ID: 412166
Sample Name: nT5pUwoJSS.dll
Cookbook: default.jbs
Time: 13:05:21
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report nT5pUwoJSS.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Rich Headers 18
Data Directories 18
Sections 18

Resources 18
Imports 18
Exports 19
Version Infos 19
Possible Origin 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 23
HTTP Packets 23
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: loaddll32.exe PID: 6924 Parent PID: 6012 24
General 24
File Activities 24
Analysis Process: cmd.exe PID: 6936 Parent PID: 6924 24
General 24
File Activities 25
Analysis Process: rundll32.exe PID: 6948 Parent PID: 6924 25
General 25
File Activities 25
Analysis Process: rundll32.exe PID: 6960 Parent PID: 6936 25
General 25
File Activities 26
Analysis Process: rundll32.exe PID: 6992 Parent PID: 6924 26
General 26
File Activities 26
Analysis Process: rundll32.exe PID: 7008 Parent PID: 6924 26
General 26
File Activities 27
Analysis Process: WerFault.exe PID: 64 Parent PID: 6992 27
General 27
File Activities 27
File Created 27
File Deleted 27
File Written 28
Registry Activities 50
Key Created 50
Key Value Created 50
Analysis Process: iexplore.exe PID: 5516 Parent PID: 800 51
General 51
File Activities 52
Registry Activities 52
Analysis Process: iexplore.exe PID: 4556 Parent PID: 5516 52
General 52
File Activities 52
Disassembly 52
Code Analysis 52

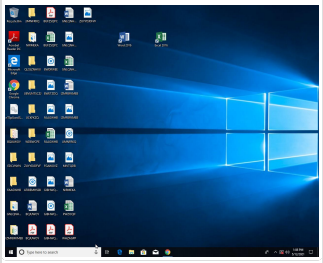
Analysis Report nT5pUwoJSS.dll

Overview

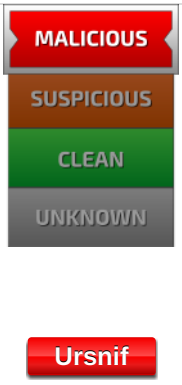
General Information

Sample Name:	nT5pUwoJSS.dll
Analysis ID:	412166
MD5:	6fdbd25f7a84da8..
SHA1:	39a52cbc48be93..
SHA256:	4bf6e9d4067cb90.
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

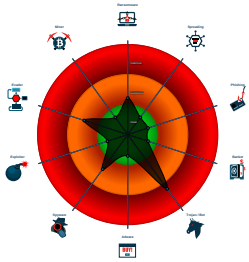


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6924 cmdline: loaddll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6936 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6960 cmdline: rundll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6948 cmdline: rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Eithernothing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6992 cmdline: rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Order MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 64 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6992 -s 892 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7008 cmdline: rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Smileschool MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5516 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4556 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5516 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KujE77ctKyR8x3/dODwZbEsxGmck+FW9384s5u0Kacw8y1gCN+8m2bfjJPovkn+Uzufcdfss+a43eI6oHR1KgWQmvEAO6LK8tJv+Wl7iCBPJP7eef8xKeXht/Mhk1PSj7mHnJ9lcqKMtTteEdSecVvMRtb/WSKVTFfHDva9My7AJ/NbXqHdzCG7znACswLxD",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "worunekulo.club",
    "horunekulo.website"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

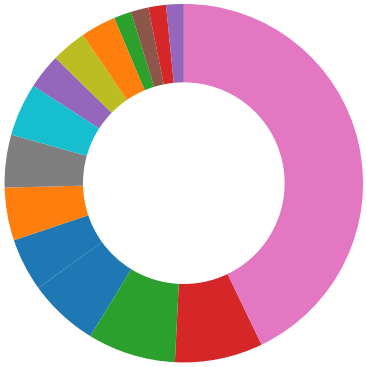
Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.881584954.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.881638380.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.881444184.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.881614039.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.881537844.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

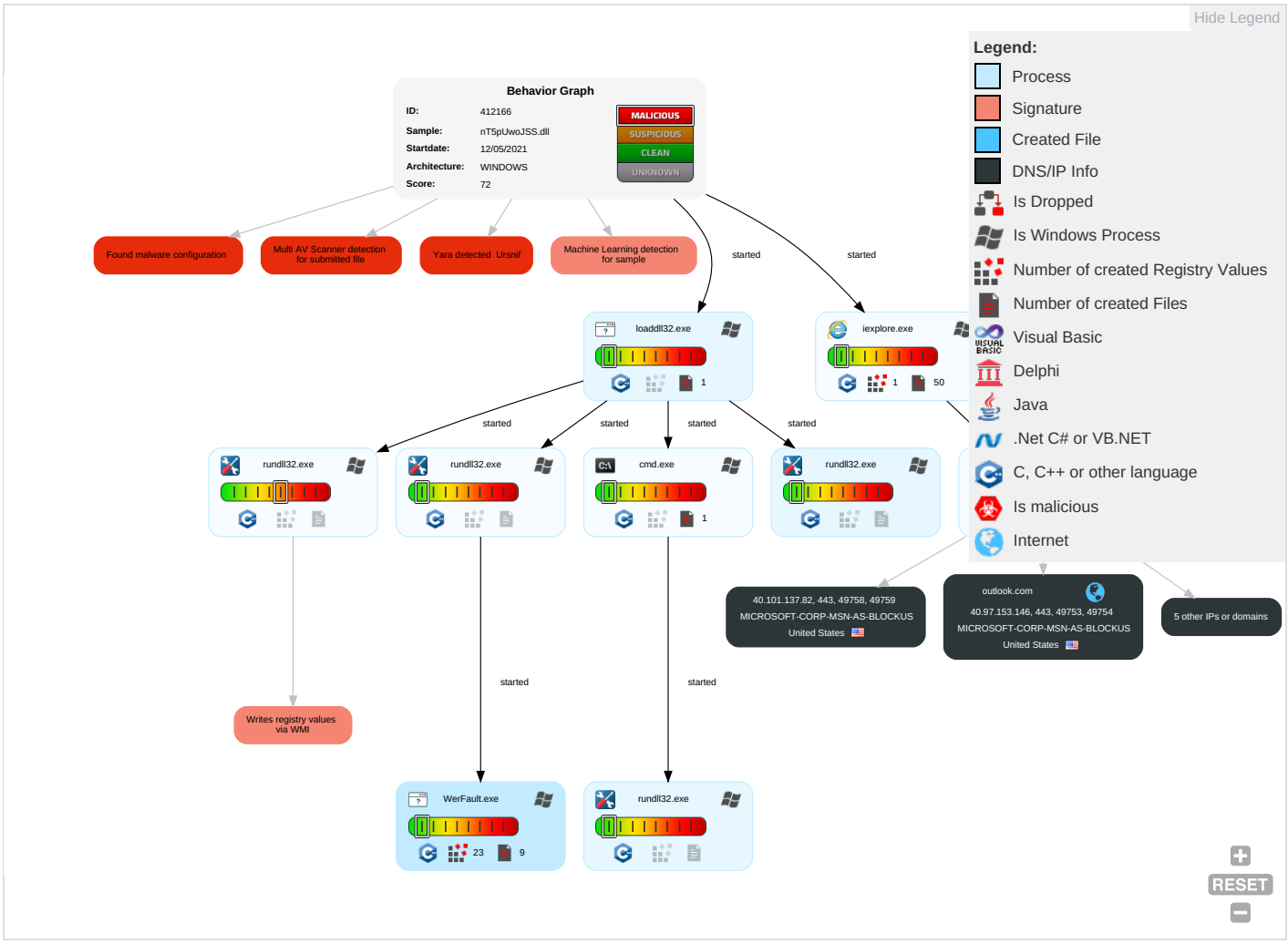
Remote Access Functionality:

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	Re Se Eff
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

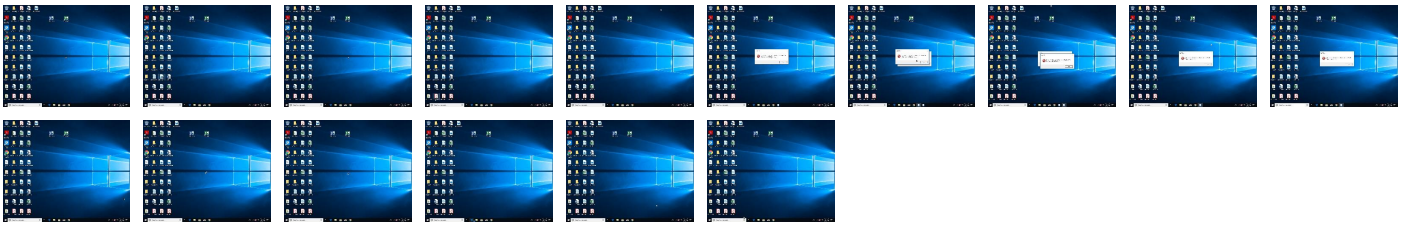
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nT5pUwoJSS.dll	21%	ReversingLabs	Win32.Trojan.Zusy	
nT5pUwoJSS.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2c80000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outlook.com	40.97.153.146	true	false		high
HHN-efz.ms-acdc.office.com	52.97.233.66	true	false		high
www.outlook.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

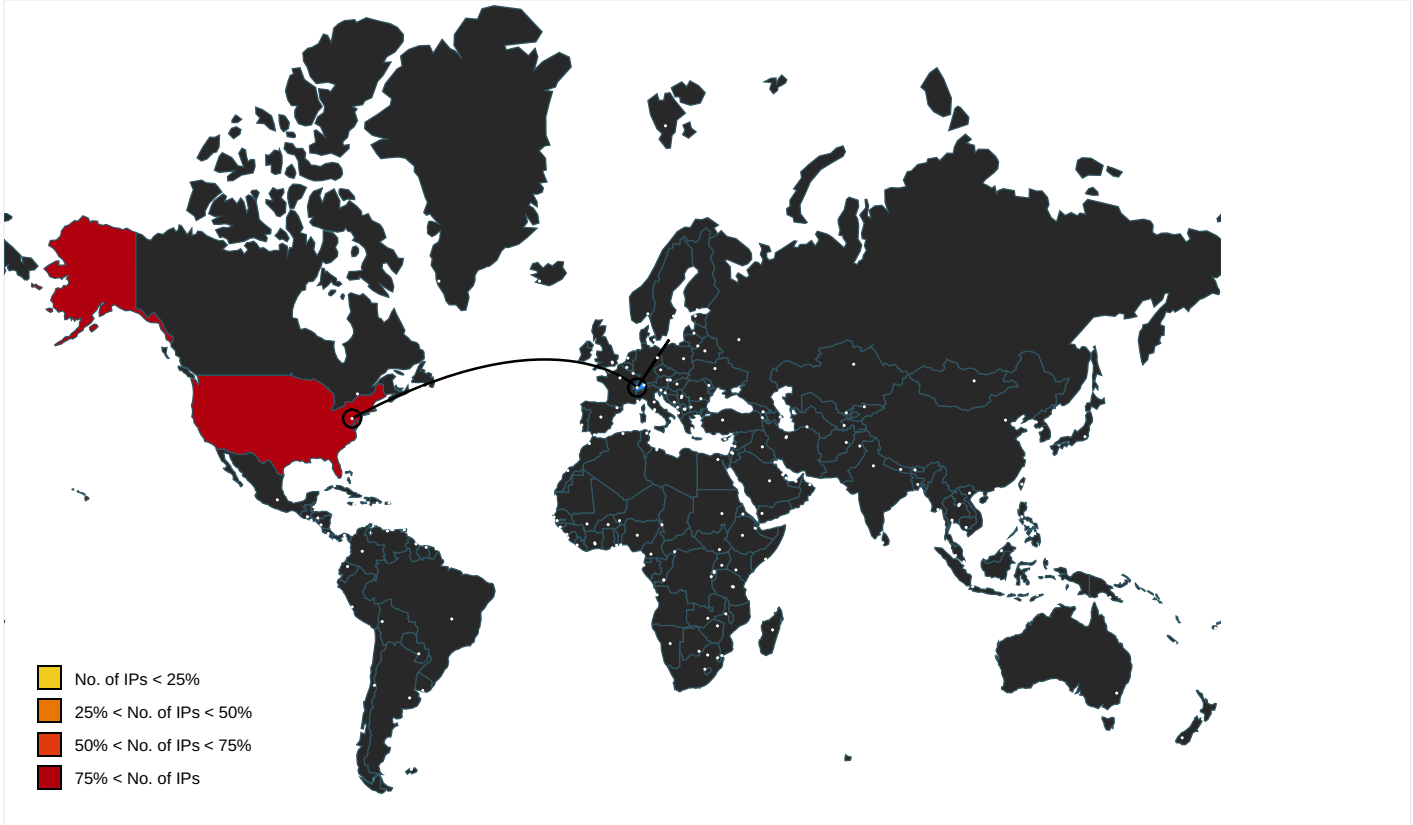
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://outlook.com/login/greed/KnH9H6Qjc_2F7/0e3_2F0_/2FRqQPyOKs18rFK5waVCGCI/jIBCBbgDdF/18TiURZdioL3eU4Wc/SUXArexakZ5d/R0lDxIGeIYj/c6FwtLcTr3EmEj/nbrTM1t_2BdTxREGmfFhs/_2BnTf5cT9dEAnPd/AFLbs3lARk22SMJ/POUz7dti2oyFXHE3_2/FgEVGs1vD/4LhoHpnAxyp/chUrsX.gfk	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/login/greed/KnH9H6Qjc_2F7/0e3_2F0_/2FRqQPyOKs18rFK5waVCGCI/jIBCBbgDdF/	{4BD5DCDF-B312-11EB-90EB-ECF4BBEA1588}.dat.17.dr	false		high
http://crl.microsoft	WerFault.exe, 0000000E.0000000 3.889153103.0000000005072000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.97.233.66	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.101.137.82	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.153.146	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412166
Start date:	12.05.2021
Start time:	13:05:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nT5pUwoJSS.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:	19
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:	mal72.troj.winDLL@15/9@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.1% (good quality ratio 10.5%) • Quality average: 79.6% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 83% • 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

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 92.122.145.220, 2.20.143.16, 2.20.142.209, 104.42.151.234, 52.147.198.201, 168.61.161.212, 20.190.159.138, 20.190.159.132, 20.190.159.136, 40.126.31.141, 40.126.31.137, 20.190.159.134, 40.126.31.139, 40.126.31.143, 20.82.209.183, 104.43.193.48, 92.122.213.247, 92.122.213.194, 88.221.62.148 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, dub2.current.a.prd.aadg.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/412166/sample/nT5pUwoJSS.dll

Simulations

Behavior and APIs

Time	Type	Description
13:07:40	API Interceptor	1x Sleep call for process: rundll32.exe modified
13:08:01	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.97.153.146	5instructio.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	61Documen.exe	Get hash	malicious	Browse	
	65document.exe	Get hash	malicious	Browse	
	29mail98@vip.son.exe	Get hash	malicious	Browse	
	57document.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HHN-efz.ms-acdc.office.com	kZcCqvNtWa.dll	Get hash	malicious	Browse	• 52.98.171.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	A5uTdwOwJ1.dll	Get hash	malicious	Browse	• 40.101.138.210
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 52.98.151.242
	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 52.97.201.34
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.150.2
	8OKQ6ogGRx.dll	Get hash	malicious	Browse	• 40.101.138.2
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2
outlook.com	A1qhcbngFV.exe	Get hash	malicious	Browse	• 104.47.54.36
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.138
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.57.138
	n6osajjc938.exe	Get hash	malicious	Browse	• 104.47.54.36
	9b3d7f02.exe	Get hash	malicious	Browse	• 104.47.54.36
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 52.101.24.0
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 104.47.53.36
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 52.101.24.0
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.W32.AIDetect.malware2.29567.exe	Get hash	malicious	Browse	• 104.47.53.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	lnqNKSyWgz.exe	Get hash	malicious	Browse	• 13.72.107.36
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 157.55.173.72
	DHL_988121.exe	Get hash	malicious	Browse	• 104.43.200.50
	DHL_988121.exe	Get hash	malicious	Browse	• 104.43.200.50
	A1qhcbngFV.exe	Get hash	malicious	Browse	• 20.47.146.252
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 52.97.201.2
	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 40.101.12.82
	iIoO9qC8yj.exe	Get hash	malicious	Browse	• 13.107.4.50
	qLi9sAxeSm.exe	Get hash	malicious	Browse	• 204.95.99.243
	f1a5fbd3e946e8db1c18bd1d30d0f8b41a873cbb76769.exe	Get hash	malicious	Browse	• 20.194.35.6
	tgix.exe	Get hash	malicious	Browse	• 137.117.64.85
	Protiviti.htm	Get hash	malicious	Browse	• 52.240.156.143
	hn80vhR3y1.exe	Get hash	malicious	Browse	• 13.69.222.243
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.161
	SCB_MT103_31951R2105050031_200505.PDF.exe	Get hash	malicious	Browse	• 157.55.136.23
	Windows_Update.exe	Get hash	malicious	Browse	• 20.52.178.148
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 204.79.197.200
	LIau1wwvy5.exe	Get hash	malicious	Browse	• 20.43.33.61
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.37.36
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82
MICROSOFT-CORP-MSN-AS-BLOCKUS	lnqNKSyWgz.exe	Get hash	malicious	Browse	• 13.72.107.36
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 157.55.173.72
	DHL_988121.exe	Get hash	malicious	Browse	• 104.43.200.50
	DHL_988121.exe	Get hash	malicious	Browse	• 104.43.200.50
	A1qhcbngFV.exe	Get hash	malicious	Browse	• 20.47.146.252
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 52.97.201.2
	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 40.101.12.82
	iIoO9qC8yj.exe	Get hash	malicious	Browse	• 13.107.4.50
	qLi9sAxeSm.exe	Get hash	malicious	Browse	• 204.95.99.243
	f1a5fbd3e946e8db1c18bd1d30d0f8b41a873cbb76769.exe	Get hash	malicious	Browse	• 20.194.35.6
	tgix.exe	Get hash	malicious	Browse	• 137.117.64.85
	Protiviti.htm	Get hash	malicious	Browse	• 52.240.156.143
	hn80vhR3y1.exe	Get hash	malicious	Browse	• 13.69.222.243
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.161
	SCB_MT103_31951R2105050031_200505.PDF.exe	Get hash	malicious	Browse	• 157.55.136.23
	Windows_Update.exe	Get hash	malicious	Browse	• 20.52.178.148
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 204.79.197.200
	LIau1wwvy5.exe	Get hash	malicious	Browse	• 20.43.33.61
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.37.36
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12274
Entropy (8bit):	3.760387811626687
Encrypted:	false
SSDEEP:	192:+5WBNis0oXZHNXwRjed+E/u7sOS274ItWco:Z7iqXJNXwRjeh/u7sOX4ItWco
MD5:	65B1A8F8223E4AB018A95B43305BB1C8
SHA1:	48B24682C2E0631A963EB2BEF63ABD6F50ECF4C5
SHA-256:	5C437229DCC881F3B4F37B7BB9B772AADD7AD70D95C1E89E9A451E8C94726565
SHA-512:	B8368FBD391A5E5076D6ECE48C7D72A54678CE7804E745C7F734AD7C0D5F9C950C261ACBAD104FCA66DA226B637B0947043A395E90F4CEE78AD4C4F2FC3B4FA
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.=.1.3.2.6.5.2.9.1.2.7.3.5.2.0.9.7.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.2.9.1.2.7.9.9.5.8.4.6.1.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.c.d.6.1.5.5.3.-.f.7.a.7.-.4.3.9.c.-.9.3.8.2.-.1.4.2.2.2.5.7.3.5.c.3.c.....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.=.4.a.0.1.e.5.c.d.-.5.2.f.7.-.4.a.c.1.-.9.e.d.f.-.3.7.4.b.4.c.7.2.e.6.c.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.b.5.0.-.0.0.0.1.-.0.0.1.b.-.8.f.e.4.-.2.3.d.0.1.e.4.7.d.7.0.1.....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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed May 12 11:07:55 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	59358
Entropy (8bit):	1.9984891529039928
Encrypted:	false
SSDEEP:	192:fMcuApA1pdJOjc9qElfIpsp6Arg76Sn/kc/XOYAg04xG2OFY+GkxMHhrUlnaOuIq:zrA1pbOiPc7NN/r1xOY+GkxMHYaOuJp
MD5:	2DFACEB2A6B8E2DB10FA736DE4498EAC
SHA1:	59577B330853D4007FFD428C7A70100F6373F93E
SHA-256:	DF885B82793B6A37F202AD54154B6CDAC1F386C92701CF861E596B7AC12BAD52
SHA-512:	E48799E4955583C38E32D6BB69659B283872CA62DB27C401B8649FC3B6E5378CEBBEFDD65BF57CD53438DC72A10605644F1EB0FCE533D40726D15876ABB98A1
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....`.....U.....B.....`.....GenuineIntelW.....T.....P.....`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.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):	8290
Entropy (8bit):	3.6921112436173114
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiRjB6dq6YTJ64LZLGgmfTkOS3A+pDB89ba6TsfSmkYm:RrlsNiVB6dq6Y964tagmfTkOS3qa64fs
MD5:	D2AE7D4FC19E3D3F00CB3BBA18716414
SHA1:	F27E57C80022F1AD378735B72957A6A4B05805E4
SHA-256:	A73833AD0DB5A85528DAD79B81C85DB2EC216A26CE6E5E54EE4EFAF76ACD3C37

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	
SHA-512:	EF0D028A7827972648BC05A27D663712021B1B60ADA68BEE39322953D14959E472A79B7929F6DDFA7CCCD49BB5A064FCEB1EBF41BF1A4DA7FA042F844D27016D
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.>.6.9.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.450080143760217
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLtJgtWI96UWSC8BZ78fm8M4JCds9FK+q8/5CA4SrSMd:uITfLH9NSN/4JgwDWMd
MD5:	3A363033BCDA509CC11610F8EAE185F1
SHA1:	78454D6E43EC4DA98F46B02EF181673BCD929E6E
SHA-256:	E9E57C10B891757381366073C1037A28BD36DB3DAB60F99BEE3D2690BC0107EB
SHA-512:	2EEE18A1B383B6EFD63A077EB19D6962376420E14767329925B1C99B8FE4E415A2482D67B9DF1D39FE3FF0744AF5407F6AA97304F6FF5B1CADDB7B3170EB834A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="986178" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4BD5DCDD-B312-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7680840235180313
Encrypted:	false
SSDEEP:	192:rwZPZTw22TwzWTwttTwyifTwVJnzMTwLvd6vbBTwuYpB:rgxilQArz0
MD5:	F75591F98019D2A0608F3FB097EA2F15
SHA1:	4787CAEFE912FB167C6FEB9FE00EEC553BDEA5FC
SHA-256:	EB3FC9C41D9193ED4B8409124C88AF54D920E178F2CF2FBF466CA0CEA4C4A534
SHA-512:	8D9EF494C0885A2E3A489E923F8934839E91B90383DD56785E715EECC13F0170C3696DDFFF0200AEC840505CF2EF538A393BDD870573BBC676F7D75D9C781D8
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4BD5DCDF-B312-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.8524964337535361
Encrypted:	false
SSDEEP:	192:rHZUQs6Skhjl2pWAM0KIRKDDZBRIRKDDZNKD/A:r5d3L9cYVTCKD5CKDvKDo
MD5:	8B7FC14949EEB4934FD6671CDF794B2E
SHA1:	258C482B68B3B6141A58274D970E0B6207DB7ED9
SHA-256:	9EC0132700BAA61FE67AFAFF537B02FE5A31E856547FD0D7528964F4AC7EC3B6
SHA-512:	E29B09803C09DE623B3BB597AF7A4993B948AEE901871C459E6B2A5F024B15313688FBBAD3F181B042C39DBCDE1B9C3321DCDD67D6E696A60BA2854AC11F9C0
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.488012965147007
Encrypted:	false
SSDEEP:	3:oVXUXvcXSdH8JOGXnEXvcSeFUUCn:o9UXEXwqEXES
MD5:	174BE973E6B0C3BD797883F3212802DF
SHA1:	954D60C1360503B14A9E51AB3ACA4BDD2A5C0EB4
SHA-256:	C13A06C3F7825D7230CB567F756CDE4F8CADDE35A8FBED07F36E4688E0432EBA
SHA-512:	2E197883B6869C97B25DF329FFDB17A3AFAFEADF364613E0DB314B3CCFEC53E74658F36F66B605987E48B8BB53CD63B017242DC22228EC2121E56DA6A443470
Malicious:	false
Preview:	[2021/05/12 13:07:54.927] Latest deploy version: ..[2021/05/12 13:07:54.974] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF7EA0309EEFF1F973.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39681
Entropy (8bit):	0.5798862163096153
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+9DhAjxIRKDDZ3IRKDDZjIRKDDZo:kBqoxKAuqR+9DhAjxCKDdCKDRCKD2
MD5:	4B91B3F5A88EEBB6F58712D6DAC44382
SHA1:	3E64372F0900AD52FE1259E702A1F0C2DE8004B0
SHA-256:	E2BA9974330571C2AD06972236C49D39DABF23514931341E6CCD45518C3F1AF4
SHA-512:	DFE874DEB1728240E12D778A374C521AD84BD7FA013D222665EF5E2032540DDB3333CEF9B722C1FEADC4E8077980F9F915517590A628CBCB0F5B4788CB9EBCB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA1436EB82669AF9C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4074938468026375
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loTwP9loTwP9lWTwkci:kBqoITwQTwuTwO
MD5:	A7BD0ABE7B8FC7B1D1EADEC39A42E343
SHA1:	83109B9245E2D070D04B32FA123C9D81EC10F66F
SHA-256:	51542B6CDC943EB6BE14D54417295C84A4FAF1FE953309D01F82ACAC05E59684
SHA-512:	B4B3E3AA2E56352062DDD43124FE1E1E8615C586546498A43346A6A8A27204601F55AA9405F90596767ECDFC2B2845AFE2A2F27CD04EE3953DFF71B1F4DBCE4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.324538219307157
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

General

File name:	nT5pUwoJSS.dll
File size:	478720
MD5:	6fdbd25f7a84da80ee9d8577122c3291
SHA1:	39a52cbc48be934cf953d4699e8a1ea5ff53a5bf
SHA256:	4bf6e9d4067cb905631ddf7452ac571c4ed9800c7eb8fc7e51b688e1154f52e3
SHA512:	935e43b18efb458f246523976f6b71655cf5c4465cddc86e5b91a9acc8e5d77f3bc3d2b0414d9e08114f286afd682cb9364193babaec4cd6b6ca871abf5b79de
SSDEEP:	12288:4Z31u8+a95+CA9lROexg8P7CbxXTTbWA:4Z31P9wr9lROog8W/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C...".J.".J.".J...J.".J.pwJ.".J4mrJ.".J.pqJ.".J.pgJ.".J.p`J.".J...J.".J.".J.#.J.pkJ.".J.pvJ.".J.ppJ.".J.puJ.".JRich.".J.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1041953
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x608B79B0 [Fri Apr 30 03:29:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a2f0d616525ae6c643810961c7d4fdfe

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FC9209ACBD7h
call 00007FC9209B153Ch
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007FC9209ACAC1h
pop ecx
pop ebp
retn 000Ch
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [01073618h+ecx*8]

Instruction
je 00007FC9209ACBE5h
inc ecx
cmp ecx, 2Dh
jc 00007FC9209ACBC3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007FC9209ACBE0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0107361Ch+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007FC9209AE4A6h
test eax, eax
jne 00007FC9209ACBD8h
mov eax, 01073780h
ret
add eax, 08h
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
mov dword ptr [0108B5ACh], eax
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
push dword ptr [0108B5ACh]
call 00007FC9209AE2A6h
pop ecx
test eax, eax
je 00007FC9209ACBE1h
push dword ptr [ebp+08h]
call eax
pop ecx
test eax, eax
je 00007FC9209ACBD7h
xor eax, eax
inc eax
pop ebp
ret
xor eax, eax
pop ebp
ret
mov edi, edi
push esi
push edi
xor esi, esi
mov edi, 0108B5B8h
cmp dword ptr [0107378Ch+esi*8], 01h
jne 00007FC9209ACBF0h

Instruction
lea eax, dword ptr [00000088h+esi*8]

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [C] VS2005 build 50727 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2008 build 21022 • [EXP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x72630	0x6f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x71e64	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8d000	0x3bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0x1544	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x49190	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x70c08	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x49000	0x15c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4732e	0x47400	False	0.745877878289	data	6.57408998047	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x49000	0x2969f	0x29800	False	0.65666768637	data	5.42368765721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x73000	0x1917c	0x1400	False	0.2435546875	data	3.63177828336	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8d000	0x3bc	0x400	False	0.4091796875	data	3.09285651514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0x2588	0x2600	False	0.456106085526	data	4.61056666922	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8d058	0x364	data	English	United States

Imports

DLL	Import
KERNEL32.dll	QueryPerformanceCounter, GetVolumeInformationW, GetSystemTime, GetModuleHandleW, GetVersionExW, OpenProcess, GetDateFormatW, FindResourceW, LockResource, GetLocalTime, HeapCreate, CreateFileW, HeapFree, HeapCompact, HeapAlloc, VirtualProtectEx, GetCurrentDirectoryW, SetConsoleCP, SetConsoleOutputCP, GetStringTypeW, GetStringTypeA, GetLocaleInfoA, LoadLibraryA, GetLastError, HeapReAlloc, RtlUnwind, GetCurrentThreadId, GetCommandLineA, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapDestroy, VirtualFree, VirtualAlloc, Sleep, GetProcAddress, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LCMapStringA, WideCharToMultiByte, MultiByteToWideChar, LCMapStringW, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, RaiseException, HeapSize, SetHandleCount, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount
ole32.dll	CoCreateInstance, CoUninitialize, OleInitialize, OleUninitialize, CoInitialize

DLL	Import
WINSPOOL.DRV	EnumPrintersW, GetPrinterDataW, GetPrinterW, DocumentPropertiesW, OpenPrinterW, ClosePrinter

Exports

Name	Ordinal	Address
Eithernothing	1	0x103a020
Order	2	0x1039f40
Smileschool	3	0x1039b20

Version Infos

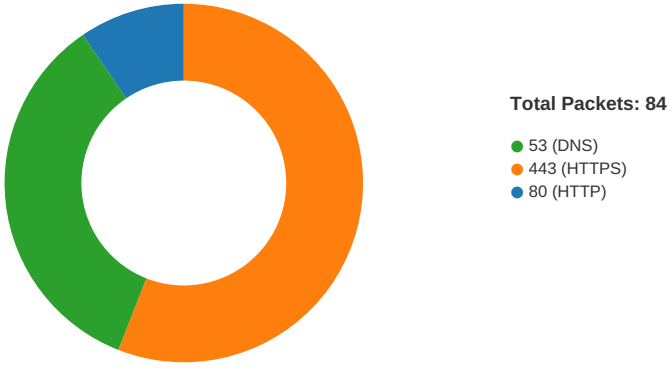
Description	Data
LegalCopyright	Notice sister Corporation. All rights reserved
InternalName	Slow
FileVersion	3.2.1.380
CompanyName	Notice sister Corporation
ProductName	Notice sister Soil read
Observe	38
ProductVersion	3.2.1
FileDescription	Notice sister Soil read Skinneed
OriginalFilename	Tail.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:07:56.524216890 CEST	49753	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.524513006 CEST	49754	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.652859926 CEST	80	49753	40.97.153.146	192.168.2.4
May 12, 2021 13:07:56.653002977 CEST	49753	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.653544903 CEST	80	49754	40.97.153.146	192.168.2.4
May 12, 2021 13:07:56.653630018 CEST	49754	80	192.168.2.4	40.97.153.146

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:07:56.654592991 CEST	49753	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.787769079 CEST	80	49753	40.97.153.146	192.168.2.4
May 12, 2021 13:07:56.788000107 CEST	49753	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.788275957 CEST	49753	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.807976961 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.917027950 CEST	80	49753	40.97.153.146	192.168.2.4
May 12, 2021 13:07:56.939476013 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:56.939598083 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:56.956787109 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.088217020 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.088253975 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.088278055 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.088347912 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.088407993 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.135567904 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.141473055 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.267406940 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.267497063 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.273684978 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.273825884 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.274255991 CEST	49755	443	192.168.2.4	40.97.153.146
May 12, 2021 13:07:57.340895891 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.341072083 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.389771938 CEST	443	49757	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.389811039 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.389878988 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.389921904 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.391278028 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.392539024 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.404428005 CEST	443	49755	40.97.153.146	192.168.2.4
May 12, 2021 13:07:57.440767050 CEST	443	49757	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.440804958 CEST	443	49757	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.440829992 CEST	443	49757	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.440850973 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.440888882 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.441837072 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.441859961 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.441878080 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.441922903 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.441966057 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.456420898 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.456739902 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.457509995 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.507992983 CEST	443	49757	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.508028984 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.508058071 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.508086920 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.508121967 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.510467052 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.510528088 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.511269093 CEST	49756	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:57.559741020 CEST	443	49756	52.97.233.66	192.168.2.4
May 12, 2021 13:07:57.595808029 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.595855951 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.645627022 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.645654917 CEST	443	49758	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.645747900 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.645814896 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.649241924 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.650088072 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.701133013 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701167107 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701189041 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701257944 CEST	49759	443	192.168.2.4	40.101.137.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:07:57.701292038 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.701807976 CEST	443	49758	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701838017 CEST	443	49758	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701862097 CEST	443	49758	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.701891899 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.701932907 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.715931892 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.716289043 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.720307112 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.765304089 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.766113043 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.766210079 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.770592928 CEST	443	49758	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.770699978 CEST	49758	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.794503927 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.794528008 CEST	443	49759	40.101.137.82	192.168.2.4
May 12, 2021 13:07:57.794564962 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:57.794585943 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:58.988245010 CEST	49754	80	192.168.2.4	40.97.153.146
May 12, 2021 13:07:58.988343954 CEST	49759	443	192.168.2.4	40.101.137.82
May 12, 2021 13:07:58.989630938 CEST	49757	443	192.168.2.4	52.97.233.66
May 12, 2021 13:07:58.989656925 CEST	49758	443	192.168.2.4	40.101.137.82

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:06:00.430233955 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:00.479023933 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 13:06:01.537579060 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:01.589147091 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 13:06:01.686364889 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:01.749185085 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 13:06:02.330004930 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:02.381606102 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 13:06:03.079670906 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:03.131386995 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 13:06:03.838140965 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:03.890248060 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:06:05.137980938 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:05.186661959 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 13:06:06.116621017 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:06.165359974 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 13:06:07.012972116 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:07.064455986 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 13:06:59.158689022 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 13:06:59.218735933 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 13:07:13.575684071 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:13.624511003 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 13:07:33.184400082 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:33.233283997 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 13:07:34.089867115 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:34.147365093 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 13:07:35.026246071 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:35.086539030 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 13:07:35.351069927 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:35.401068926 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 13:07:36.008440971 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:36.083830118 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 13:07:37.127737045 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:37.176460028 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 13:07:38.093313932 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:38.143081903 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 13:07:39.032254934 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:39.081478119 CEST	53	51255	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:07:41.426986933 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:41.476294041 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 13:07:42.213614941 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:42.263492107 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 13:07:42.913527966 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:42.973959923 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 13:07:43.147269964 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:43.198693991 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 13:07:44.032737017 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:44.083465099 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 13:07:54.982896090 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:55.040282965 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 13:07:56.442893982 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:56.493007898 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 13:07:57.287398100 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:57.337733984 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 13:07:57.538420916 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 13:07:57.587490082 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 13:08:01.508614063 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 13:08:01.557399988 CEST	53	62420	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 13:07:56.442893982 CEST	192.168.2.4	8.8.8.8	0x4465	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.287398100 CEST	192.168.2.4	8.8.8.8	0x80a2	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.538420916 CEST	192.168.2.4	8.8.8.8	0x4050	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 13:07:35.401068926 CEST	8.8.8.8	192.168.2.4	0x64b5	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 12, 2021 13:07:56.493007898 CEST	8.8.8.8	192.168.2.4	0x4465	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.66	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.98	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.337733984 CEST	8.8.8.8	192.168.2.4	0x80a2	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.82	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.82	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.98	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.18	A (IP address)	IN (0x0001)
May 12, 2021 13:07:57.587490082 CEST	8.8.8.8	192.168.2.4	0x4050	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.18	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- outlook.com

HTTP Packets

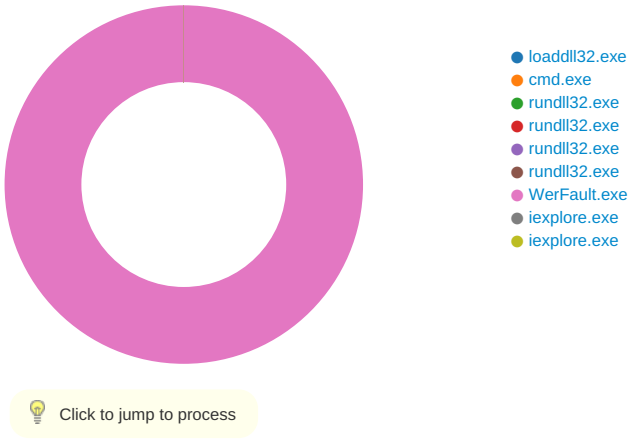
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49753	40.97.153.146	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 13:07:56.654592991 CEST	1552	OUT	GET /login/greed/KnH9H6Qjc_2F7/0e3_2F0_/2FRqQPyOKs18rFK5waVCGCI/jIBCBbgDdF/18TiURZdioL3eU4Wc/SUXArexakZ5d/R0lDxIGeIYj/c6FwtLcTr3EmEj/nbrTM1t_2BdTxREGmfFhs/_2BnTf5cT9dEAnPd/AFLbs3lARk22SMJ/POUz7dti2oyFXHE3_2/FgEVGs1vD/4LhoHpnAxyp/chUrsX.gfk HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: outlook.com Connection: Keep-Alive
May 12, 2021 13:07:56.787769079 CEST	1552	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/login/greed/KnH9H6Qjc_2F7/0e3_2F0_/2FRqQPyOKs18rFK5waVCGCI/jIBCBbgDdF/18TiURZdioL3eU4Wc/SUXArexakZ5d/R0lDxIGeIYj/c6FwtLcTr3EmEj/nbrTM1t_2BdTxREGmfFhs/_2BnTf5cT9dEAnPd/AFLbs3lARk22SMJ/POUz7dti2oyFXHE3_2/FgEVGs1vD/4LhoHpnAxyp/chUrsX.gfk Server: Microsoft-IIS/10.0 request-id: d22bf8f3-ef91-4d9e-851c-4890d74dfbb5 X-FEServer: BN6PR2001CA0017 X-RequestId: 83f746fe-8412-4293-9793-e5f694c948c0 X-Powered-By: ASP.NET X-FEServer: BN6PR2001CA0017 Date: Wed, 12 May 2021 11:07:56 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6924 Parent PID: 6012

General

Start time:	13:06:05
Start date:	12/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll'
Imagebase:	0x190000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6936 Parent PID: 6924

General

Start time:	13:06:06
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6948 Parent PID: 6924

General

Start time:	13:06:06
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Eithernothing
Imagebase:	0x2a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6960 Parent PID: 6936

General

Start time:	13:06:06
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\nT5pUwoJSS.dll',#1
Imagebase:	0x2a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881584954.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881638380.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881444184.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881614039.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881537844.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881689753.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881502007.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.881360850.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6992 Parent PID: 6924

General

Start time:	13:06:10
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Order
Imagebase:	0x2a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7008 Parent PID: 6924

General

Start time:	13:06:14
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nT5pUwoJSS.dll,Smileschool
Imagebase:	0x2a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 64 Parent PID: 6992

General

Start time:	13:07:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6992 -s 892
Imagebase:	0xcf0000
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:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F4E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp	success or wait	1	6F4E497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	success or wait	1	6F4E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	success or wait	1	6F4E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp.xml	success or wait	1	6F4E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A78.tmp.csv	success or wait	1	6F4E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E61.tmp.txt	success or wait	1	6F4E4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 0b b7 9b 60 a4 05 12 00 00 00 00 00	MDMP..... .....`.....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 60 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 50 1b 00 00 a1 b6 9b 60 1e 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	.....U.....B.....`..... ..GenuineIntelW.....T... ....P.....`..... .....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 48 6d 00 00 e2 04 ff ff ff ff b0 01 48 6d 4a 4a 00 00 01 da 00 00 c4 f5 b3 06 35 46 0f 77 23 00 00 00 06 02 01 00 b8 f5 b3 06 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?..+...S...+. ..+.....Hm..........HmJJ...... ....5F.w#...........+.........	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	168	18 19 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 35 46 0f 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 e2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 3e 25 00 00	........................5F.w.. ....>%..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	20	1b 00 00 00 00 60 07 03 00 00 00 00 00 10 00 00 ba 37 00 00	.....`...........7..	success or wait	27	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	4096	88 f6 b3 06 00 00 b4 06 00 40 b3 06 00 00 00 00 00 1e 00 00 00 00 00 00 00 60 07 03 00 00 00 00 50 1b 00 00 18 19 00 00 00 00 00 00 c8 9f 29 03 00 10 06 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.........@..............`.... ..P.............)............ ....p.w.............	success or wait	26	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	4096	1c f9 ab 06 00 00 ac 06 00 40 ab 06 00 00 00 00 00 1e 00 00 00 00 00 00 00 30 07 03 00 00 00 00 50 1b 00 00 38 17 00 00 00 00 00 00 00 00 00 00 00 10 06 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.........@..............0.... ..P...8....................... ....p.w.............	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 a0 79 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 fd f9 02 cc 97 11 77 23 00 00 00 02 02 00 00 a4 fc f9 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+....y.w................... x......w#...........+.........	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	48	18 19 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 60 07 03 00 00 00 00 b4 f5 b3 06 00 00 00 00 4c 0a 00 00 46 68 00 00 cc 02 00 00 3a 33 00 00	....`............ ..L....Fh......:3..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	4	31 00 00 00	1...	success or wait	49	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	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	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	49	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	120	00 00 23 6f 00 00 00 00 00 b0 08 00 9b ad 08 00 8e 34 fa ca f4 24 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 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 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	..#o.............4...$........ ....B.......B?........... ....*............ ..@A.........................	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	34	1c 00 00 00 6e 00 54 00 35 00 70 00 55 00 77 00 6f 00 4a 00 53 00 53 00 2e 00 64 00 6c 00 6c 00 00 00	....n.T.5.p.U.w.o.J.S.S...d.l.l...	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	668	00 00 48 6d 00 00 00 00 00 00 f0 00 00 00 00 00 00 00 ff de 92 60 1c 25 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 90 62 02 00 00 00 00 00 d0 2c 03 00 00 00 00 b9 62 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 29 c2 03 00 00 00 00 00 b7 c6 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 31 1b 00 00 00 00 00 e0 cd 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 17 0f 05 00 00 00 00 00 7e e6 00 35 01 00 00 00 c3 01 62 17 00 00 00 00 61 16 5b 0e 00 00 00 00 91 8e f7 00 00 00 00 00 de ab 00 00 57 d4 00 00 1d a0 05 00 12 eb 0a 00 e0 cd 04 00 fb 7e 15 00 17 0f 05 00 17 31 29 00 1e 48 01 00 a8 5d 13 00 00 00 00 00 15 ef 15 00 ba 35 05	..Hm.....`.%.....Zb ..... .....b..... ,.....b.....)... .....`1..... .....@.....~..5.... ..b.....a.[.....W. .....~.....1)..H.. .]..... .....5.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	12540	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 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	unknown	120	03 00 00 00 f4 00 00 00 08 07 00 00 04 00 00 00 b0 14 00 00 08 08 00 00 0e 00 00 00 24 00 00 00 b8 1c 00 00 05 00 00 00 b4 01 00 00 06 36 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 58 21 00 00 ce c6 00 00 15 00 00 00 ec 01 00 00 dc 1c 00 00 16 00 00 00 98 00 00 00 c8 1e 00 00	....8.....T.....X!	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.". 1...0.". .e.n.c.o.d.i.n.g.=.". U.T.F.-.1.6.".?.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s. i.o.n.>.1.0...0. <./.W.i.n.d.o.w. s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.9.2.<./.P.i.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 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	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 36 00 32 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.0.6.2.2.6.<./.U.p.t.i.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 36 00 31 00 30 00 35 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.6.6.1.0.5.0.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 31 00 32 00 35 00 31 00 33 00 32 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	<.V.i.r.t.u.a.l.S.i.z.e.>.1.6.1.2.5.1.3.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 34 00 36 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.6.8.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 35 00 39 00 39 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.5.9.9.8.9.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 34 00 35 00 36 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.1.4.5.6.5.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.4.1.4.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 31 00 34 00 35 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.1.4.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.0.5.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.8.9.2.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 37 00 37 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.7.7.7.6.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 32 00 35 00 32 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.0.2.5.2.2.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 37 00 37 00 37 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.7.7.7.6.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.2.4.<./.P.i.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 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	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 30 00 32 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.1.0.2.7.0.<./.U.p.t.i.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 31 00 35 00 30 00 33 00 33 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.9.1.5.0.3.3.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 31 00 34 00 36 00 32 00 34 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.9.1.4.6.2.4.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 31 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.1.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 36 00 36 00 33 00 35 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.6.3.5.5.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 36 00 36 00 33 00 31 00 34 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.6.3.1.4.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.6.7.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.6.7.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 30 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 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.0.0.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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 38 00 37 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.7.6.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 35 00 39 00 39 00 32 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.5.9.9.2.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 30 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.0.3.3.2.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 35 00 39 00 39 00 32 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.5.9.9.2.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 76 00 76 00 76 00 61 00 6d 00 6d 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.v.v.v.a.m.m.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 76 00 76 00 61 00 6d 00 6d 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.v.v.v.a.m.m.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 37 00 36 00 36 00 32 00 30 00 37 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.7.6.6.2.0.7.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	70	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 2d 00 30 00 31 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	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.8.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 30 00 37 00 3a 00 35 00 36 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.2.T.1.1.:.0.7.:.5.6.Z.".>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	270	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 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 39 00 39 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 30 00 30 00 33 00 30 00 37 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 30 00 30 00 33 00 30 00 37 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.2.". .P.I.D.=.".6.9.9.2.". .U.p.t.i.m.e.M.S.=.".1.0.0.3.0.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.0.0.3.0.7.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 63 00 64 00 36 00 31 00 35 00 35 00 33 00 2d 00 66 00 37 00 61 00 37 00 2d 00 34 00 33 00 39 00 63 00 2d 00 39 00 33 00 38 00 32 00 2d 00 31 00 34 00 32 00 32 00 32 00 35 00 37 00 33 00 35 00 63 00 33 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.7.c.d.6.1.5.5.3.-.f.7.a.7.-.4.3.9.c.-.9.3.8.2.-.1.4.2.2.2.5.7.3.5.c.3.c.<./.G.u.i.d.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 30 00 37 00 3a 00 35 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.2.T.1.1.:.0.7.:.5.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9808.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A6B.tmp.xml	unknown	4629	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83\Report.wer	unknown	2	ff fe	..	success or wait	1	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	180	6F4E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_002dad83\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 37 00 30 00 38 00 30 00 37 00 36 00 30 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.7.0.8.0.7.6.0.4.	success or wait	1	6F4E497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6F5036BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F501FB2	RegCreateKeyExW
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F4E43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F5036BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6F5036BF	unknown
\REGISTRY\A\{93be86a8-d00e-48f6-25c8-e2ac0f9641e6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6F5036BF	unknown
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 35 46 0F 77 02 00 00 00 00 00 00 00 08 00 E2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6F501FE8	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 5516 Parent PID: 800

General

Start time:	13:07:53
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7fded0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4556 Parent PID: 5516

General

Start time:	13:07:54
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5516 CREDAT:17410 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis