers 19
Data Directories 19
Sections 19

Resources 20
Imports 20
Possible Origin 20
Network Behavior 20
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 23
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: PrWP76ejHO.exePID: 1832, Parent PID: 3452 24
General 24
File Activities 24
Analysis Process: iscan.exePID: 1764, Parent PID: 1832 24
General 24
File Activities 25
File Created 25
File Written 25
File Read 25
Registry Activities 25
Analysis Process: conhost.exePID: 5268, Parent PID: 1764 25
General 25
Analysis Process: iscan.exePID: 5188, Parent PID: 1764 26
General 26
File Activities 26
File Read 26
Analysis Process: explorer.exePID: 3452, Parent PID: 5188 26
General 26
File Activities 27
Registry Activities 27
Analysis Process: iijhlev.exePID: 4468, Parent PID: 3452 27
General 27
File Activities 27
File Read 27
Analysis Process: conhost.exePID: 1836, Parent PID: 4468 27
General 28
Analysis Process: WerFault.exePID: 5096, Parent PID: 4468 28
General 28
File Activities 28
File Created 28
File Deleted 29
File Written 29
Registry Activities 51
Analysis Process: iijhlev.exePID: 4864, Parent PID: 3452 51
General 51
File Activities 51
File Read 51
Analysis Process: conhost.exePID: 5872, Parent PID: 4864 51
General 51
Analysis Process: WerFault.exePID: 2436, Parent PID: 4864 52
General 52
File Activities 52
File Created 52
File Deleted 52
File Written 53
Registry Activities 74
Analysis Process: ipconfig.exePID: 1916, Parent PID: 3452 74
General 74
File Activities 75
File Deleted 75
File Read 75
Registry Activities 75
Disassembly 75

Copyright Joe Security LLC 2022

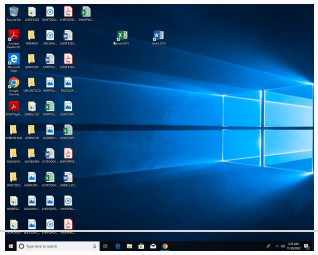
Windows Analysis Report

PrWP76ejHO.exe

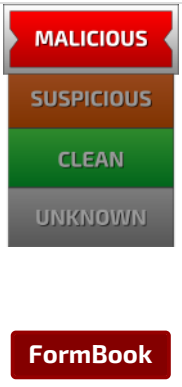
Overview

General Information

Sample Name:	PrWP76ejHO.exe
Analysis ID:	756343
MD5:	db102a67350060.
SHA1:	a3131a3df17a15..
SHA256:	98420cf47e1957..
Tags:	32 exe Formbook trojan
Infos:	



Detection



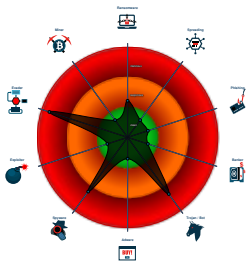
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Found evasive API chain (may stop…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- PrWP76ejHO.exe (PID: 1832 cmdline: C:\Users\user\Desktop\PrWP76ejHO.exe MD5: DB102A67350060A1E967AEF81118F18D)
  - iscan.exe (PID: 1764 cmdline: "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c MD5: 2B4B3369E04DEDD66517641DB0F5A8AB)
    - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - iscan.exe (PID: 5188 cmdline: "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c MD5: 2B4B3369E04DEDD66517641DB0F5A8AB)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - iijhlev.exe (PID: 4468 cmdline: "C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe" "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca MD5: 2B4B3369E04DEDD66517641DB0F5A8AB)
          - conhost.exe (PID: 1836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - WerFault.exe (PID: 5096 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4468 -s 452 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - iijhlev.exe (PID: 4864 cmdline: "C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe" "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca MD5: 2B4B3369E04DEDD66517641DB0F5A8AB)
          - conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - WerFault.exe (PID: 2436 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4864 -s 420 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - ipconfig.exe (PID: 1916 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fedefarmatour.online/dwdp/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x7d38:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x209e7:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xc0c6:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1960e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1940c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18eb8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1950e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x19686:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xbc91:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18103:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1f62e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20751:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1b910:$sqlite3step: 68 34 1C 7B E1 • 0x1c488:$sqlite3step: 68 34 1C 7B E1 • 0x1b952:$sqlite3text: 68 38 2A 90 C5 • 0x1c4cd:$sqlite3text: 68 38 2A 90 C5 • 0x1b969:$sqlite3blob: 68 53 D8 7F 8C • 0x1c4e3:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.359082875.0000000000590000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 25 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.iscan.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.iscan.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6f38:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1fbe7:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xb2c6:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1880e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.iscan.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1860c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x180b8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1870e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x18886:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xae91:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17303:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1e82e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1f951:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.iscan.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1ab10:$sqlite3step: 68 34 1C 7B E1 • 0x1b688:$sqlite3step: 68 34 1C 7B E1 • 0x1ab52:$sqlite3text: 68 38 2A 90 C5 • 0x1b6cd:$sqlite3text: 68 38 2A 90 C5 • 0x1ab69:$sqlite3blob: 68 53 D8 7F 8C • 0x1b6e3:$sqlite3blob: 68 53 D8 7F 8C
3.2.iscan.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking



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

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected FormBook

System Summary



Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior



Uses ipconfig to lookup or modify the Windows network settings

Malware Analysis System Evasion



Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion



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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information



Yara detected FormBook

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

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

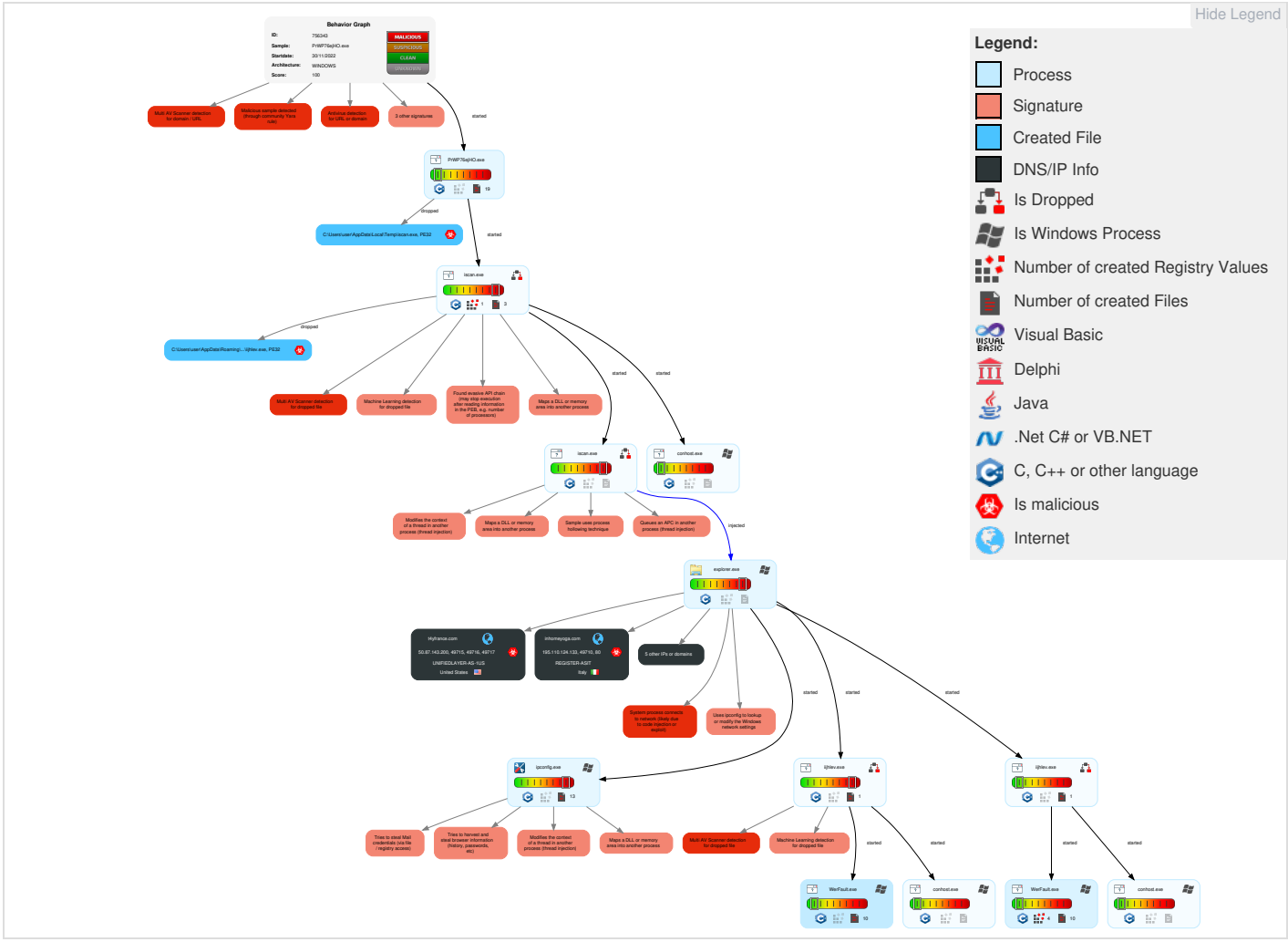
Yara detected FormBook

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	1 Registry Run Keys / Startup Folder	5 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	2 1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Masquerading	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 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 Virtualization/Sandbox Evasion	NTDS	1 4 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	5 1 2 Process Injection	LSA Secrets	1 Virtualization/Sandbox Evasion	SSH	2 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 Process 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	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

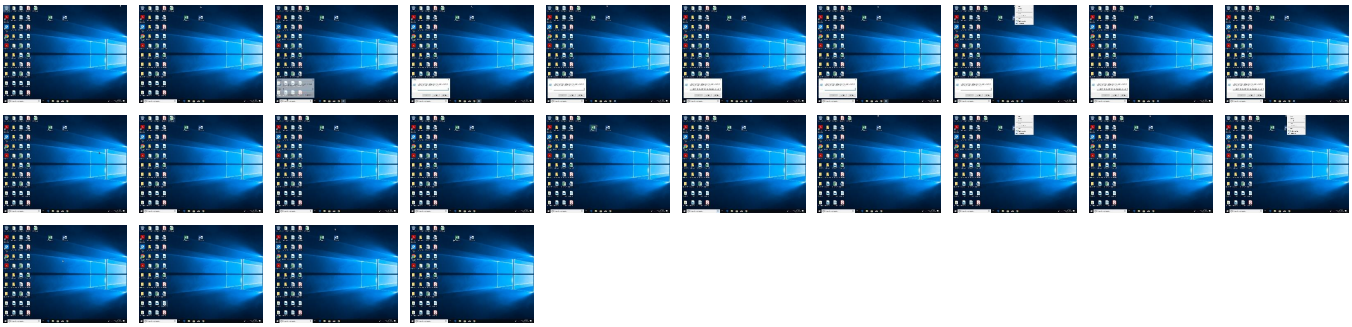
Copyright Joe Security LLC 2022



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
PrWP76ejHO.exe	73%	ReversingLabs	Win32.Trojan.FormBook	
PrWP76ejHO.exe	32%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\iscan.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\iscan.exe	27%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe	27%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.iscan.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.PrWP76ejHO.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
3.2.iscan.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.PrWP76ejHO.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.iscan.exe.8d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
inhomeyoga.com	11%	Virustotal		Browse
t4yfrance.com	9%	Virustotal		Browse
fedefarmatour.online	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.fedefarmatour.online/dwdp/	100%	Avira URL Cloud	malware	
http://www.t4yfrance.com/dwdp/	100%	Avira URL Cloud	malware	
http://www.a8-group.com/dwdp/	100%	Avira URL Cloud	malware	
http://www.fedefarmatour.online/dwdp/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
inhomeyoga.com	195.110.124.133	true	true	• 11%, Virustotal, Browse	unknown
t4yfrance.com	50.87.143.200	true	true	• 9%, Virustotal, Browse	unknown
www.a8-group.com	194.58.112.174	true	true		unknown
fedefarmatour.online	81.88.48.71	true	true	• 14%, Virustotal, Browse	unknown
www.fedefarmatour.online	unknown	unknown	true		unknown
www.t4yfrance.com	unknown	unknown	true		unknown
www.inhomeyoga.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fedefarmatour.online/dwdp/	true	• Avira URL Cloud: malware	unknown
http://www.t4yfrance.com/dwdp/	true	• Avira URL Cloud: malware	unknown
www.fedefarmatour.online/dwdp/	true	• Avira URL Cloud: malware	low
http://www.a8-group.com/dwdp/	true	• Avira URL Cloud: malware	unknown

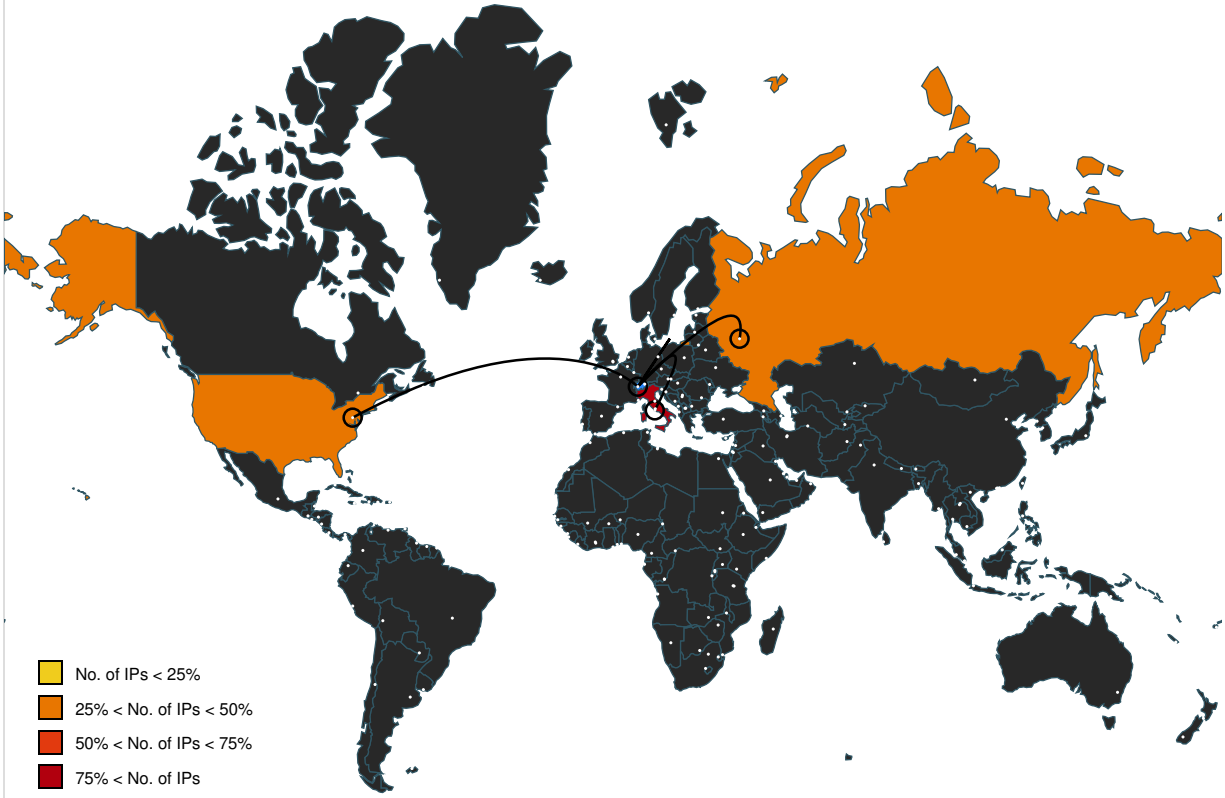
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	1x6VE38oK.22.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high
http://https://duckduckgo.com/chrome_newtab	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high
http://https://duckduckgo.com/ac/?q=	1x6VE38oK.22.dr	false		high
http://nsis.sf.net/NSIS_Error	PrWP76ejHO.exe	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	1x6VE38oK.22.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	PrWP76ejHO.exe	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	1x6VE38oK.22.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	ipconfig.exe, 00000016.00000003.42603576 8.0000000006F71000.00000004.00000800.000 20000.00000000.sdmp, 1x6VE38oK.22.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.110.124.133	inhomeyoga.com	Italy		39729	REGISTER-ASIT	true
50.87.143.200	t4yfrance.com	United States		46606	UNIFIEDLAYER-AS-1US	true
194.58.112.174	www.a8-group.com	Russian Federation		197695	AS-REGRU	true
81.88.48.71	fedefarmatour.online	Italy		39729	REGISTER-ASIT	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756343
Start date and time:	2022-11-30 02:20:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PrWP76ejHO.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211

Copyright Joe Security LLC 2022

Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@14/14@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73.7% (good quality ratio 68%) • Quality average: 75.2% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 20.42.73.29
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:21:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run oipsxnj C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca
02:21:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run oipsxnj C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca
02:21:30	API Interceptor	2x 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_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8041050886194944
Encrypted:	false
SSDEEP:	192:TAudawvDwZHBUZMX/g3jR9T/u7s3S274ltDdB:DdawvDwJBUZMX/g3jv/u7s3X4ltDdB
MD5:	D3E58825370A9CACD63AA4E4D610D741
SHA1:	F7A585CCB546E6A648498538B0605EC204FBC0EE
SHA-256:	1651821B53A4F9DD251C1953C1B72AE0B4011ACEAA488539FF2BD106CFE0394A
SHA-512:	4C47F499D4DBADF7049BFDB92E98D28F5AC21AB5642AE97A7BDD970E62ADDD10CBB1F0912516FE228DAB5C2919AD3ED84F365EFE44EDC8CD4C96FF4746AC C3A5
Malicious:	false
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.=.1.3.3.1.4.2.7.7.2.8.3.6.6.0.3.4.4.0.....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.=.1.3.3.1.4.2.7.7.2.8.4.7.0.6.9.0.0.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.b.e.4.3.d.1.d.-.a.0.0.a.-.4.9.2.c.-.8.0.4.3.-.0.c.f.a.d.e.7.3.8.9.0.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.f.5.4.c.f.b.-.c.9.a.e.-.4.9.7.d.-.a.9.f.e.-.3.d.a.6.2.5.3.c.3.4.9.5.....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.=.i.i.j.h.l.e.v...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.0.0.-.0.0.0.1.-.0.0.1.f.-.7.e.3.f.-.0.1.7.e.a.5.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.c.0.1.a.e.c.9.d.6.e.6.9.2.4.d.f.0.0.f.a.0.b.5.8.5.4.e.1.e.d.4.0.0.0.0.f.f.f.f.!.0.0.0.0.a.5.e.4.8.2.5.9.7.f.6.f.2.d.6.8.2.5.0.a.4.e.b.2.8.9.1.1.6.8.3.e.5.0.f.a.c.4.d.e.!.i.i.j.h.l.e.v...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8114076405556345
Encrypted:	false
SSDEEP:	192:dy7awvTwZHBUZMX/g3jBR//u7s3S274ltDdBf:M7awvTwJBUZMX/g3j//u7s3X4ltDdB
MD5:	881007555D6141EE38396F9FA7BF3A14
SHA1:	CDC7784DF7C4DD49A3EF5ABB10B752D256B78EB6
SHA-256:	D7B254489920F804CF2FD39544563BE82347DADDA6984681709E507ED9724D4C
SHA-512:	1BB3A11587A8959C82FC524F7050ADA653B4E01D96D1F2918DE8E00304AD8B1FCD0CAD359526C0B839E4B65340EF861DC84AB0A385B44A81745F8454EE74E11E
Malicious:	false
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.=.1.3.3.1.4.2.7.7.2.8.0.1.9.7.3.1.5.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.4.2.7.7.2.8.2.0.5.6.6.7.6.9.....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.=.1.4.0.3.a.b.f.4.-.2.7.f.6.-.4.3.9.a.-.9.b.7.b.-.4.a.5.8.e.e.9.c.f.d.6.7.....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.=.6.4.3.1.b.8.7.4.-.7.1.a.3.-.4.2.d.b.-.b.b.f.3.-.d.d.8.0.2.a.4.0.6.b.b.2.....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.=.i.i.j.h.l.e.v...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.7.4.-.0.0.0.1.-.0.0.1.f.-.f.b.7.7.-.0.a.7.9.a.5.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.c.0.1.a.e.c.9.d.6.e.6.9.2.4.d.f.0.0.f.a.0.b.5.8.5.4.e.1.e.d.4.0.0.0.0.f.f.f.f.!.0.0.0.0.a.5.e.4.8.2.5.9.7.f.6.f.2.d.6.8.2.5.0.a.4.e.b.2.8.9.1.1.6.8.3.e.5.0.f.a.c.4.d.e.!.i.i.j.h.l.e.v...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 30 10:21:21 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36978
Entropy (8bit):	2.094980958939099
Encrypted:	false
SSDEEP:	192:cPS9WAJmJotO9UHWmUcGk7XPzEJWjSi0XDS6FbzcZc:lTqmmg9UpGyh+XP

MD5:	2D96E5A0275FABD6DC46BA6A86F9ABE5
SHA1:	3837483602ED6BBC97307DC18ECE9169540EBBE2
SHA-256:	4C42A3E21ADFDCB82EAC0FFEDB79FBFA7E8BD9BFF72A9311FE18485FB3A0DDC1
SHA-512:	B8ADC0B9C406098E590A0BBECCC7AD109436C99955D00E6D56E1DF0A6DB8E401B88F25039E83A3276780CB46A65697350CFDF4357F5C23382F0322F10DFAA8E8
Malicious:	false
Preview:	MDMP..... .....c.....@$.....T.....8.....T.....0...B~.....p.....\.....U.....B.....GenuineIntelW.....T.....t.....c..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8324
Entropy (8bit):	3.7043995876261486
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivC56P+aghd6YqhYSUEPcugmfAqgS+2CprV89bxsGsfBzKm:RrlsNiv862aghd6Y8YSUEkugmfAqgSFU
MD5:	FBDCA69F879137AF87609249DF723473
SHA1:	2B2A5976AE858D96B32364F6BB0354CA49ACB58C
SHA-256:	33F7BC8B7ECA2FF10E04ED46836350C0A1B74F9C45B9DB61816591B5977B1237
SHA-512:	81DDE1A21D59565FCA15830D437559C5327D39824573B8573FEC6A7A92414E414F23AEDDCC12D929C0BFF5D16088E6EDBC57A2FCB018ACBD432BA8ADF88140781
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.4.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4588
Entropy (8bit):	4.480173772723793
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtWI9JVWgc8sqYjs8fm8M4J62ZFtE+q8+mjB++Od:uITf4OkgrsqY9JRxEsjc+Od
MD5:	4980E483DD65840DE2CF11A7BB98A8E9
SHA1:	0305346ED6363F22F7000210E8884CDDD94629D8
SHA-256:	21DA4C57570B00D154DD236761AC94C1E7D347BCAD358645CAE3DBDF3A77122D
SHA-512:	E58D71FC52CDFEFF1F50E1D2CBCA149C1093670229330B2F5DB88943D4922A2F096CDDE37B261DA3D5CBA8B7EE4ABE559B2311884351BA27ED576F97BBB916BC
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1802612" />.. <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\WERAB95.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 30 10:21:24 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36510
Entropy (8bit):	2.0994747264122124
Encrypted:	false
SSDEEP:	192:Z5bhE6b5VtOGJNqajSWW6kekyPPzU+sFezyJSbH03F:bhE6bngGnjEe9wFeo
MD5:	262A2F0165598CB8C1F089568D15DAC8
SHA1:	84BAB5E35242AA585E97DAFC3EFAE51723E8546A

SHA-256:	F279E69F1224E8C691922D0B2D94300A1C600BFA8C19CCBF04B9C772CC774CFE
SHA-512:	667B3C1CB3B06A470B77FC668C289DEF5A079FF050A3E99720280B07F04D852D6920AFC9B93B22D99F72DDBC7FE9A0CF1ADE7E36E2D812E11974303816F06F4
Malicious:	false
Preview:	MDMP..... .....c.....h.....#.....T.....8.....T.....}.....U.....B.....GenuineIntelW.....T.....c..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8332
Entropy (8bit):	3.702271813703967
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiPC36NMCIgRj6YqhdSUmncugmfAqgS+2CprG89bxRcsfmzBm:RrlsNiPi6NMCIkj6Y8dSUmcugmfAqgSQ
MD5:	99775E557955AA9043F52F99B06CBFF8
SHA1:	8EB88504C9A5828A9E6E48A7B4A2AFF8289E9F55
SHA-256:	C05FE079520B71127C0B907EB55C0B959D6E915B6183DC51E5561D91E03E4144
SHA-512:	D4A198D5F33EDDF54BBBC10C9FD12855EA394A6DB3A37614CD64638D52AE8028FF20C6046902F56BA5D34B9A3CAA1F32A952CFAA8789F738587639A790F92E61
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.8.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4588
Entropy (8bit):	4.478340495331477
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtWI9JVWgc8sqYjz8fm8M4J62ZFxQ+q8+mDB+++d:uITf4OkgrsqYMJRtQsDc++d
MD5:	8C38EA0ACD36EC05355658D475637FF4
SHA1:	3485C2B4747A68A67A90331589B86F03B5E20CD5
SHA-256:	02F2D88DC261B7B05CF0DA2D91CD419B5FB6F8AF54D5B8B5CA8ED1B58879F860
SHA-512:	EB4818785BD72214D2EA8AED23E561A884492F3479AF713A9C4266A3B6E38CC225F8B47B6348249FF43876C1990BBFC113265FF37F25CA0123577F73B9E23B2F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1802612" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\1x6VE38oK

Process:	C:\Windows\SysWOW64\ipconfig.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false

Preview:	SQLite format 3.....@ .....-.....=.....[5.....*.....

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

Process:	C:\Users\user\Desktop\PrWP76ejHO.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	125440
Entropy (8bit):	6.283809308716995
Encrypted:	false
SSDEEP:	3072:6sqyHK7EF9cU5FO/hcf9hUnBZFXBultTL6OhiF:BHK7o9W5uhSFXEY
MD5:	2B4B3369E04DEDD66517641DB0F5A8AB
SHA1:	A5E482597F6F2D68250A4EB28911683E50FAC4DE
SHA-256:	A4C4BF78E737CCADBABF71B57E5676A846D9ADFC5442344EDA8267325223B964
SHA-512:	67EB46AB147AD92DB741B60F851A78B6BF88F2DA93601542EE67D4FAAD448CECA73938207F5DAEB0153D5D2C1C84A64949CD7856F404C0781C4E96337273540C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\.....2.....2.....2.....v..*.....*.t...*.....Rich .....PE..L....h.c.....f.....9.....@.....@.....0..... .....@...@..... .....text....e.....f..... ..`.rdata...k.....l..j.....@..@.data...(+.....@....gfids..... .....@..@.rsrc.....0.....@..@..... .....

C:\Users\user\AppData\Local\Temp\mmbedbm.jl

Process:	C:\Users\user\Desktop\PrWP76ejHO.exe
File Type:	data
Category:	dropped
Size (bytes):	189952
Entropy (8bit):	**7.998520046706668**
Encrypted:	**true**
SSDEEP:	3072:lfffffffffffff01MFDR7elXwjs6LDZf5X2a2GdUbA1CRe7vDlJGc4U9WKoCaAdY:lfffffffffffff3JexZcZV2a2GdPokvx
MD5:	AE2C848F5A91F0EEFBCFAECB3660089D
SHA1:	A280F4205AABBCADC444FD983207E41A5871784E
SHA-256:	72B7C4D8E791EA9A4A34BA3626C1FF4BE294988650E960C7F7ED18CA90847098
SHA-512:	66B79443D897DAB52B4D5FF19D790FDCA1C2A070B481C201265988B490770747B83F3888CBC5B2A07ECA8CA1B90008DC33F615126B3F73E419D2484B9B48719
Malicious:	false
Preview:	._ 5b...[...u....)#.gt..I...M....v.5~aR.A.&n...f..:.]....h9/'.n.^Y.fF.&..L?NZ..... ....P.....YD..ew..%f.....kU..n~..n.....y.e..q.Q/.<...a>..s.....[.0...3.].....S..d..,.,5.(m.O.pn=.x...%. .U.:.+`..rs.....W.....{.L.1+...M-..6.p....<.R.V#...@#...P.....5.aR.A.&n..f..:.]....h9.'.n._.wf%.....%X8.....2J-.ve6..p..r..H..{...Y.*.Q...!fZG..n~..n.P.....%.....O.sg~06.PA.q#.. ..d.g....U..E.O.....S.&s..,.,.D.m...pq..Z.v..%....tj..T..rs.....WL...j..{.k.%+...M-..6.p...[<.R.V#....#.].P.....v.5~aR.A.&n...f..:.]....h9.'.n._.wf%.....%X8.....2J-.ve6..p..r..H..{.. .Y.*.Q...!fZG..n~..n.P.....%.....O.sg~06.PA.q#....d.g....U..E.O.....S..d..,.,.E(m.q.pq@.Z...%....tj.+T..rs.....WL...j..{.k.%+...M-..6.p...[<.R.V#....#.].P.....v.5~aR.A.&n...f..:.]. ...h9.'.n._.wf%.....%X8.....2J-.ve6..p..r..H..{...Y.*.Q...!fZG..n~..n.P.....%.....O.sg~06.PA.q#....d.g....U..E.O.....S..d..,.,.E(m.q.pq@.Z...%....tj.+T..rs.....

C:\Users\user\AppData\Local\Temp\nsx4EFE.tmp

Process:	C:\Users\user\Desktop\PrWP76ejHO.exe
File Type:	data
Category:	dropped
Size (bytes):	330372
Entropy (8bit):	7.553183899203401
Encrypted:	false
SSDEEP:	6144:MMiffffffffffff3JexZcZV2a2GdPokvDlJGc4U9HV6Epw5Da3iffuHK7o9W5ui:Mfffffffffffff3YxZa4qokrIlc4Woy
MD5:	5D51FD4B6E844AE16602B13E24A93BF8
SHA1:	9F071B7B261C17DA0862C4029EB9530A9912EFB1
SHA-256:	501989AB0623183D2CA2B4E4BCFC74B8C865A03E55899889B92E7D81957B25E0
SHA-512:	6E0279EEADB8E9604FA944A5EB5D4E673F0667E79983C451E0A00B403D28062AA4F2AA60773269DFC3A23AC62F6927743565907A1D8CD33994CB267371F1DF5E
Malicious:	false
Preview:	.....,.....^...$..... .....J.....j.....$..... .....

C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c	
Process:	C:\Users\user\Desktop\PrWP76ejHO.exe
File Type:	data
Category:	dropped
Size (bytes):	8152
Entropy (8bit):	6.20728143173311
Encrypted:	false
SSDEEP:	192:tEnLkq8ChRVmucs9kMZk1thk1XRKjR5SeOyrkIBrzG6iyw:4LkqfRVLSMZkVQXWsbUKn
MD5:	64C3C26CE45E8C154D7CA9FEBB385997
SHA1:	D606B7D8CD6E3046992ED26D869E47AFD2A390AE
SHA-256:	A2F81AB67DA82F261E6979CAF0DF1E366499015C6ABABBD1A020601D4FB58185
SHA-512:	7A61FAC51B7ABD0D20D7EF06161BD417D120181E67E3CEF891BB6D149B0BA656B0F9229CCE9ED77B00B9CE37A9FB871B355EFF925D904FB4DDE26288370E3AB3
Malicious:	false
Preview:	3<.$$..$$$..(..(.$.$..,y.H..$$$...(..(.E..<...*;$$.d.....E.1.d19.....z0$.H..<b..$$.1..Rk\{[5..\|9M9k.^.z...3...z0$.H...$$$..(..(.$.$...,X6..\.$$$.d.+..8...TEl.d..8Sy.dSy.H..<.4.d....(.j.&.....T.(.....-;.G...z($.H.....<.F.....9u.....9e...9=..,9M..8..L..<.d...0.9u.\.....(.*..8...<.U.d...Sz<$..L..0..0.9u11.H.....$$$..(..(.$.$.,...f..\.....<.l.L.i..(.4.i.4...8$..i.d....(.u..(.. ...z...l..].d...L.z...R..]....L.....T..N.y..T..e....<...8.u:...<.8..L.l..(.o.d19.d..Sz<$.H..<b..$$.1..Rk\{[5..:.\|9M9k...z...U...z0$.H.H.....h.A.....N....j...`...f....l...B.....X.d..L..T..>..D..Z\.....L..f..\.....5.x...h..T.\.....V..4\....._...8\.....?.....4\&.....LU...H\<....!K[...\\"....@f...@\H.....(..P.f.L;...$$$..$$$.9.5.$$$...<..8.4.....4.L.....0.$.$$.M{[:....H..<.d....L.....\.d.....@..$$$.;.5.$$$...(..8.4..L....<...P.d.9.A....@.y1:.d...Sz<$.H.H(.$$.....

C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe	
Process:	C:\Users\user\AppData\Local\Temp\iscan.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	125440
Entropy (8bit):	6.283809308716995
Encrypted:	false
SSDEEP:	3072:6sqyHK7EF9cU5FO/hcf9hUnBZFXBultTL6OhiF:BHK7o9W5uhSFXEY
MD5:	2B4B3369E04DEDD66517641DB0F5A8AB
SHA1:	A5E482597F6F2D68250A4EB28911683E50FAC4DE
SHA-256:	A4C4BF78E737CCADBABF71B57E5676A846D9ADFC5442344EDA8267325223B964
SHA-512:	67EB46AB147AD92DB741B60F851A78B6BF88F2DA93601542EE67D4FAAD448CECA73938207F5DAEB0153D5D2C1C84A64949CD7856F404C0781C4E9633727354CC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\.....2.....2.....2.....v..*.....*.t...*.....Rich.....PE..L....h.c.....f.....9.....@.....@.....0..... .....@...@.....text....e.....f..... ..`.rdata...k.....l...j.....@..@.data...(+.....@....gfids..... .....@..@.rsrc.....0.....@..@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.686417648025134
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PrWP76ejHO.exe
File size:	318559
MD5:	db102a67350060a1e967aef81118f18d
SHA1:	a3131a3df17a154e41c09973ca8a9aabac29929e
SHA256:	98420cf47e19574739cff3f1f74bd3c6c70e103d0b28040b64fd3c77588c7ee7
SHA512:	daad205a305f7774164f0ed2298501e8a4cade236b93f63db31e40713a66a379145a2e9ca861f8c337dcb5e3a29cbe50b1b77589941e1e1c7090c950766de7a3
SSDEEP:	6144:NBn0ph65gGns2YvYPUaC55QAU4wVdsTbUi:EpoGHiO554Nbwb3
TLSH:	D664CD762170EF66D91F3830C86382F69667DE0ADE1457DFB6903E1A7832192F932643
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon



Icon Hash:	d08eb292f2e89ce2

Static PE Info

General

Entrypoint:	0x40324f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 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:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007F5EF0F47EB3h
push ebx
call 00007F5EF0F4ACA1h
cmp eax, ebx
je 00007F5EF0F47EA9h
push 00000C00h
call eax
push 004091E0h
call 00007F5EF0F4AC22h
push 004091D8h
call 00007F5EF0F4AC18h
push 004091CCh
call 00007F5EF0F4AC0Eh
push 0000000Dh
call 00007F5EF0F4AC71h
push 0000000Bh
call 00007F5EF0F4AC6Ah

Instruction
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007F5EF0F4A8A1h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F5EF0F4A88Fh
push ebx
call dword ptr [00407144h]

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73cc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x9ee0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x2d000	0x9ee0	0xa000	False	0.1594970703125	data	3.5990213744393147	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d280	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 11811 x 11811 px/m	English	United States
RT_ICON	0x314a8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 11811 x 11811 px/m	English	United States
RT_ICON	0x33a50	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 11811 x 11811 px/m	English	United States
RT_ICON	0x34af8	0x1045	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x35b40	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304, resolution 11811 x 11811 px/m	English	United States
RT_ICON	0x364c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 11811 x 11811 px/m	English	United States
RT_DIALOG	0x36930	0x100	data	English	United States
RT_DIALOG	0x36a30	0x11c	data	English	United States
RT_DIALOG	0x36b50	0x60	data	English	United States
RT_GROUP_ICON	0x36bb0	0x5a	data	English	United States
RT_MANIFEST	0x36c10	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

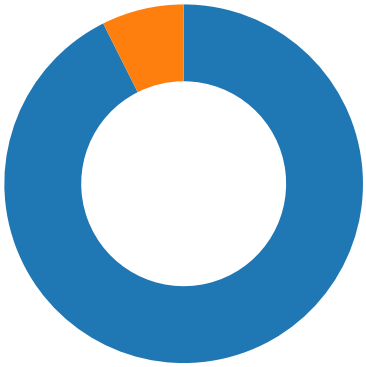
DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 54

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:22:22.784383059 CET	49710	80	192.168.2.3	195.110.124.133
Nov 30, 2022 02:22:22.842713118 CET	80	49710	195.110.124.133	192.168.2.3
Nov 30, 2022 02:22:22.842864037 CET	49710	80	192.168.2.3	195.110.124.133
Nov 30, 2022 02:22:22.848509073 CET	49710	80	192.168.2.3	195.110.124.133
Nov 30, 2022 02:22:22.906733036 CET	80	49710	195.110.124.133	192.168.2.3
Nov 30, 2022 02:22:22.911145926 CET	80	49710	195.110.124.133	192.168.2.3
Nov 30, 2022 02:22:22.914767981 CET	80	49710	195.110.124.133	192.168.2.3
Nov 30, 2022 02:22:22.914897919 CET	49710	80	192.168.2.3	195.110.124.133
Nov 30, 2022 02:22:22.914952993 CET	49710	80	192.168.2.3	195.110.124.133
Nov 30, 2022 02:22:22.973588943 CET	80	49710	195.110.124.133	192.168.2.3
Nov 30, 2022 02:22:27.959201097 CET	49711	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:28.016766071 CET	80	49711	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:28.018054008 CET	49711	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:28.018217087 CET	49711	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:28.075455904 CET	80	49711	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:28.078820944 CET	80	49711	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:28.078874111 CET	80	49711	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:28.079058886 CET	49711	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:29.031352043 CET	49711	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:30.171621084 CET	49712	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:30.229381084 CET	80	49712	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:30.229496002 CET	49712	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:30.229651928 CET	49712	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:30.287029982 CET	80	49712	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:30.288594961 CET	80	49712	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:30.288676023 CET	80	49712	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:30.288764954 CET	49712	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:31.238483906 CET	49712	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:32.250713110 CET	49713	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:32.308607101 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.308743954 CET	49713	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:32.309048891 CET	49713	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:32.366486073 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.366560936 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.366606951 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.366653919 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.373341084 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.373418093 CET	80	49713	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:32.373527050 CET	49713	80	192.168.2.3	81.88.48.71

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:22:33.312879086 CET	49713	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.328996897 CET	49714	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.387155056 CET	80	49714	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:34.387286901 CET	49714	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.387420893 CET	49714	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.445230007 CET	80	49714	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:34.450206041 CET	80	49714	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:34.450313091 CET	80	49714	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:34.450730085 CET	49714	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.451093912 CET	49714	80	192.168.2.3	81.88.48.71
Nov 30, 2022 02:22:34.509608984 CET	80	49714	81.88.48.71	192.168.2.3
Nov 30, 2022 02:22:39.630742073 CET	49715	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:39.798660994 CET	80	49715	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:39.798887014 CET	49715	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:39.798988104 CET	49715	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:39.966043949 CET	80	49715	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:39.973978996 CET	80	49715	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:39.974056005 CET	80	49715	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:39.974246979 CET	49715	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:40.820147991 CET	49715	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:41.832281113 CET	49716	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:41.999494076 CET	80	49716	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:42.001230001 CET	49716	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:42.001358032 CET	49716	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:42.168423891 CET	80	49716	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:42.176863909 CET	80	49716	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:42.176980972 CET	80	49716	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:42.177134991 CET	49716	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:43.016860962 CET	49716	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:44.035156012 CET	49717	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:44.203669071 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.203809977 CET	49717	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:44.204161882 CET	49717	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:44.372004032 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.372042894 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.372071028 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.372103930 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.372131109 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.379828930 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.379976034 CET	80	49717	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:44.380150080 CET	49717	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:45.204660892 CET	49717	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:46.220715046 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:46.387703896 CET	80	49718	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:46.387904882 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:46.388169050 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:46.555027008 CET	80	49718	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:46.590737104 CET	80	49718	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:46.642049074 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:56.607110977 CET	80	49718	50.87.143.200	192.168.2.3
Nov 30, 2022 02:22:56.607465029 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:56.607465029 CET	49718	80	192.168.2.3	50.87.143.200
Nov 30, 2022 02:22:56.774600029 CET	80	49718	50.87.143.200	192.168.2.3
Nov 30, 2022 02:23:01.713402987 CET	49719	80	192.168.2.3	194.58.112.174
Nov 30, 2022 02:23:01.775351048 CET	80	49719	194.58.112.174	192.168.2.3
Nov 30, 2022 02:23:01.775471926 CET	49719	80	192.168.2.3	194.58.112.174
Nov 30, 2022 02:23:01.775626898 CET	49719	80	192.168.2.3	194.58.112.174
Nov 30, 2022 02:23:01.837239027 CET	80	49719	194.58.112.174	192.168.2.3
Nov 30, 2022 02:23:01.837311029 CET	80	49719	194.58.112.174	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:23:01.837358952 CET	80	49719	194.58.112.174	192.168.2.3
Nov 30, 2022 02:23:01.837461948 CET	49719	80	192.168.2.3	194.58.112.174

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:22:22.742185116 CET	52387	53	192.168.2.3	8.8.8.8
Nov 30, 2022 02:22:22.777436972 CET	53	52387	8.8.8.8	192.168.2.3
Nov 30, 2022 02:22:27.925657988 CET	56924	53	192.168.2.3	8.8.8.8
Nov 30, 2022 02:22:27.958118916 CET	53	56924	8.8.8.8	192.168.2.3
Nov 30, 2022 02:22:39.482861042 CET	60625	53	192.168.2.3	8.8.8.8
Nov 30, 2022 02:22:39.629431009 CET	53	60625	8.8.8.8	192.168.2.3
Nov 30, 2022 02:23:01.644376993 CET	49302	53	192.168.2.3	8.8.8.8
Nov 30, 2022 02:23:01.712326050 CET	53	49302	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 02:22:22.742185116 CET	192.168.2.3	8.8.8.8	0x14f2	Standard query (0)	www.inhomeyoga.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:22:27.925657988 CET	192.168.2.3	8.8.8.8	0xdff8	Standard query (0)	www.fedefarmatour.online	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:22:39.482861042 CET	192.168.2.3	8.8.8.8	0xe02d	Standard query (0)	www.t4yfrance.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:23:01.644376993 CET	192.168.2.3	8.8.8.8	0xd8c3	Standard query (0)	www.a8-group.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 02:22:22.777436972 CET	8.8.8.8	192.168.2.3	0x14f2	No error (0)	www.inhomeyoga.com	inhomeyoga.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:22:22.777436972 CET	8.8.8.8	192.168.2.3	0x14f2	No error (0)	inhomeyoga.com		195.110.124.133	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:22:27.958118916 CET	8.8.8.8	192.168.2.3	0xdff8	No error (0)	www.fedefarmatour.online	fedefarmatour.online		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:22:27.958118916 CET	8.8.8.8	192.168.2.3	0xdff8	No error (0)	fedefarmatour.online		81.88.48.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:22:39.629431009 CET	8.8.8.8	192.168.2.3	0xe02d	No error (0)	www.t4yfrance.com	t4yfrance.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:22:39.629431009 CET	8.8.8.8	192.168.2.3	0xe02d	No error (0)	t4yfrance.com		50.87.143.200	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:23:01.712326050 CET	8.8.8.8	192.168.2.3	0xd8c3	No error (0)	www.a8-group.com		194.58.112.174	A (IP address)	IN (0x0001)	false

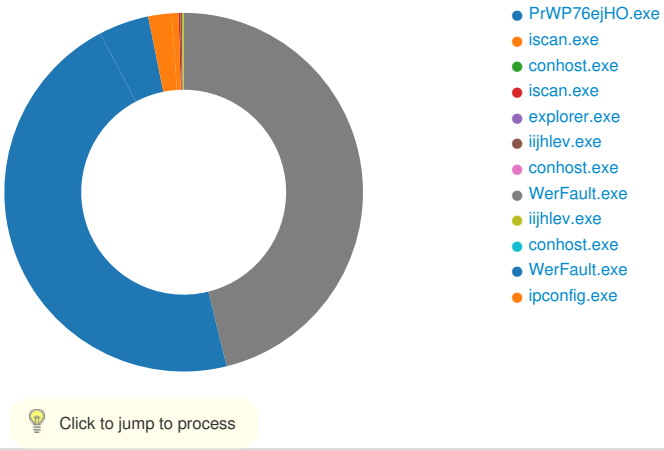
HTTP Request Dependency Graph

- www.inhomeyoga.com
- www.fedefarmatour.online
- www.t4yfrance.com
- www.a8-group.com

Copyright Joe Security LLC 2022

Statistics

Behavior



System Behavior

Analysis Process: PrWP76ejHO.exe PID: **1832**, Parent PID: **3452**

General

Target ID:	0
Start time:	02:20:59
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\PrWP76ejHO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PrWP76ejHO.exe
Imagebase:	0x400000
File size:	318559 bytes
MD5 hash:	DB102A67350060A1E967AEF81118F18D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: iscan.exe PID: **1764**, Parent PID: **1832**

General

Target ID:	1
Start time:	02:21:00
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\iscan.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	2B4B3369E04DEDD66517641DB0F5A8AB
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iidryiceixqa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4508FC	CreateDirectoryW
C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	450372	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe	0	125440	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iscan.exe PID: **5188**, Parent PID: **1764**

General

Target ID:	3
Start time:	02:21:01
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\iscan.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Local\Temp\zxtnbfvzh.c
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	2B4B3369E04DEDD66517641DB0F5A8AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.358869941.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.359082875.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.359082875.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.359082875.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.359082875.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.359171338.00000000006D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.359171338.00000000006D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.359171338.00000000006D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.359171338.00000000006D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E08E	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5188**

General

Target ID:	4
Start time:	02:21:06
Start date:	30/11/2022

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.318358624.000000000EF49000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.318358624.000000000EF49000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.318358624.000000000EF49000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.318358624.000000000EF49000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: iijhlev.exe PID: **4468**, Parent PID: **3452**

General

Target ID:	5
Start time:	02:21:13
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe" "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	2B4B3369E04DEDD66517641DB0F5A8AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iscan.exe	unknown	125440	success or wait	1	409809	ReadFile

Analysis Process: conhost.exe PID: **1836**, Parent PID: **4468**

General	
Target ID:	6
Start time:	02:21:13
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **5096**, Parent PID: **4468**

General	
Target ID:	9
Start time:	02:21:18
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4468 -s 452
Imagebase:	0x140000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D6A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp.xml	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB4.tmp.csv	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD4.tmp.txt	success or wait	1	6D69497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 2e fd 63 fd 05 12 00 00 00 00 00	MDMP .c	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	5620	6	00 00 00 00 00 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	200	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 15 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 74 11 00 00 fd 2e fd 63 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 20 00 00 0d 00 00 00 00 00 00 00 01 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 0b 00 00 00 01 00 02 00 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	UBGenuineIntelWTt.c Pacific Standard TimePacific Daylight Time	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	6416	716	7f 00 01 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	25788	4096	fd fd 19 00 00 00 1a 00 00 fd 19 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 40 39 00 00 00 00 00 00 74 11 00 00 fd 08 00 00 00 00 00 00 20 1f 58 00 00 10 39 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	4868	752	00 00 7a 73 00 00 00 00 00 fd 00 00 fd 53 00 00 25 7e 71 75 fd 18 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 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 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 00 70 fd 02 00 00 00 00 00 00 40 fd 02 00 00 00 00 5b 46 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 70 03 00 00 00 00 00 43 71 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 17 1b 00 00 00 00 00 68 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 17 05 00 00 00 00	zsS%~quBB?"@AZbp@[FpCqh@	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	29884	7094	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E08.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 0b 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 40 24 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 30 12 00 00 42 7e 00 00 15 00 00 00 fd 01 00 00 70 13 00 00 16 00 00 00 fd 00 00 00 5c 15 00 00	@$T8T0B~p\	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 34 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4468</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1002	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 69 00 69 00 6a 00 68 00 6c 00 65 00 76 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>iijhlev.exe</ImageName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1078	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 32 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>00000002</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1176	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 33 00 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8395</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1430	86	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 35 00 39 00 39 00 30 00 38 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>59908096</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1516	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1520	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1526	70	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 35 00 39 00 38 00 39 00 39 00 39 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>59899904</VirtualSize>	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1606	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 32 00 36 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2679</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1690	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 31 00 30 00 33 00 39 00 39 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10399744</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1798	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 31 00 30 00 33 00 39 00 39 00 37 00 34 00 34 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>10399744</WorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106960</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106792</QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2122	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 35 00 30 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>50152</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 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>49800</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 32 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5427200</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 33 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5435392</PeakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 32 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5427200</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2642	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2736	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 35 00 36 00 30 00 37 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4956074</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3164	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3228	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 37 00 31 00 31 00 30 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>67110</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 33 00 35 00 35 00 32 00 35 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>143552512</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 33 00 35 00 35 00 32 00 35 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>143552512</WorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 39 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 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>1142952</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 38 00 36 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1098616</QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4024	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 39 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4162	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 38 00 33 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>83336</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4284	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 34 00 37 00 34 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>474275 84</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4376	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 34 00 38 00 34 00 35 00 39 00 37 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>48 459776</P eakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4484	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 34 00 37 00 34 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4742758 4</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4570	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4626	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4714	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4762	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4808	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	4878	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 69 00 69 00 6a 00 68 00 6c 00 65 00 76 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>iijhlev.exe</Parameter0>	success or wait	8	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5522	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5568	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	5614	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6174	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6220	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6266	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6368	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 69 00 74 00 71 00 77 00 6b 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>bitqwk, Inc. </SystemManufacturer>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6482	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 69 00 74 00 71 00 77 00 6b 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>bitqwk7,1</ SystemProductName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6586	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6714	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 38 00 32 00 37 00 39 00 37 00 36 00 33 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>1618279763</OSInstallDate>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6804	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6914	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	6988	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7034	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7076	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7178	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7220	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7252	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7498	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7502	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7504	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7536	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 31 00 31 00 2d 00 33 00 30 00 54 00 31 00 30 00 3a 00 32 00 31 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-30T10:21:21Z">	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7636	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7640	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7644	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 32 00 39 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 34 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 35 00 33 00 31 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="293" PID="4468" UptimeMS="1531" TimeSinceCreationMS="1531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7914	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7940	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7978	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7982	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	7984	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8022	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8026	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8030	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 34 00 30 00 33 00 61 00 62 00 66 00 34 00 2d 00 32 00 37 00 66 00 36 00 2d 00 34 00 33 00 39 00 61 00 2d 00 39 00 62 00 37 00 62 00 2d 00 34 00 61 00 35 00 38 00 65 00 65 00 39 00 63 00 66 00 64 00 36 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1403abf4-27f6-439a-9b7b-4a58ee9cfd67</Guid>	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8128	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8132	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8136	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 31 00 31 00 2d 00 33 00 30 00 54 00 31 00 30 00 3a 00 32 00 31 00 3a 00 32 00 31 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>2022-11-30T10:21:21Z</CreationTime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8234	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8238	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8240	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8280	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2EB.tmp.WERInternalMetadata.xml	8284	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3E6.tmp.xml	0	4588	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 3c 6f 73 3e 0d 0a 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 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 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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\Report.wer	0	2	fd fd		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\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	153	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_13a3c518\Report.wer	9920	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 35 00 38 00 34 00 35 00 34 00 30 00 33 00 36 00 32 00	MetadataHash=5845403 62	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: iijhlev.exe PID: **4864**, Parent PID: **3452**

General

Target ID:	12
Start time:	02:21:21
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\iidryiceixqa\iijhlev.exe" "C:\Users\user\AppData\Local\Temp\iscan.exe" C:\Users\user\AppData\Loca
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	2B4B3369E04DEDD66517641DB0F5A8AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iscan.exe	unknown	125440	success or wait	1	409809	ReadFile

Analysis Process: conhost.exe PID: **5872**, Parent PID: **4864**

General

Target ID:	13
Start time:	02:21:21
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **2436**, Parent PID: **4864**

General

Target ID:	17
Start time:	02:21:23
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4864 -s 420
Imagebase:	0x140000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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	6D6A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	success or wait	1	6D69497A	unknown

Copyright Joe Security LLC 2022

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.xml	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1883.tmp.csv	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18A4.tmp.txt	success or wait	1	6D69497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 2e fd 63 fd 05 12 00 00 00 00 00	MDMP .c	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	5512	6	00 00 00 00 00 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	200	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 15 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 00 13 00 00 fd 2e fd 63 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 20 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBGenuineIntelWT.c Pacific Standard TimePacific Daylight Time	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	6280	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	1620	168	fd 07 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5d 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	6996	716	3f 00 01 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	29748	6762	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 68 0b 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 23 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 10 00 00 fd 7d 00 00 15 00 00 00 fd 01 00 00 04 13 00 00 16 00 00 00 fd 00 00 00 fd 14 00 00	h#T8T}	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4864</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1002	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 69 00 69 00 6a 00 68 00 6c 00 65 00 76 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>iijhlev.exe</ImageName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1078	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 32 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>00000002</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1176	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 38 00 37 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2874</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1430	86	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 35 00 39 00 32 00 35 00 36 00 38 00 33 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>59256832</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1516	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1520	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1526	70	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 35 00 39 00 32 00 34 00 38 00 36 00 34 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>59248640</VirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1606	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 32 00 35 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2579</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1690	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 31 00 30 00 30 00 33 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10035200</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1798	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 31 00 30 00 30 00 33 00 35 00 32 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10035200</WorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 35 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>105704</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 35 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>105536</QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>49632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 32 00 38 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>49280</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 37 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5373952</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 38 00 32 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5382144</PeakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 37 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5373952</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2642	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2736	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6D69497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 35 00 38 00 38 00 38 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4958880</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3164	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3228	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 37 00 39 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>67916</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 35 00 35 00 34 00 37 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>145547264</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 35 00 35 00 34 00 37 00 32 00 36 00 34 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>145547264</WorkingSetSize>	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 39 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 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>114295 2</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 31 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1091352</ QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4024	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 39 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4162	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 38 00 33 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>83064</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4284	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 34 00 37 00 32 00 30 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>47206400</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4376	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 34 00 38 00 34 00 35 00 39 00 37 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>48459776</PeakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4484	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 34 00 37 00 32 00 30 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>47206400</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4570	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4626	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4714	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4762	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4808	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	4878	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 69 00 69 00 6a 00 68 00 6c 00 65 00 76 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>iijhlev.exe</Parameter0>	success or wait	8	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5522	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5568	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	5614	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6174	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6220	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6266	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6368	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 69 00 74 00 71 00 77 00 6b 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>bitqwk, Inc.</SystemManufacturer>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6482	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 69 00 74 00 71 00 77 00 6b 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>bitqwk7,1</SystemProductName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6586	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6714	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 38 00 32 00 37 00 39 00 37 00 36 00 33 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>1618279763</OSInstallDate>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6804	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6914	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	6988	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7034	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7076	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7178	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7220	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7252	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7516	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7548	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 31 00 31 00 2d 00 33 00 30 00 54 00 31 00 30 00 3a 00 32 00 31 00 3a 00 32 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-30T10:21:24Z">	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7656	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 38 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 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 36 00 37 00 31 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 00 31 00 22	<Process AsId="301" PID="4864" UptimeMS="671" TimeSinceCreationMS="671" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7922	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7948	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	7992	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8038	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 62 00 65 00 34 00 33 00 64 00 31 00 64 00 2d 00 61 00 30 00 30 00 61 00 2d 00 34 00 39 00 32 00 63 00 2d 00 38 00 30 00 34 00 33 00 2d 00 30 00 63 00 66 00 61 00 64 00 65 00 37 00 33 00 38 00 39 00 30 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3be43d1d-a00a-492c-8043-0cfade73890b</Guid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8144	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 31 00 31 00 2d 00 33 00 30 00 54 00 31 00 30 00 3a 00 32 00 31 00 3a 00 32 00 34 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>2022-11-30T10:21:24Z</CreationTime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8246	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8248	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8288	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADE7.tmp.WERInternalMetadata.xml	8292	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE2.tmp.xml	0	4588	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer	0	2	fd fd		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_iijhlev.exe_1f8fea7f532b19688b19ecb27f0cb421e50658_51a01df6_09cfc527\Report.wer	9820	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 33 00 32 00 31 00 32 00 39 00 36 00 39 00 33 00	MetadataHash=-632129693	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: **1916**, Parent PID: **3452**

General

Target ID:	22
Start time:	02:21:49
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x210000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.510165837.0000000002B00000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.510165837.0000000002B00000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.510165837.0000000002B00000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.510165837.0000000002B00000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.509923040.0000000002A00000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.509923040.0000000002A00000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.509923040.0000000002A00000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.509923040.0000000002A00000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.509338770.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.509338770.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.509338770.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.509338770.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1x6VE38oK	object name not found	1	2B1C987	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1x6VE38oK	sharing violation	1	2B1C987	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1x6VE38oK	sharing violation	1	2B1C987	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2B1C957	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly