ID: 321086
Sample Name: PO.exe
Cookbook: default.jbs
Time: 10:59:15
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

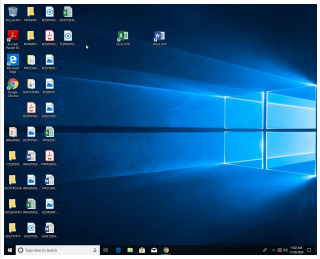
Analysis Report PO.exe

Overview

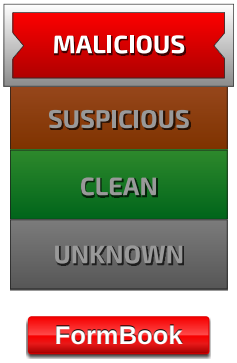
General Information

Sample Name:	PO.exe
Analysis ID:	321086
MD5:	1a278a89f8176f9..
SHA1:	50beebd33a8b68..
SHA256:	73a8ac37a0f0c67..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

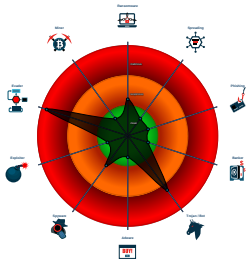


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Hides threads from debuggers
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect virtualization through…
- Uses netsh to modify the Windows n…

Classification



Startup

- **System is w10x64**
- PO.exe (PID: 3064 cmdline: 'C:\Users\user\Desktop\PO.exe' MD5: 1A278A89F8176F9D38A04F4E58A8C072)
  - PO.exe (PID: 5820 cmdline: C:\Users\user\Desktop\PO.exe MD5: 1A278A89F8176F9D38A04F4E58A8C072)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 6964 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 7052 cmdline: /c del 'C:\Users\user\Desktop\PO.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WerFault.exe (PID: 4456 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3064 -s 1204 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.484649434.00000000031B0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.484649434.00000000031B0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

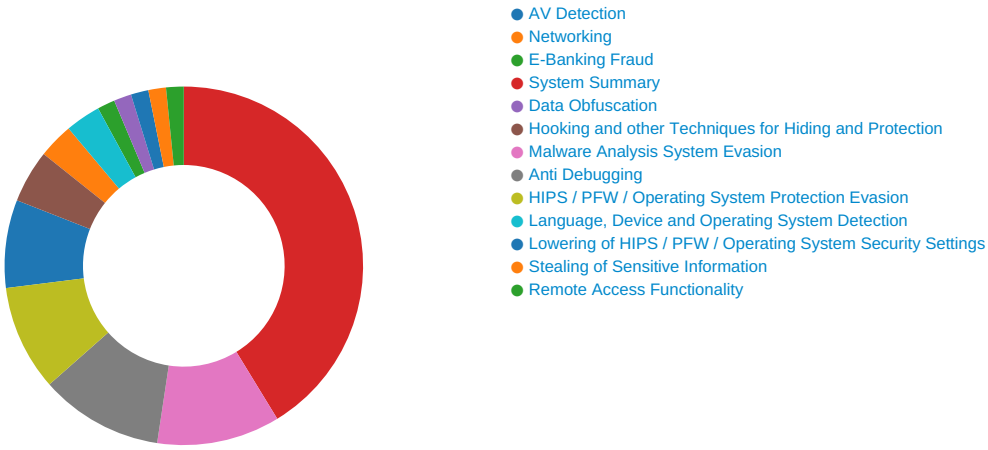
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.PO.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.PO.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.PO.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
3.2.PO.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.PO.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

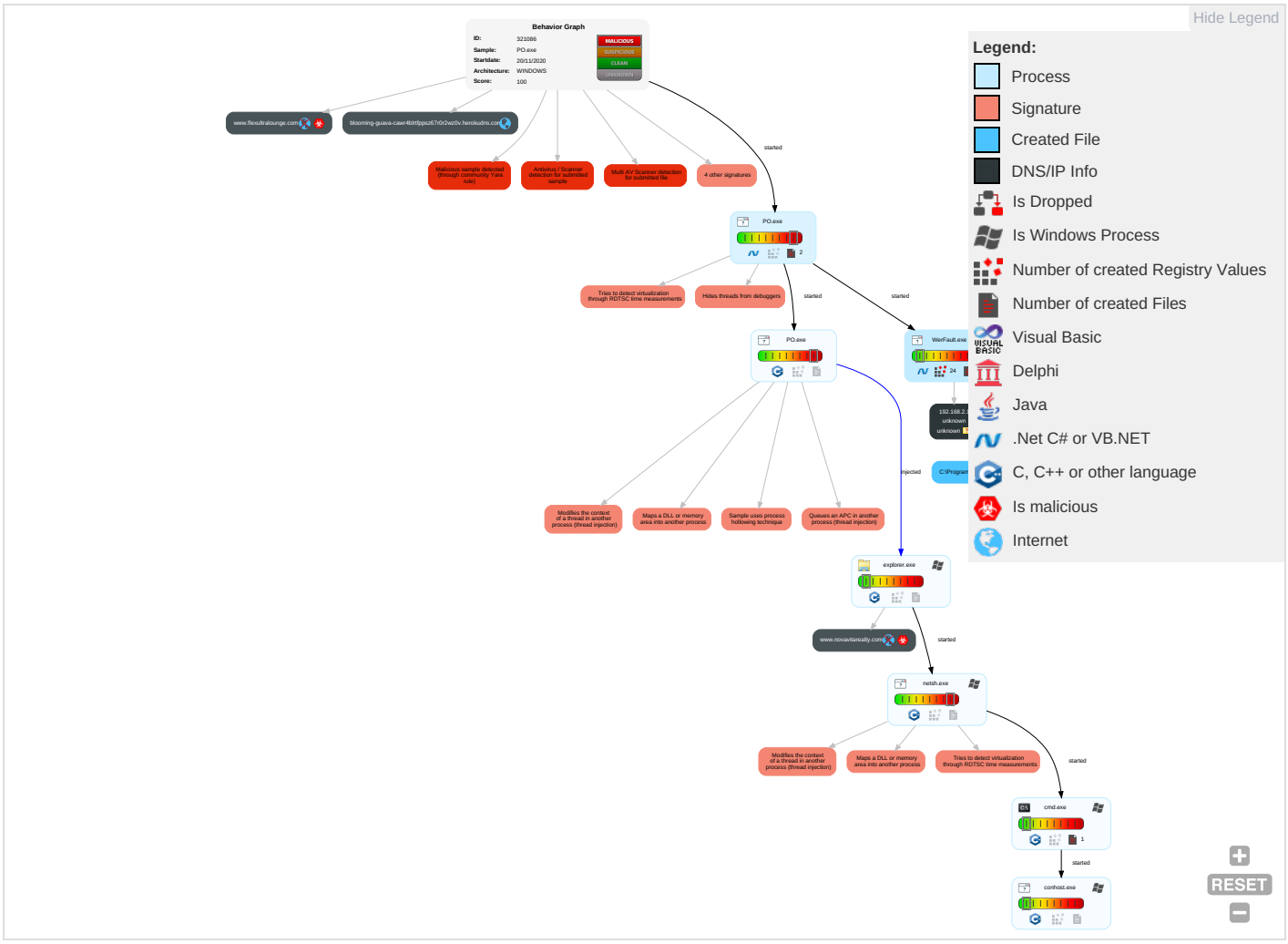
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 4 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 1 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 4 1 2	LSA Secrets	System Information Discovery 1 2 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

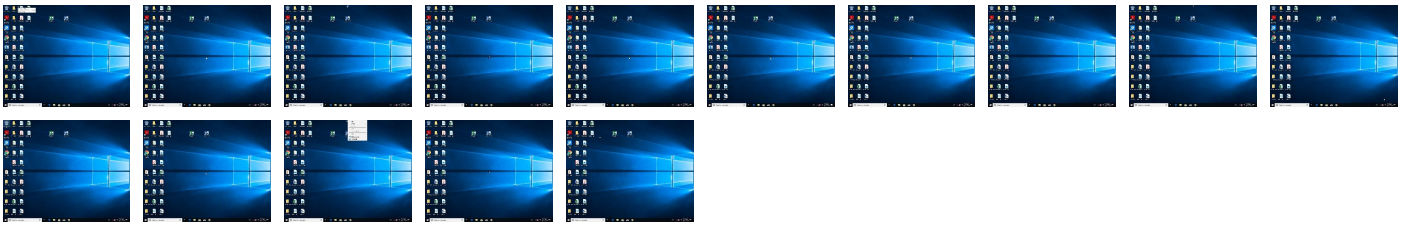
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO.exe	39%	Virustotal		Browse
PO.exe	10%	ReversingLabs		
PO.exe	100%	Avira	TR/Injector.eajju	
PO.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.PO.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
www.flexultralounge.com	0%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://crl.v	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

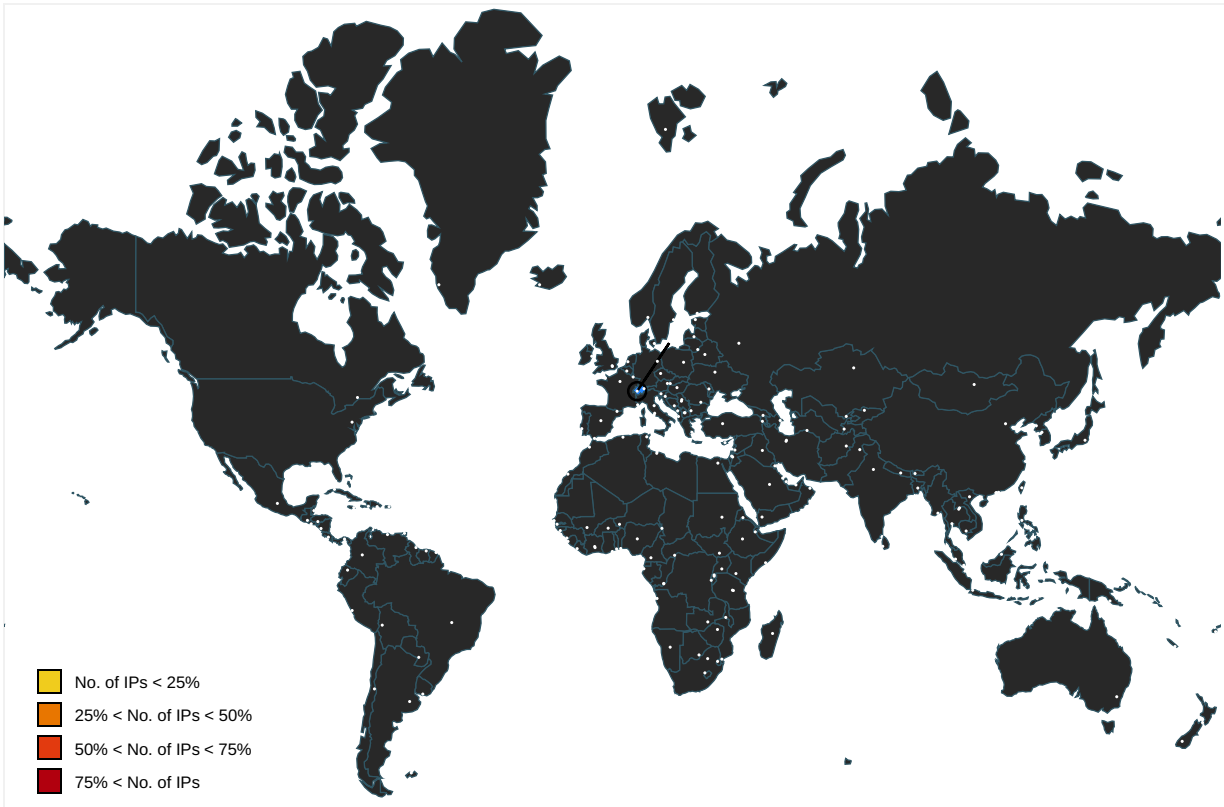
Name	IP	Active	Malicious	Antivirus Detection	Reputation
blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com	34.232.47.250	true	false		unknown
www.novavitarealty.com	unknown	unknown	true		unknown
www.flexultralounge.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css	netsh.exe, 00000010.00000002.4 91969634.000000000432F000.0000 0004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.288649915.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.v	explorer.exe, 00000006.0000000 2.484389821.0000000001398000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321086
Start date:	20.11.2020
Start time:	10:59:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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.evad.winEXE@8/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.7% (good quality ratio 26.3%) • Quality average: 72.7% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.193.48, 23.210.248.85, 51.104.139.180, 8.248.121.254, 8.241.11.126, 67.26.83.254, 8.241.9.126, 8.248.113.254, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:00:38	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14094
Entropy (8bit):	3.7695922857449777
Encrypted:	false
SSDEEP:	192:pigwqmHBUZMXCaKKYKd9/u7sFS274Itl/:m7BUZMXCad9/u7sFX4Itl/
MD5:	D77377036B2D229A28FD4B25F0044C71
SHA1:	52D3B8CE5C9ACBEB6F4F0920D840AA10105B2BCA
SHA-256:	A157F350D251B06DEF44269C215FD29D559D99C65D617D99A96301288122A534
SHA-512:	904701C489605A0C4736E45BFED1CC00394C8DDA7D7EAA7DFCCBF73489850563BA7BA88E51A7508A7C1AF9511CAC9327EA80F02A7BF2F4B8AB1874322B2CC7C2
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.3.7.2.4.3.5.0.7.6.9.0.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.3.7.2.4.3.6.4.8.3.1.5.0.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.d.b.1.e.c.7.8.-.2.5.8.b.-.4.d.2.e.-.8.e.d.d.-.d.a.9.c.c.e.9.7.3.8.2.a.....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.=.1.f.1.9.9.3.2.e.-.8.4.b.7.-.4.5.b.3.-.a.d.2.f.-.f.7.a.6.3.0.4.c.4.2.f.7.....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.=.P.O...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.b.f.8.-.0.0.0.1.-.0.0.1.7.-.b.5.7.c.-.6.0.5.e.6.f.b.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.1.5.5.8.2.5.8.1.7.f.b.3.c.a.1.d.e.4.7.3.6.2.b.f.7.d.2.2.7.6.e.0.0.0.0.f.f.f.f.!.0.0.0.0.5.0.b.e.e.b.d.3.3.a.8.b.6.8.6.0.2.6.3.2.e.1.e.c.0.6.5.c.c.6.e.3.b.7.0.b.4.0.e.a.!.P.O...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 20 19:00:35 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	241083
Entropy (8bit):	3.943938856250719
Encrypted:	false
SSDEEP:	3072:+90FUCgUdQjOJsR0Zjd+p+EeYE18oe9gIOgF5L2:AmTj160OpIYlf9RpDC
MD5:	6CDBA3737AB2EFAD72CCC19F1C0466BC
SHA1:	FB09AC375E482B6916422B243BDFDFBF7076E35F
SHA-256:	4B617196F7F20BE5F6551F2478B4E11C3491789CA047C324E145563267B949E0
SHA-512:	4069D5F9D62486F5057EB95155C7C1AAFE70AB0F1DD801555A4F9ADB8AA4EC929BFF42A6B7A965949C9DE401D786833947271F94894F32B4A4FC3E2436E11327
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....S..._.....U.....B.....#.....GenuineIntelW.....T.....9.._.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8376
Entropy (8bit):	3.69264885519139
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiHa6A/6YSvSUZ2YTgmfZlSjCprR389b9vsf2fm:RrlsNi66A/6Y6SUZ20gmfrSgo9Uf/
MD5:	A73C345620533EB3DE4FE45689A7A1C7
SHA1:	43E861C1A038FF6EB5DC382876BB7BAE2FE5ADFB
SHA-256:	0AD12BBDA211A7FD2C51F4189CDB84CF223BD5F4977F37E8DDA7411B3A60A803
SHA-512:	4DD6D27F349DADE56F291D80112D700336468C0E0CC266888F95B39CB9A460DF42838D91E148F9C9E73F9372C867A4FA6EDD506B99982005A895F917DBEB52A
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	
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.>.3.0.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4645
Entropy (8bit):	4.446423142087213
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI9yiVhWSC8Bu8fm8M4Jw0RFFgt+q8vARxYNUZCqvBL6d:uITfO5imSNlJw5KsYOvBL6d
MD5:	2C42EEB13CBB3E68A1ECA68B67CFA1BA
SHA1:	869D79D69054BCB04B98A69DD4D05970B310CF3B
SHA-256:	4E7957DE3EFE71E934F817E1CDA120347C1188ACEE25B6412B299706763E135B
SHA-512:	04D94FA3F1873C7195B4750512CD1B4A1651A8F6FF106EFBA732900F1225B6C3C4D670FB39814C21C94DBF350EB2B8461AED2241A0024640A34F6A000CE85610
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="737531" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.014394252916949
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO.exe
File size:	2490880
MD5:	1a278a89f8176f9d38a04f4e58a8c072
SHA1:	50beebd33a8b68602632e1ec065cc6e3b70b40ea
SHA256:	73a8ac37a0f0c6761800a276b77b0fd34d1cf43830f822ef18ff50dbda934751
SHA512:	7c2d439eaae875951c07a5f216448f17b93561e3f6083eee94de7c6241c24ea4da1021c3f12b7986d9edc7ef281d5604d30aae8ce61d90be76d34f3fbfb41291
SSDEEP:	24576:GDJXK2pQMdCIUPf20glUlSFDHucLADt25NcJ60f4fj:E6HtX2NpucA+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....%.....n.&.. ... &...@.. .....@&.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x661c6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB6EFFB [Thu Nov 19 22:21:47 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x261c14	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x262000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x25fc74	0x25fe00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x262000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:00:06.446355104 CET	60152	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:06.474493980 CET	53	60152	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:07.272624016 CET	57544	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:07.299825907 CET	53	57544	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:09.618983984 CET	55984	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:09.646159887 CET	53	55984	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:10.788634062 CET	64185	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:10.815763950 CET	53	64185	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:11.596980095 CET	65110	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:11.624150038 CET	53	65110	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:12.485497952 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:12.512454987 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:14.322824955 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:14.349788904 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:20.443007946 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:20.470057964 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:22.127502918 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:22.154567957 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:25.648582935 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:25.675843000 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:26.850882053 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:26.878113031 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:28.221642971 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:28.248595953 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:29.089920044 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:29.117016077 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:29.745894909 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:29.772902966 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:31.008836031 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:31.044528008 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:32.229650021 CET	57084	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:00:32.256700993 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:32.679534912 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:32.716883898 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:33.041760921 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:33.068943024 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:37.599292040 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:37.626326084 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:37.886054993 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:37.913269043 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 11:00:53.379832029 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:00:53.406965971 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:06.848416090 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:06.896358013 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:07.781565905 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:07.840471029 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:08.251220942 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:08.286914110 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:08.575808048 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:08.611509085 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:08.945375919 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:08.981035948 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:09.396877050 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:09.434571981 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:09.708476067 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:09.735516071 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:09.859127998 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:09.894753933 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:10.490293026 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:10.525974989 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:11.119065046 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:11.146034956 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:11.605583906 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:11.641343117 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:24.849941015 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:24.887193918 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:50.388691902 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:50.415774107 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:51.969986916 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:51.997040987 CET	53	56130	8.8.8.8	192.168.2.3
Nov 20, 2020 11:01:56.846453905 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:01:56.901777983 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 11:02:17.057722092 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 11:02:17.100363970 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:01:56.846453905 CET	192.168.2.3	8.8.8.8	0x2335	Standard query (0)	www.novavi tarealty.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.057722092 CET	192.168.2.3	8.8.8.8	0x380c	Standard query (0)	www.flexul tralounge.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:01:56.901777983 CET	8.8.8.8	192.168.2.3	0x2335	Name error (3)	www.novavi tarealty.com	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	www.flexul tralounge.com	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		34.232.47.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		34.227.164.168	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		3.209.148.13	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		3.222.114.249	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		54.164.152.149	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		3.90.94.177	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		3.213.190.117	A (IP address)	IN (0x0001)
Nov 20, 2020 11:02:17.100363970 CET	8.8.8.8	192.168.2.3	0x380c	No error (0)	blooming-guava-cawr4blrtfppsz67r0r2wz0v.herokudns.com		35.170.115.131	A (IP address)	IN (0x0001)

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

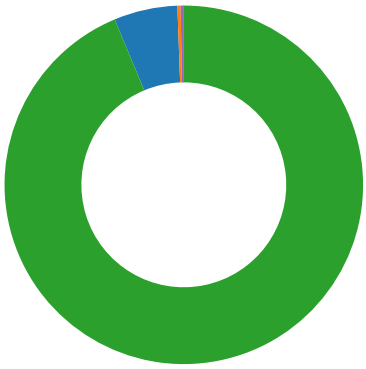
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE7
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE7
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE7
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE7

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO.exe PID: 3064 Parent PID: 5736

General

Start time:	11:00:10
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO.exe'
Imagebase:	0xe30000
File size:	2490880 bytes
MD5 hash:	1A278A89F8176F9D38A04F4E58A8C072
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEFCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DEDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DEDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DEDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DEDD72F	unknown
C:\Users\user\Desktop\PO.exe	unknown	4096	success or wait	1	6DEDD72F	unknown
C:\Users\user\Desktop\PO.exe	unknown	512	success or wait	1	6DEDD72F	unknown

Analysis Process: PO.exe PID: 5820 Parent PID: 3064

General

Start time:	11:00:32
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0x670000
File size:	2490880 bytes
MD5 hash:	1A278A89F8176F9D38A04F4E58A8C072
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: 00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.314545610.0000000001580000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.313036443.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.313036443.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.313036443.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.314657268.00000000015B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.314657268.00000000015B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.314657268.00000000015B0000.00000040.00000001.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	41A027	NtReadFile

Analysis Process: WerFault.exe PID: 4456 Parent PID: 3064

General

Start time:	11:00:34
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3064 -s 1204
Imagebase:	0xee0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6ABD1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6ABC497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp	success or wait	1	6ABC497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	success or wait	1	6ABC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	success or wait	1	6ABC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp.xml	success or wait	1	6ABC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF0F4.tmp.csv	success or wait	1	6ABC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF105.tmp.txt	success or wait	1	6ABC4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 53 12 b8 5f a4 05 12 00 00 00 00 00	MDMP..... .....S.._.....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 bc 23 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f8 0b 00 00 39 12 b8 5f 00 00 00 00 02 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 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	.....U.....B.....#.... ..GenuineIntelW.....T... .....9.._..... .....0..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 08 ed 4f 01 05 00 00 00 00 00 00 00 05 00 00 00 48 ec 4f 01 a0 ec 4f 01 22 d7 21 75 23 00 00 00 16 02 00 00 48 ec 4f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.........O.............H.O. ..O.".!u#.......H.O.+.........	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	168	68 05 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 21 75 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 6d 00 00 00 00 e8 26 74 01 00 00 00 00 88 ed 4f 01 00 00 00 00 01 00 00 00 00 00 00 00 10 ed 4f 01 00 00 00 00 08 ed 4f 01 00 00 00 00 f4 76 d9 6d 00 00 00 00 14 86 67 03 00 00 00 00 e8 26 74 01 00 00 00 00 7a 77 d9 6d 00 00 00 00 68 ec 4f 01 00 00 00 00 cc 02 00 00 88 2a 00 00	h.......RCC.............".!u.. ....m.....&t....... O...............O.......O..... .v.m......g......&t.....zw.m.. ..h.O..........*..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	20	4f 02 00 00 0c 9d 5d 03 00 00 00 00 04 00 00 00 74 6b 00 00	O.....].........tk..	success or wait	591	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	4	6c fc d9 6c	l..l	success or wait	590	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	4	a4 ed d9 6c	...l	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	4	09 00 00 00	....	success or wait	9	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 e0 dd 4f 01 bc 9a e5 77 23 00 00 00 16 02 00 00 50 dc 4f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+.......................... ..O....w#.......P.O.+.........	success or wait	9	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	48	40 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 20 01 00 00 00 00 e4 f8 d8 05 00 00 00 00 1c 07 00 00 b7 67 01 00 cc 02 00 00 b4 43 00 00	@....... ....g.......C..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	4	3a 00 00 00	:...	success or wait	58	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	18	0c 00 00 00 50 00 4f 00 2e 00 65 00 78 00 65 00 00 00	....P.O...e.x.e...	success or wait	58	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	752	00 00 e5 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 62 2a 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 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 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 80 53 02 00 00 00 00 00 60 9b 02 00 00 00 00 95 5b 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 67 66 03 00 00 00 00 00 32 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 26 42 1b 00 00 00 00 00 1a bd 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 6e cc 0b 00 00 00 00	...j.............`.Zb*........ ..................?........... ................)............. ..@A..................Zb...... .............................. ................S......`....... [..................gf......2l ....&B............. @.......n......	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	19256	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	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F6.tmp.dmp	unknown	108	03 00 00 00 b4 01 00 00 fc 06 00 00 04 00 00 00 7c 18 00 00 bc 08 00 00 05 00 00 00 f4 24 00 00 80 46 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 68 2f 00 00 9b 7e 03 00 15 00 00 00 ec 01 00 00 38 21 00 00 16 00 00 00 98 00 00 00 24 23 00 00	.....|.....$...F.....T.....8.....T.....h/...~.....8!.....$#..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 30 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.0.6.4.<./.P.i.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	58	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 4f 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	<.I.m.a.g.e.N.a.m.e.>.P.O..e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 36 00 32 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.6.2.6.6.<./.U.p.t.i.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 37 00 32 00 34 00 35 00 38 00 32 00 34 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.3.2.7.2.4.5.8.2.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 36 00 32 00 39 00 35 00 30 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	<.V.i.r.t.u.a.l.S.i.z.e.>.2.0.6.2.9.5.0.4.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 33 00 30 00 32 00 38 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.3.0.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 39 00 33 00 38 00 34 00 33 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.9.3.8.4.3.2.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 33 00 31 00 34 00 38 00 39 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.3.1.4.8.9.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 37 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.7.9.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 30 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.0.4.4.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 30 00 31 00 34 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 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.7.0.1.4.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	110	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 31 00 30 00 39 00 39 00 39 00 32 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.9.9.9.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 36 00 37 00 32 00 35 00 31 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.0.6.7.2.5.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 35 00 36 00 36 00 39 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.9.5.6.6.9.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 36 00 37 00 32 00 35 00 31 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.0.6.7.2.5.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 31 00 33 00 38 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.2.1.3.8.5.7.<./.U.p.t.i.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 35 00 38 00 38 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.7.5.8.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 34 00 37 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.2.4.7.2.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 32 00 32 00 37 00 32 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.2.2.2.7.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 39 00 39 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 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.9.9.2.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 32 00 37 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.2.7.1.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 35 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 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.5.0.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.9.0.8.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 32 00 39 00 33 00 31 00 39 00 31 00 36 00 38 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.3.1.9.1.6.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 32 00 38 00 39 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.2.8.9.9.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 32 00 39 00 33 00 31 00 39 00 31 00 36 00 38 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.3.1.9.1.6.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	62	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 50 00 4f 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	<.P.a.r.a.m.e.t.e.r.0.>.P.O..e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 71 00 79 00 6c 00 77 00 76 00 69 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.q.y.l.w.v.i.,. .I.n.c...</.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 79 00 6c 00 77 00 76 00 69 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.q.y.l.w.v.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 32 00 36 00 39 00 39 00 35 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.6.9.9.5.0.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 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	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 30 00 2d 00 31 00 31 00 2d 00 32 00 30 00 54 00 31 00 39 00 3a 00 30 00 30 00 3a 00 33 00 36 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.1.-.2.0.T.1.9.:.0.0.:.3.6.Z.".>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 30 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 32 00 33 00 32 00 36 00 35 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 32 00 33 00 32 00 36 00 35 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.1.". .P.I.D.=.".3.0.6.4.". .U.p.t.i.m.e.M.S.=.".2.3.2.6.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.3.2.6.5.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 64 00 62 00 31 00 65 00 63 00 37 00 38 00 2d 00 32 00 35 00 38 00 62 00 2d 00 34 00 64 00 32 00 65 00 2d 00 38 00 65 00 64 00 64 00 2d 00 64 00 61 00 39 00 63 00 63 00 65 00 39 00 37 00 33 00 38 00 32 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.d.b.1.e.c.7.8.-.2.5.8.b.-.4.d.2.e.-.8.e.d.d.-.d.a.9.c.c.e.9.7.3.8.2.a.<./.G.u.i.d.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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 30 00 2d 00 31 00 31 00 2d 00 32 00 30 00 54 00 31 00 39 00 3a 00 30 00 30 00 3a 00 33 00 36 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.1.-.2.0.T.1.9.:.0.0.:.3.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73D.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD809.tmp.xml	unknown	4645	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 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8\Report.wer	unknown	2	ff fe	..	success or wait	1	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	190	6ABC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO.exe_501eda88e083e4b8ea75a1ac83a7c11b0f8b4_f9ae678b_1136dfa8\Report.wer	unknown	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 37 00 37 00 30 00 39 00 35 00 39 00 36 00 31 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.7.7.0.9.5.9.6.1.6.	success or wait	1	6ABC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	success or wait	1	6ABE36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6ABE1FB2	RegCreateKeyExW
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6ABC43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	ProgramId	unicode	00063155825817fb3ca1de47362bf7d2276e0000ffff	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	FileId	unicode	000050beebd33a8b68602632e1ec065cc6e3b70b40ea	success or wait	1	6ABE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	LowerCaseLongPath	unicode	c:\users\user\desktop\po.exe	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	LongPathHash	unicode	po.exe|8dd059df	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	Name	unicode	po.exe	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	Publisher	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	Version	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	BinFileVersion	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	BinaryType	unicode	pe32_clr_32	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	ProductName	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	ProductVersion	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	LinkDate	unicode	11/19/2020 22:21:47	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	BinProductVersion	unicode		success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	Size	B	00 02 26 00 00 00 00 00	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	Language	dword	0	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	IsPeFile	dword	1	success or wait	1	6ABE36BF	unknown
\REGISTRY\A\{d046f2e4-2b30-23a1-285c-ce96e7f43f64}\Root\InventoryApplicationFile\po.exe|8dd059df	IsOsComponent	dword	0	success or wait	1	6ABE36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 21 75 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D8 6D E8 26 74 01 88 ED 4F 01 01 00 00 00 10 ED 4F 01 08 ED 4F 01 F4 76 D9 6D 14 86 67 03 E8 26 74 01 7A 77 D9 6D 68 EC 4F 01	success or wait	1	6ABE1FE8	RegSetValueExW

Analysis Process: explorer.exe PID: 3388 Parent PID: 5820

General

Start time:	11:00:35
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: 6964 Parent PID: 3388

General

Start time:	11:00:52
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0xd90000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 00000010.00000002.484649434.00000000031B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.484649434.00000000031B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.484649434.00000000031B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.483269971.0000000002E50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.483269971.0000000002E50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.483269971.0000000002E50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.483171472.0000000002DB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.483171472.0000000002DB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.483171472.0000000002DB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2DCA027	NtReadFile

Analysis Process: cmd.exe PID: 7052 Parent PID: 6964

General

Start time:	11:00:56
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO.exe'
Imagebase:	0xbd0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7060 Parent PID: 7052

General

Start time:	11:00:56
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis