ID: 344595
Sample Name:
SecuriteInfo.com.Trojan.Packed2.42783.14936.6333
Cookbook: default.jbs
Time: 19:14:36
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

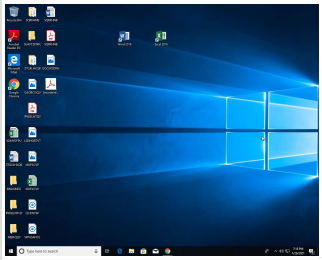
Analysis Report SecuriteInfo.com.Trojan.Packed2.42783…

Overview

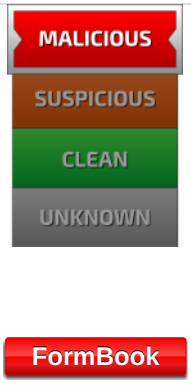
General Information

Sample Name:	SecuriteInfo.com.Trojan.Packed2.42783.14936.6333 (renamed file extension from 6333 to exe)
Analysis ID:	344595
MD5:	25fcc01067cabbf…
SHA1:	9f45d2e8e415ab3.
SHA256:	ba4721d93c056e..

Most interesting Screenshot:



Detection



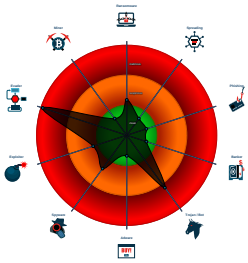
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.Packed2.42783.14936.exe (PID: 5980 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe' MD5: 25FCC01067CABBF5D1AA3A2F8B18ED50)
  - AddInProcess32.exe (PID: 6476 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 3476 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 5992 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 2896 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WerFault.exe (PID: 7108 cmdline: C:\Windows\system32\WerFault.exe -u -p 3424 -s 8832 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- SearchUI.exe (PID: 960 cmdline: 'C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe' -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca MD5: C4A9ACE9CDB9E5DB7CBA996CFA9EA7A2)
- SearchUI.exe (PID: 6652 cmdline: 'C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe' -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca MD5: C4A9ACE9CDB9E5DB7CBA996CFA9EA7A2)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x99bf",
    "KEY1_OFFSET 0x1e3ca",
    "CONFIG SIZE : 0xcd",
    "CONFIG OFFSET 0x1e4d3",
    "URL SIZE : 26",
    "searching string pattern",
    "strings_offset 0x1cfa3",
    "searching hashes pattern",
    "--------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------",
    "0x3a0289d",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
```

```
"0x7d54c891",
"0x47cb721",
"0xf72d719b",
"0x9f715010",
"0xbf0a5e41",
"0x2902d074",
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad011e04",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014b1",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
```

```
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
```

```
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"----------------------------------------------------",
"Decrypted Strings",
"----------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
```

```
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"whatchicken.com",
"sarayatalk.com",
"madammomala.info",
"himizoli.pro",
"korobkapaket.ltda",
"amd-investissement.com",
"southerneclipse2024.com",
"g2vies.com",
"roseyogacoach.com",
"allprounlimted.com",
"medicaresbenefit.com",
"castagno.info",
"showcertificates.com",
"cheapcraftbeer.com",
"roxorsuperstore.info",
"ossierugs.com",
"honeyandtuelle.com",
"wotulove.com",
"infomgt.net",
"pinknadeboutique.com",
"tophamfardy.com",
"henry-app.com",
"power2bank.com",
"estivalconsultancy.com",
"anyagenxy.com",
"woomentrend.com",
"cherishfloraldesign.com",
"euroqq.info",
"techologytestinginc.com",
"jokerwirewheels.com",
"bucklandnewton.net",
"owldrinktothat.com",
"laceystrucking.com",
"englishprotips.com",
"0852qcw.com",
"joebowmanforlafayette.com",
"mystrandnews.com",
"1980vallejo.com",
"miramelfruits.com",
"jollfree.com",
"renttoowngenius.com",
"nepali-rudraksha.com",
"chloeboinnot.com",
"doitimpex.online",
"edu4go.com",
"gvanmp.com",
"furnacerepairtacoma.net",
"myfreecopyright.info",
"listenmelody.com",
"cbothwelltest2020081703.com",
"bblfz.com",
"baanboosakorn.com",
"ancident.com",
"serenityhomedits.com",
"distinctivewearstore.com",
"qianyin1b.com",
"ywf-lishui.com",
"luohu666.com",
"studiocitylandscapedesigner.com",
"thesunchronical.com",
"6obusiness.com",
```

```
    "shortsscape.com",
    "nbgurki.com",
    "smoothsailingexpress.com",
    "f-end",
    "------------------------------------------------",
    "Decrypted CnC URL",
    "------------------------------------------------",
    "www.theprintshop.ink/bsl/\u0000"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\Report.wer	SUSP_WER_Critical_Heap Corruption	Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation)	Florian Roth	• 0xd6:$a1: ReportIdentifier= • 0x158:$a1: ReportIdentifier= • 0x63a:$a2: .Name=Fault Module Name • 0x7e8:$s1: c0000374

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.1027686906.00000000008F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1027686906.00000000008F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 20 entries				

Unpacked PEs

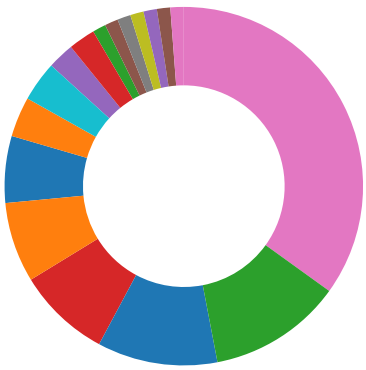
Source	Rule	Description	Author	Strings
1.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
1.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- 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

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

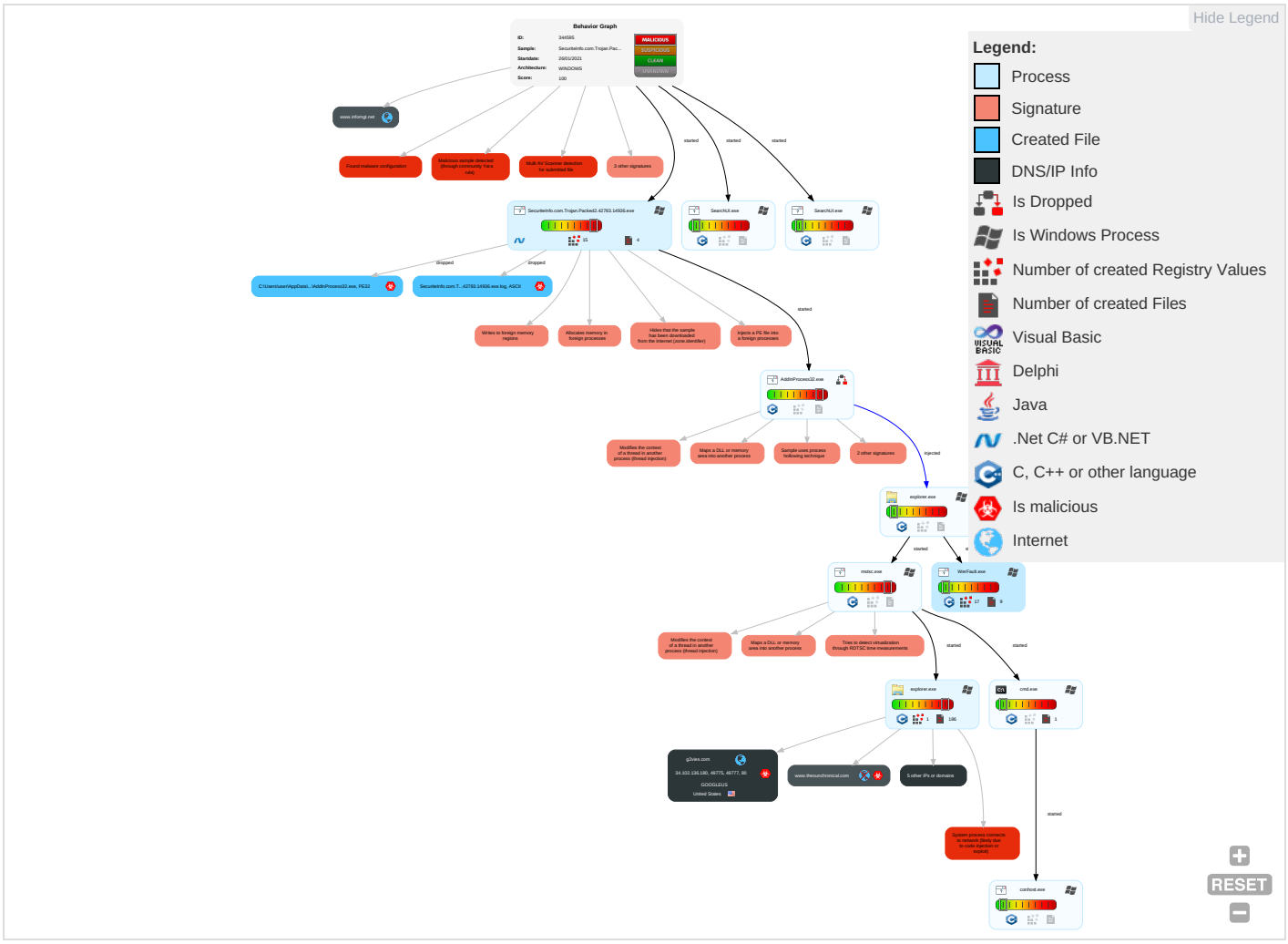
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 2 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress To Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 8 1 2	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicatior Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 5	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicatior Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Disable or Modify Tools 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 8 1 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatior Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transf Protocols

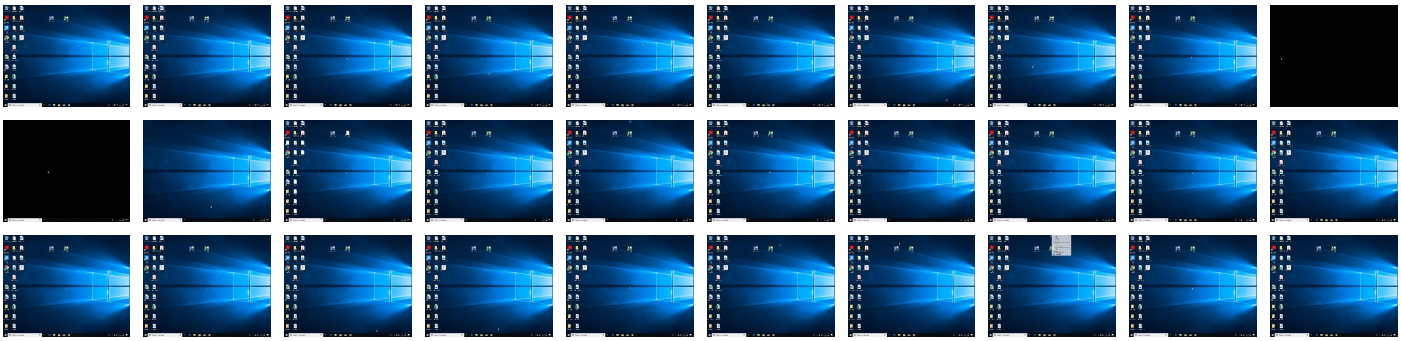
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	29%	Virustotal		Browse
SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.luohu666.comReferer:	0%	Avira URL Cloud	safe	
http://www.g2vies.com	0%	Avira URL Cloud	safe	
http://www.gvanmp.com	0%	Avira URL Cloud	safe	
http://www.listenmelody.comReferer:	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cingr	0%	Avira URL Cloud	safe	
http://www.infomgt.net/bsl/www.renttoowngenius.com	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.edu4go.com/bsl/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://www.whatchicken.comReferer:	0%	Avira URL Cloud	safe	
http://www.theprintshop.ink	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.estivalconsultancy.com/bsl/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ns.adb	0%	Avira URL Cloud	safe	
http://www.infomgt.netReferer:	0%	Avira URL Cloud	safe	
http://www.thesunchronical.com/bsl/	0%	Avira URL Cloud	safe	
http://www.edu4go.com/bsl/www.infomgt.net	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jokerwirewheels.com	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://www.gvanmp.com/bsl/www.whatchicken.com	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://www.whatchicken.com/bsl/www.estivalconsultancy.com	0%	Avira URL Cloud	safe	
http://www.gvanmp.com/bsl/	0%	Avira URL Cloud	safe	
http://www.theprintshop.ink/bsl/www.cbothwelltest2020081703.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.renttoowngenius.com/bsl/www.jokerwirewheels.com	0%	Avira URL Cloud	safe	
http://www.renttoowngenius.comReferer:	0%	Avira URL Cloud	safe	
http://www.thesunchronical.com	0%	Avira URL Cloud	safe	
http://www.edu4go.com/bsl/?mt=meRO04KZ+tRueejEQ1mKApUC+xiZQAGZPTeO6WstMPZoEBgumINoRWRpGBFK3WkMjtLu&2d=hxlpdRkxCvtTgBzP	0%	Avira URL Cloud	safe	
http://www.g2vies.comReferer:	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingrms	0%	Avira URL Cloud	safe	
http://www.g2vies.com/bsl/?2d=hxlpdRkxCvtTgBzP&mt=B72SzM4OK6YheLE+tS6SAH+1fBRAvDBThfWED1RPUqC7thw4cowf+3ukjA/mpLG53kNi	0%	Avira URL Cloud	safe	
http://www.infomgt.net/bsl/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.thesunchronical.com/bsl/www.serenityhomedits.com	0%	Avira URL Cloud	safe	
http://www.cbothwelltest2020081703.com/bsl/	0%	Avira URL Cloud	safe	
http://www.renttoowngenius.com	0%	Avira URL Cloud	safe	
http://www.jokerwirewheels.com/bsl/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.edu4go.com	0%	Avira URL Cloud	safe	
http://https://mths.be/fromcodepoint	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.thesunchronical.comReferer:	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.serenityhomedits.com	0%	Avira URL Cloud	safe	
http://www.estivalconsultancy.com	0%	Avira URL Cloud	safe	
http://https://aefd.nel	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.luohu666.com	0%	Avira URL Cloud	safe	
http://www.estivalconsultancy.com/bsl/www.furnacerepairtacoma.net	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.serenityhomedits.comReferer:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
edu4go.com	34.102.136.180	true	true		unknown
www.infomgt.net	188.166.214.231	true	false		unknown
g2vies.com	34.102.136.180	true	true		unknown
www.g2vies.com	unknown	unknown	true		unknown
www.edu4go.com	unknown	unknown	true		unknown
www.serenityhomedits.com	unknown	unknown	true		unknown
www.thesunchronical.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.edu4go.com/bsl/?mt=meRO04KZ+tRueejEQ1mKApUC+xiZQAGZPTeO6WstMPZoEBgumINoRWRpGBFK3WkMjtLu&2d=hxlpdRkxCvtTgBzP	true	• Avira URL Cloud: safe	unknown
http://www.g2vies.com/bsl/?2d=hxlpdRkxCvtTgBzP&mt=B72SzM4OK6YheLE+tS6SAH+1fBRAvDBThfWED1RPUqC7thw4cowf+3ukjA/mpLG53kNi	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.luohu666.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g2vies.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gvanmp.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.listenmelody.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp, explorer.exe, 00000010.00000002.1047288395.0000 0000063EC000.00000004.00000001 .sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?cingr	SearchUI.exe, 00000016.0000000 2.910509404.000001B8D0EE3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.infomgt.net/bsl/www.renttoowngenius.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000003.682654205.00000000082B2 000.00000004.00000001.sdmp, Se curiteInfo.com.Trojan.Packed2. 42783.14936.exe, 00000000.0000 0003.668183280.00000000082A100 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.edu4go.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000002.683370070.00000000024CF 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.whatchicken.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theprintshop.ink	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000002.683370070.00000000024CF 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://substrate.office.com/api/v2.0/Users(	SearchUI.exe, 00000016.0000000 2.911449678.000001B8D1204000.0 0000004.00000001.sdmp	false		high
http://https://substrate.office.com/profile/v0/users/	SearchUI.exe, 00000016.0000000 2.911449678.000001B8D1204000.0 0000004.00000001.sdmp	false		high
http://www.estivalconsultancy.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000003.682654205.00000000082B2 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.infomgt.netReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thesunchronical.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

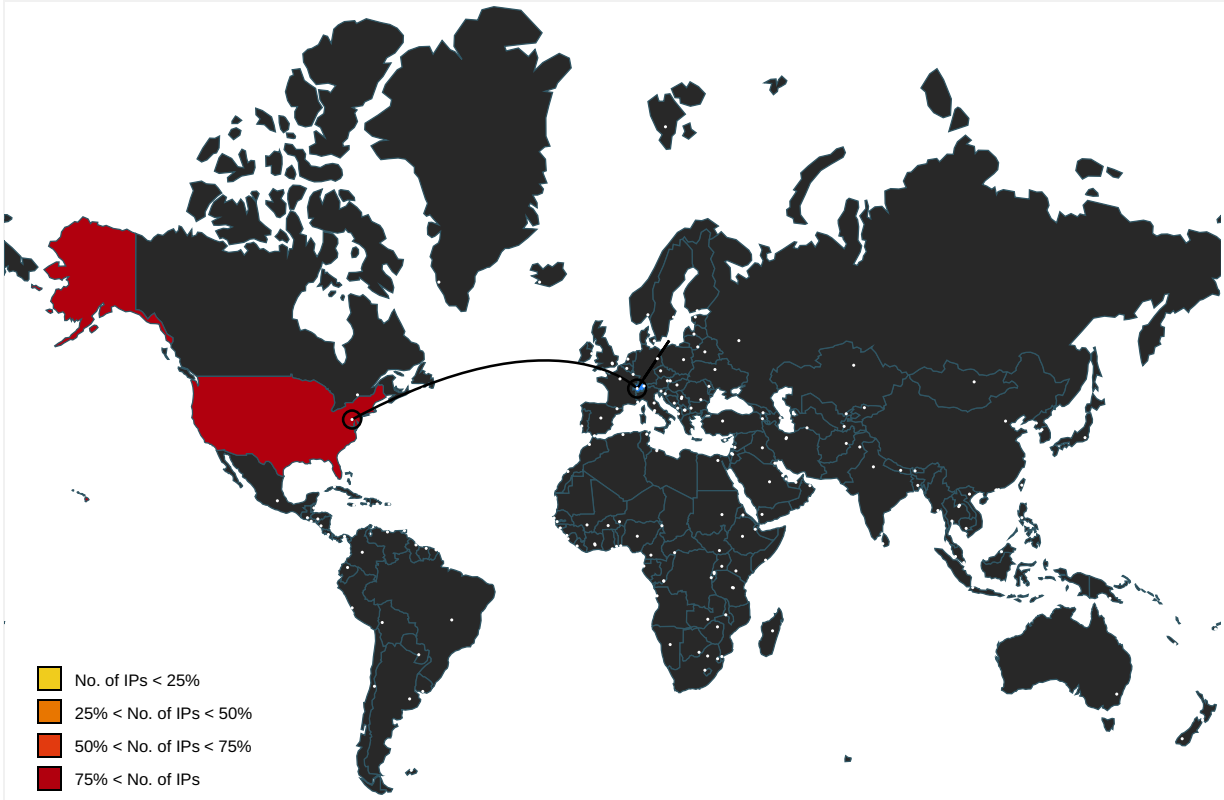
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.edu4go.com/bsl/www.infomgt.net	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000002.683345162.00000000024A1 000.00000004.00000001.sdmp	false		high
http://www.jokerwirewheels.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobj	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000003.682654205.00000000082B2 000.00000004.00000001.sdmp, Se curiteInfo.com.Trojan.Packed2. 42783.14936.exe, 00000000.0000 0003.668183280.00000000082A100 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gvanmp.com/bsl/www.whatchicken.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000002.683370070.00000000024CF 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.whatchicken.com/bsl/www.estivalconsultancy.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gvanmp.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.theprintshop.ink/bsl/www.cbothwelltest2020081703.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://substrate.office.com	SearchUI.exe, 00000016.0000000 2.918398229.000001B8D25E0000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http:// www.renttoowngenius.com/bsl/www.jokerwirewheels.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.renttoowngenius.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thesunchronical.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g2vies.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?cat=bingrms	SearchUI.exe, 00000016.0000000 2.911665172.000001B8D128D000.0 0000004.00000001.sdmp, SearchUI.exe, 00000016.00000003.830851464.00000 1B8D12E5000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.infomgt.net/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.thesunchronical.com/bsl/www.serenityhomedits.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.cbothwelltest2020081703.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.renttoowngenius.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jokerwirewheels.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.edu4go.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mths.be/fromcodepoint	SearchUI.exe, 00000016.0000000 2.915055024.000001B8D1DD1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.thesunchronical.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/	SearchUI.exe, 00000016.0000000 2.911449678.000001B8D1204000.0 0000004.00000001.sdmp	false		high
http://schema.org/WebPage	SecuriteInfo.com.Trojan.Packed 2.42783.14936.exe, 00000000.00 000002.683370070.00000000024CF 000.00000004.00000001.sdmp	false		high
http://www.typography.netD	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.serenityhomedits.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/User.ReadWrite	SearchUI.exe, 00000016.0000000 2.911449678.000001B8D1204000.0 0000004.00000001.sdmp	false		high
http://www.estivalconsultancy.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nel	SearchUI.exe, 00000016.0000000 3.817365227.000001B8D126F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	explorer.exe, 00000002.0000000 2.751926871.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://api.msn.com/news/feed?market=en-us&query=	SearchUI.exe, 00000016.0000000 2.916371805.000001B8D20E0000.0 0000004.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.luohu666.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.estivalconsultancy.com/bsl/www.furnacerepairtacoma.net	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.serenityhomedits.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?c	SearchUI.exe, 00000016.0000000 2.910509404.000001B8D0EE3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g2vies.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g2vies.com/bsl/www.edu4go.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://facebook.github.io/react/docs/error-decoder.html?invariant	SearchUI.exe, 00000016.0000000 2.914254001.000001B8D1BAF000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.cbothwelltest2020081703.com/bsl/www.luohu666.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.infomgt.net	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theprintshop.inkReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.luohu666.com/bsl/www.gvanmp.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cbothwelltest2020081703.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.furnacerepairtacoma.netReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.serenityhomedits.com/bsl/www.g2vies.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theprintshop.ink/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.furnacerepairtacoma.net/bsl/www.listenmelody.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jokerwirewheels.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.whatchicken.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cbothwelltest2020081703.comReferer:	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.whatchicken.com	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.luohu666.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aefd.nelreports.net/api/report?cat=bingaot	SearchUI.exe, 00000016.0000000 3.817365227.000001B8D126F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.furnacerepairtacoma.net	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.704890174.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.serenityhomedits.com/bsl/	explorer.exe, 00000010.0000000 3.893668393.00000000063E8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344595
Start date:	26.01.2021
Start time:	19:14:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Packed2.42783.14936.6333 (renamed file extension from 6333 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
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.troj.evad.winEXE@11/24@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 12.5%) • Quality average: 73.8% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, wermgr.exe, ShellExperienceHost.exe, backgroundTaskHost.exe, svchost.exe, mobsync.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 172.217.23.68, 51.104.144.132, 95.101.22.203, 95.101.22.224, 23.62.99.40, 2.21.243.41, 20.54.26.129, 52.155.217.156, 95.101.22.216, 204.79.197.200, 13.107.21.200, 40.88.32.150, 51.104.139.180, 52.147.198.201 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKey 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 NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:15:40	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.Packed2.42783.14936.exe modified
19:16:20	API Interceptor	695x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• www.worldwide-mt.com/kzd/
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQV/txd+LHV0DSgDXQ==
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.jikzo.com/c8so/?3ff87=Bcwq9mo1SLdxGMzaDRBSbVH3gidTK8xbNEF8M/tGLQ2aKWcuDQCQFtxR7k1oF3yRZXKc&uZWD=XPmPajepJ2gdvnZ
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.simplifiedvirtualsolutions.com/oean/?MdLxlt=mKgmb7I6yODGcWmnOnDfCd0CfDEQGPBdVeZhKsaKMoR3Qh4v4CLN6oxN3p9trG3799qCow==&gnU4Pf=yZPLGZXHl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.kaiyuansu.pro/incn/?9r_PU=-ZQLEn&e2Jdlzf8=4y+UTKzAJ4dBlp/RYYS74WaP+qCjnKVRzK/jF/x906cXBmLcUo8gxmNUvdqUiR1QG2msPA==
	winlog(1).exe	Get hash	malicious	Browse	• www.growingequity.fund/oean/?8pNhXv=yVML0zB0&u4XpH=VZAj6Grbo5w3dBd7w+9BSoe0Fg1VHX3dphJz9/egos9dVzX5qD6mqxE3tlZZ2ImCjS7epxmUBA==
	win32.exe	Get hash	malicious	Browse	• www.findthatsmartphone.com/incn/?8pBP5p=/AA5bjKPiaWw22bzCdt7lqNbxAyyPpv3elVlM12b4Zuyr5w4xH0F6TIfefQNvJyZz9qG&L6Ah=2dSLFXghYtFd0
	1-26.exe	Get hash	malicious	Browse	• www.catalogcardgames.net/bf3/?UXrxP8=0T3HW8l&URfXx=Sdh36sWiaQaHmuW5OuhNg2ZSKBobeXsq4DWTIDdmgtvI732RtscB8O3t4ssmBmGg4ghZ
	Request.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?Rf=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBlvIcl/Xp4fU197lMA==&LDHHp=z4D80PDX
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• www.5050alberta.com/xle/?8pqhs=XuVPlIEgAAku+dXH+MR8cy20ZHkP0iJzlT7lKUj3PYBKa8v0bSmzSfHWFfmBCUSgIWFn2Q==&tDH=XRR8
	RFQ.xlsx	Get hash	malicious	Browse	• www.blacknation.info/c8so/?pBU=HzuD_&gb24XB=6ATEh1s0NdZErsRPIUioXmvz20sSLCkN4f+QHjKAbluYenOJN9FSbPt8XJ2H+dMMf4Jp2Q==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• www.primeoneimplants.com/qjnt/?tB=TtdpPpppFvG&1bwhC=nh3Tl/oLs4HXZ5hiWyD3n36TA5+xQ+CwXb+KxfiJNOta6blp58Sj1H/LHtoCWuUTeWdwKg==
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• www.harperandchloe.com/xle/?5jFlkJJh=FNtvxHF14RtgzuhKSaLd0lIzxL3LkdKZj/Q/Opos8UfLtbug0tkzhu0XdD0TouZ6I/qGUQ==&LR-T=vBK0GdQp
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• www.ctfocbdwholesale.com/bw82/?W6=Rxta6xhtzzdBFDuy4SYKtO8XUaMinJcredo77YczPu8Lep1ecFiaWqXH8h2T5haNROfU&odeTY=cnxhAP6x
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.engageautism.info/bw82/?GFND=n1L9MQk6NEQOasYlfxU4KXziLGivOllQbNtATfsC4RjAZctNbAJfQ2ExV87fcKcU54A&Rlj=YVIX8Hyx
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?Mjklsrcx=4rzgp1jZc7l8Whg0lztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtls6qqwwlb5soGHyjF&Hp0xlh=EVvxc8
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• www.conanbiopharma.com/z9n/?GzuX=Jhwq104eoCBg19EU7i3a/UNFlUD6BU+epYAdz34/Q5fuIRMc24e0hydyrjaAvIdaUf1m&9rspoR=ffn0iZa81
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• www.4thop.com/ur06/?2d=9rm4l4y&nt=yKWvtfxgXgd1h/cfVfwsL+vVHM9GHRLI6tHsLUWr1fII7HM154cThMJKgGXJGqB7HwFq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	560911_P.EXE	Get hash	malicious	Browse	• www.leaguoeofwomengolfers.com/bf3/?2d=8pJhqv2&mt=Rg5SRlzVdqtJGgbKsvZ2Ay09186BQEC1kuNds6zR1M82qUcQWtSjBMIC0cP/+2kk9Xcq

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 216.58.207.179
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 34.102.136.180
	o3Z5sgjhEM.exe	Get hash	malicious	Browse	• 35.186.223.98
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 35.228.108.144
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	winlog(1).exe	Get hash	malicious	Browse	• 34.102.136.180
	win32.exe	Get hash	malicious	Browse	• 34.102.136.180
	DAT.doc	Get hash	malicious	Browse	• 35.200.206.198
	Bestellung.doc	Get hash	malicious	Browse	• 172.217.6.174
	.01.2021a.js	Get hash	malicious	Browse	• 35.228.108.144
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.119.109
	1-26.exe	Get hash	malicious	Browse	• 34.102.136.180
	Request.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RFQ.xlsx	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	SlaZL2LqI2.exe	Get hash	malicious	Browse	
	4NoiNHCNoU.exe	Get hash	malicious	Browse	
	SoPwZKv1Mf.exe	Get hash	malicious	Browse	
	bXFjrxjRlb.exe	Get hash	malicious	Browse	
	Generator.cont.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	560911_P.EXE	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_61779.pdf.exe	Get hash	malicious	Browse	
	IMG_5391.EXE	Get hash	malicious	Browse	
	czZ769nM6r.exe	Get hash	malicious	Browse	
	IMG_1107.EXE	Get hash	malicious	Browse	
	r3q6Bv8naR.exe	Get hash	malicious	Browse	
	sy1RnlHl8Y.exe	Get hash	malicious	Browse	
	qyMlTIBawC.exe	Get hash	malicious	Browse	
	Qn2AQrgfqJ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.28611.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.17348.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.7497.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_12283.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\Report.wer	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	33064
Entropy (8bit):	3.6808226116631357
Encrypted:	false
SSDEEP:	192:hoHaHvSJv6j0PCXmmd1i+cf5PAGXNBttIUMfMgho/u7seS274ltnG:h4yvyv6jbq+cfxAlxtLJ/u7seX4ltnG
MD5:	AE85F99B123BA2CBDD27669B668B8055
SHA1:	E7773B7DF36B519420E9A6B2A2942A21875FED95
SHA-256:	B8053E43545C813CA6A35F8B5E3BE81FFF6BF869DF3EE00BF3874DAA14BBD3E3
SHA-512:	BBC95698F34C9E259940E9203AAD36E35904AFC53B58208E60DD65DC9456DCDD6A555F90445AD55577E1D98D799508233E6222ABCD9CBD9566FF77207058A9A
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Critical_HeapCorruption, Description: Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation), Source: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\Report.wer, Author: Florian Roth
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.1.5.8.5.6.7.4.0.0.6.2.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.F.l.a.g.s.=.5.2.4.2.8.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.6.2.c.1.1.3.b.-.5.a.8.6.-.4.4.8.e.-.b.7.c.0.-.0.0.7.3.8.d.3.8.4.d.2.f.....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.=.5.f.c.c.7.2.2.3.-.4.2.4.5.-.4.8.3.6.-.b.4.e.f.-.0.4.d.c.9.6.b.f.2.6.0.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.E.x.p.l.o.r.e.r...E.X.E.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.E.X.P.L.O.R.E.R...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.6.0.-.0.0.0.1.-.0.0.1.b.-.7.5.e.3.-.e.6.d.5.f.e.f.3.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.f.5.d.0.2.9.9.1.4.0.c.f.9.8.8.7.5.b.0.7.d.b.d.2.d.8.9.2.6.1.7.4.0.1.d.a.d.8.b.9.!.e.x.p.l.o.r.e.r...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.0.5././.0.4././.1.2.:.0.2.:.2.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10546
Entropy (8bit):	3.7121189576874825
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7JR6YtTQ3ikLgmfqK8ShM+prp89bZxs7ng+ycfSzm:RrlsNilR6Y63iIgmfqK8SQZa7ng+ycfv
MD5:	E8578A0AF29B8FC7A703230F563297CD
SHA1:	2617A69C062282248FCE2F8BAAEA3F719BE38D24
SHA-256:	31F5F78290119F7F9E386184F7EDB83D677C22ABE647BE23A1E41E323B77AC9F
SHA-512:	0E79798D9371E940C52B089E2735BC52F365361DF0014919EE5F49C45D4441C479F34B4A142FF79031E4F53C31897053A3D8D06E360646631871343l5AC8C3F8
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.4.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4745
Entropy (8bit):	4.5179008550026465
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxRJgtBI9I+WSC8BT78fm8M4JlNlQ6FOuXyq85klVQn0qAQd:uITfRG/SNyJL3bc0qAQd
MD5:	FBE9AC3A4C00E6E76CDFC0B54BA7B7FF
SHA1:	94DC25D55E846A621BAC74782EB2732E57373878
SHA-256:	87A156E368D306BAA669A33E1DDF37D02CF23118E6A15859D8FCB71817145653
SHA-512:	44E797951F90F3A78BD795C0463FB29F89B1AB2DEB4CB2ECFBD815C5F127D3F0F83566E2511040141D5C2FA48B7666559087D369CBCDDFDFF472046CE39C740
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="833966" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 16 streams, Tue Jan 26 18:16:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1079338
Entropy (8bit):	1.3827411222548762
Encrypted:	false
SSDEEP:	1536:Nu1mqjmEwmQy0CVdPze+HbtmFXdjiM06uGDBPLudUHKrndxpdigCj6Mw6P:5hmQxCLPze+7IdjiMxxud0PV
MD5:	80EA4A10004616EE730CCD4396A810E1
SHA1:	CB9BC12B2D4EE4025CD3D330F7874ACBD682B614
SHA-256:	7138CAD36DB6FA5CF892E655D09C279DFAABF4D25F102F83B6B84646AAD92576
SHA-512:	1249B5A014E2D17C2347A6F38C7A1E224959D87C0CD9185A0D13874E0BEB001C577E213298D7F2B14D7547D9B64531D8B3AF8FE464C2E98F9665FF153604835A
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....i\.`.....U.....B.....}.....Lw.....T.....`....@.`.....0.....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...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..... ....d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtIxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:5l:7
MD5:	2DD3F3C33E7100EC0D4DBBCA9774B044
SHA1:	B254D47F2B9769F13B033CAE2B0571D68D42E5EB
SHA-256:	5A00CC998E0D0285B729964AFD20618CBAECFA7791FECDB843B535491A83AE21
SHA-512:	C719D8C54A3A749A41B8FC430405DB7FCDE829C150F27C89015793CA06018AD9D6833F20AB7E0CFDA99E16322B52A19C080E8C618F996FC8923488819E6E14B
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.408222675578688
Encrypted:	false
SSDEEP:	3:d:d
MD5:	419A089E66B9E18ADA06C459B000CB4D
SHA1:	ED2108A58BA73AC18C3D2BF0D8C1890C2632B05A
SHA-256:	C48E42E9AB4E25B92C43A7B0416D463B9FF7C69541E4623A39513BC98085F424
SHA-512:	BBD57BEA7159748E1B13B3E459E2C8691A46BDC9323AFDB9DBF9D8F09511750D46A1D98C717C7ADCA07D79EDC859E925476DD03231507F37F45775C0A79A59 C
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1920.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:A/lll:A/
MD5:	635E15CB045FF4CF0E6A31C827225767
SHA1:	F1EAAA628678441481309261FABC9D155C0DD6CB
SHA-256:	67219E5AD98A31E8FA8593323CD2024C1CA54D65985D895E8830AE356C7BDF1D
SHA-512:	81172AE72153B24391C19556982A316E16E638F5322B11569D76B28E154250D0D2F31E83E9E832180E34ADD0D63B24D36DD8A0CEE80E8B46D96639BFF811FA58
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:7/lll:x
MD5:	F6B463BE7B50F3CC5D911B76002A6B36
SHA1:	C94920D1E0207B0F53D623A96F48D635314924D2
SHA-256:	16E4D1B41517B48CE562349E3895013C6D6A0DF4FCFFC2DA752498E33C4D9078
SHA-512:	4D155DFEDD3D44EDFBBE7AC84D3E81141D4BB665399C2A5CF01605C24BD12E6FAF87BB5B666EA392E1B246005DFABDE2208ED515CD612D34BAC7F965FD6C 57E
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_2560.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:lX:1
MD5:	2D84AD5CFDF57BD4E3656BCFD9A864EA
SHA1:	B7B82E72891E16D837A54F94960F9B3C83DC5552
SHA-256:	D241584A3FD4A91976FAFD5EC427E88F6E60998954DEC39E388AF88316AF3552
SHA-512:	0D9BC1EE51A4FB91B24E37F85AFBF88376C88345483D686C6CFF84066544287C98534AA701D7D4D52E53F10A3BEA73EE8BC38D18425FDE6D66352F8B76C0CBE
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:2/l/:S/
MD5:	60476A101249AEDFF09A43E047040191
SHA1:	DE5B6A0ADC7DE7180E19286CF0F13567278CDB64
SHA-256:	35BC77A06BFDDE8C8F3A474C88520262B88C7B8992EE6B2D5CF41DDDC77A83FB
SHA-512:	F1D2DCC562A36434C6C6405EC4EAC7ECFA76FC5A940114DA6F94495B77584A132D5D82AD3556DF749490BE096CFD238FA8B484B7C734CBC4D074E963E5D451 4
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:3X:n
MD5:	AE6FBDED57F9F7D048B95468DDEE47CA
SHA1:	C4473EA845BE2FB5D28A61EFD72F19D74D5FC82E
SHA-256:	D3C9D1FF7B54B653C6A1125CAC49F52070338A2DD271817BBA8853E99C0F33A9
SHA-512:	F119D5AD9162F0F5D376E03A9EA15E30658780E18DD86E81812DDA8DDF59ADDD1DAA0706B2F5486DF8F17429C2C60AA05D4F041A2082FD2EC6EA8CC9469FAE E3
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_768.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:Wtl:WX
MD5:	D192F7C343602D02E3E020807707006E
SHA1:	82259C6CB5B1F31CC2079A083BC93C726BFC4FBF
SHA-256:	BB4D233C90BDBEE6EF83E40BFF1149EA884EFA790B3BEF496164DF6F90297C48
SHA-512:	AEC90CF52646B5B0EF00CEB2A8D739BEFE456D08551C031E8DEC6E1F549A6535C1870ADB62EEC0A292787AE6A7876388DD1B2C884CBA8CC6E2D7993790102F 43
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:s:s
MD5:	2A8875D2AF46255DB8324AAD9687D0B7
SHA1:	7A066FA7B69FB5450C26A1718B79AD27A9021CA9
SHA-256:	54097CCCAE0CFCE5608466BA5A5CA2A3DFEAC536964EEC532540F3B837F5A7C7
SHA-512:	2C39F05A4DFFD30800BB7FBB3FF2018CF4CC96398460B7492F05CE6AFD59079FD6E3EB7C4F8384A35A954A22B4934C162A38534AD76CFB2FD772BCF10E211F7
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_custom_stream.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:a/l/:e/
MD5:	F732BF1006B6529CFFBA2B9F50C4B07F
SHA1:	D3E8D4AF812BBC4F4013C53C4FFAB992D1D714E3
SHA-256:	77739084A27CB320F208AC1927D3D9C3CAC42748DBDF6229684EF18352D95067
SHA-512:	064D56217AEB2980A3BFAA1E252404613624D600C3A08B5CF0ADCB259596A1C60EE903FDC2650972785E5AE9B7B51890DED01EC4DA7B4DE94EBDA08AEAF662DF
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_exif.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:EX:EX
MD5:	FC94FE7BD3975E75CEFAD79F5908F7B3
SHA1:	78E7DA8D08E8898E956521D3B1BABBF6524E1DCA
SHA-256:	EE1ED3B49720B22D5FDA63D3C46D62A96CA8838C76AB2D2F580B1E7745521AA5
SHA-512:	4CEAF9021B30734F4CE8B4D4A057539472E68C0ADD199CF9C3D1C1C95320DA3884CAF46943FC9F7281607AB7FA6476027860EBED8BBAA9C44B3F4056B5E074D3
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	7416
Entropy (8bit):	0.018369280867001292
Encrypted:	false
SSDEEP:	3:tn1lllt:y
MD5:	C481876E5724DACEEA95544E8D8464B3
SHA1:	AC446C8AE756FF79632A6CDA049A63F753332967
SHA-256:	74D44331B0E0AD282D34B5667F454B593769AB5E24FE00E80975E688939F3792
SHA-512:	788F79C7AFE4D4AC8B37D34753CF9AC290908C87260DF176CFE07DABE8F95E3F686F725485E1F9238719E2DA9810D2E8D1D364636CAC729EC584EC0E7058A22
Malicious:	false
Preview:	..0 IMMM .....e..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:6:6
MD5:	379523B9F5D5B954E719B664846DBF8F
SHA1:	930823EC80B85EDD22BAF555CAD21CDF48F066AA
SHA-256:	3C9002CAEDF0C007134A7E632C72588945A4892B6D7AD3977224A6A5A7457BF4
SHA-512:	ECA44DE86BBC3309FA6EAB400154D123DCD97DC1DB79554CE58CE2426854197E2365F5EEE42BAC6E6E9455561B206F592E159EF82FAF229212864894E6021E9
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:V/l/:/
MD5:	5F243BF7CC0A348B6D31460A91173E71
SHA1:	5696B34625F027EC01765FC2BE49EFCFD882BF8E
SHA-256:	1B1AED169F2ACFAE4CF230701BDA91229CB582FF2CE29A413C5B8FE3B890D289
SHA-512:	9E08DFBBF20668B86DF696A0D5969E04E6EE4A67E997FF392099BC7FF184B1B8965502215744BE7FE423668B69099242BBA54DF3F0BFE4E70ACDC7CAD8195B0
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide_alternate.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.6368421881310118
Encrypted:	false
SSDEEP:	3:J:J
MD5:	DB7C049E5E4E336D76D5A744C28C54C8
SHA1:	A4DB9C8586B9E4FA24416EB0D00F06A9EBD16B02
SHA-256:	E8830E7AC4088CF3DD464CAEC33A0035D966A7DE5AE4EFC3580D59A41916FF7B
SHA-512:	B614037FB1C7D19D704BF15F355672114D25080223E7EE4424AD2CB7B89782219E7877B373BBC7FA44F3AD8DF8A27EEF4E8CCC765D44EC02A61E3B7FAE88AE6 9
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache132561585936642615.txt.~tmp	
Process:	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	113942
Entropy (8bit):	5.192679852203261
Encrypted:	false
SSDEEP:	384:f/Y1U/gT2/Hb/jn/WI/Zk/Ey/eX/NV/CzS/1o/Yd/e6/Wo/ie/L//6Ij/kh2oO/a:izrotYW9Nmri84qgA
MD5:	C0F583E4B7E550A2C45110DF648535C7
SHA1:	23FD5D6DC6FAD4EFE6C8D230BEE44A94B3C0AE22
SHA-256:	ADC27844BB5ECDB42F3614E3F347BFFDBBC95670E96139F35F872F0EEFF6D48A
SHA-512:	5A2F2ACAD92A97DA3EDBFE0E26A78E6EA6FF91CA64BEE73DD75F8A1746D65CD26C461396A0B61D33685CCC8E601C41CA145036ACF668703C35013F081915F0 8
Malicious:	false
Preview:	[{"System.FileExtension":{"Value":".exe","Type":12},"System.Software.ProductVersion":{"Value":"N/A","Type":12},"System.Kind":{"Value":"program","Type":12},"System.ParsingName":{"Value":"Chrome","Type":12},"System.Software.TimesUsed":{"Value":2,"Type":5},"System.Tile.Background":{"Value":4284441448,"Type":5},"System.AppUserModel.PackageFullName":{"Value":"N/A","Type":12},"System.Identity":{"Value":"N/A","Type":12},"System.FileName":{"Value":"chrome","Type":12},"System.ConnectedSearch.JumpList":{"Value":"[]","Type":12},"System.ConnectedSearch.VoiceCommandExamples":{"Value":"[]","Type":12},"System.ItemType":{"Value":"Desktop","Type":12},"System.DateAccessed":{"Value":1.324592461032E+17,"Type":14},"System.Tile.EncodedTargetPath":{"Value":"{6D809377-6AF0-444B-8957-A3773F02200E}\\Google\\Chrome\\Application\\chrome.exe","Type":12},"System.Tile.SmallLogoPath":{"Value":"N/A","Type":12},"System.ItemNameDisplay":{"Value":"Google Chrome","Type":12}},{"System.FileExtension":{"Value":".com/","Type"

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\TempState\Traces\CortanaTrace1.etl	
Process:	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
File Type:	Targa image data - Map 65536 x 65536 x 0
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.12612858904227983
Encrypted:	false
SSDEEP:	12:GqKVXZ/EyM2xX/7EHIJY6iK8tJRKQ1UMCl2rjoD7CePglyDQqmU9:GqKblbWMY6iKUJ9SMClCjoHCeIyjb
MD5:	AA5171A81CD83B2A43E07991ED2DD12A
SHA1:	D31D9647C43692172CD69816A8E302A5C90C8B67
SHA-256:	60E8DBC665930E28464E6023919CE1C3D1042690E1F4C35443136541BFAF4EA9
SHA-512:	02D1732A4087C742764A444186BE904A6B2F27327A5586443D3528778CDBD242DF3D06747F109CF3A2BB627F6DDEE9F0F6D91E47858AF0C761ACF235848DB72A

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\TempState\Traces\CortanaTrace1.etl	
Malicious:	false
Preview:	.....d.....W.f.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.3.2.2..... .....@.t.z.r.e.s...d.l.l.,-.3.2.1.....*..... .....W.f.....C.7.C.B.3.E.B.D.-.9.9.8.4.-.4.2.9.F.-.A.4.2.8.-.B.6.E.5.1.2.5.8.A.0.B.5...C.: .\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.a.c.k.a.g.e.s.\.M.i.c.r.o.s.o.f.t...W.i.n.d.o.w.s...C.o.r.t.a.n.a._.c.w.5.n.1.h.2.t.x.y.e.w.y.\.T.e.m.p.S.t.a.t.e.\.T.r.a.c.e.s.\.C.o .r.t.a.n.a.T.r.a.c.e.1...e.t.l.....P.P.....9p..... .....

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SlaZL2LqI2.exe, Detection: malicious, Browse • Filename: 4NoiNHCNoU.exe, Detection: malicious, Browse • Filename: SoPwZKv1Mf.exe, Detection: malicious, Browse • Filename: bXFjrxjRlb.exe, Detection: malicious, Browse • Filename: Generator.cont.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: 560911_P.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_61779.pdf.exe, Detection: malicious, Browse • Filename: IMG_5391.EXE, Detection: malicious, Browse • Filename: czZ769nM6r.exe, Detection: malicious, Browse • Filename: IMG_1107.EXE, Detection: malicious, Browse • Filename: r3q6Bv8naR.exe, Detection: malicious, Browse • Filename: sy1RnlHl8Y.exe, Detection: malicious, Browse • Filename: qyMlTIBawC.exe, Detection: malicious, Browse • Filename: Qn2AQrgfqJ.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.28611.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.17348.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.7497.exe, Detection: malicious, Browse • Filename: IMG_12283.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.628782115819407
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe
File size:	775168
MD5:	25fcc01067cabbf5d1aa3a2f8b18ed50
SHA1:	9f45d2e8e415ab38f42e4edb9b503ce82fed2402
SHA256:	ba4721d93c056ef1763667732344fdc82066d71f0003e18ad03f6d93307b82fe

General

SHA512:	6bb9a73bfec5a0cb20b16ecaae7d31ef5c8a069d83466b1 247046e766204fedd9d8fe86d59856fe143498e27791594 494131e31a7d0fea7fe1a16de05ea12a94
SSDEEP:	12288:27r001HnHfNbxp+pPnGUw2DargRxEc3kstvo:Ur 00n/mfM/8HUY
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L...9 .q*.....................J........... ....@.. ....@......... ...`................................

File Icon

	
Icon Hash:	8aeeae8e96a2d0d6

Static PE Info

General

Entrypoint:	0x4ba6fe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x2A71AA39 [Sat Jul 25 19:23:37 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xba6b0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x46e6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb8704	0xb8800	False	0.55824705708	data	5.61495245399	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x46e6	0x4800	False	0.153917100694	data	2.48496463764	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc130	0x4028	data		
RT_GROUP_ICON	0xc0158	0x14	data		
RT_VERSION	0xc016c	0x390	data		
RT_MANIFEST	0xc04fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2003 4IJ<EF<2H2?B5?<65J5
Assembly Version	1.0.0.0
InternalName	IMG_4785.exe
FileVersion	4.7.9.11
CompanyName	4IJ<EF<2H2?B5?<65J5
Comments	AE6B@7::I5B26:CFAD:

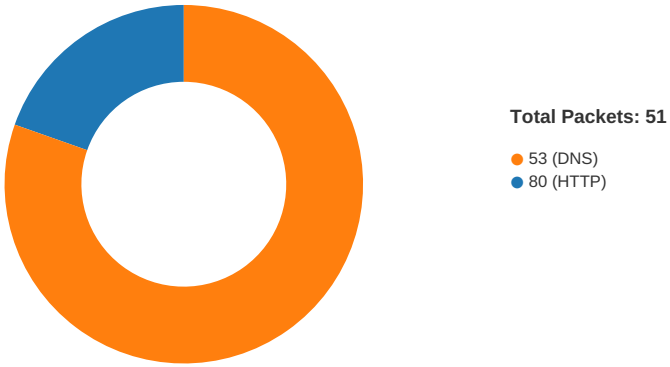
Description	Data
ProductName	5DC7?JD?CD=C<8::@2I
ProductVersion	4.7.9.11
FileDescription	5DC7?JD?CD=C<8::@2I
OriginalFilename	IMG_4785.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-19:17:56.119248	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49775	34.102.136.180	192.168.2.4
01/26/21-19:18:16.574495	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49777	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:17:55.940206051 CET	49775	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:17:55.980139971 CET	80	49775	34.102.136.180	192.168.2.4
Jan 26, 2021 19:17:55.980253935 CET	49775	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:17:55.980583906 CET	49775	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:17:56.020441055 CET	80	49775	34.102.136.180	192.168.2.4
Jan 26, 2021 19:17:56.119247913 CET	80	49775	34.102.136.180	192.168.2.4
Jan 26, 2021 19:17:56.119296074 CET	80	49775	34.102.136.180	192.168.2.4
Jan 26, 2021 19:17:56.119566917 CET	49775	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:17:56.119647026 CET	49775	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:17:56.159765959 CET	80	49775	34.102.136.180	192.168.2.4
Jan 26, 2021 19:18:16.393987894 CET	49777	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:18:16.435101986 CET	80	49777	34.102.136.180	192.168.2.4
Jan 26, 2021 19:18:16.435297966 CET	49777	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:18:16.435353041 CET	49777	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:18:16.476150036 CET	80	49777	34.102.136.180	192.168.2.4
Jan 26, 2021 19:18:16.574495077 CET	80	49777	34.102.136.180	192.168.2.4
Jan 26, 2021 19:18:16.574590921 CET	80	49777	34.102.136.180	192.168.2.4
Jan 26, 2021 19:18:16.574881077 CET	49777	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:18:16.574917078 CET	49777	80	192.168.2.4	34.102.136.180
Jan 26, 2021 19:18:16.615082026 CET	80	49777	34.102.136.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:15:27.024445057 CET	63153	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:27.081223965 CET	53	63153	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:28.005300045 CET	52991	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:28.055263042 CET	53	52991	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:28.874692917 CET	53700	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:28.923250914 CET	53	53700	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:29.776381969 CET	51726	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:29.824234009 CET	53	51726	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:30.749382973 CET	56794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:30.797584057 CET	53	56794	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:31.740092039 CET	56534	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:31.787905931 CET	53	56534	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:32.632246017 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:32.684386969 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:32.696290016 CET	56621	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:32.747148037 CET	53	56621	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:33.686146975 CET	63116	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:33.734003067 CET	53	63116	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:34.584127903 CET	64078	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:34.635238886 CET	53	64078	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:35.543693066 CET	64801	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:35.595021009 CET	53	64801	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:36.322415113 CET	61721	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:36.370259047 CET	53	61721	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:37.251609087 CET	51255	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:37.302993059 CET	53	51255	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:51.065363884 CET	61522	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:51.116044044 CET	53	61522	8.8.8.8	192.168.2.4
Jan 26, 2021 19:15:57.363372087 CET	52337	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:15:57.423877001 CET	53	52337	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:14.392684937 CET	55046	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:14.440687895 CET	53	55046	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:16.078816891 CET	49612	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:16.137025118 CET	53	49612	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:19.638396978 CET	49285	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:19.702785969 CET	53	49285	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:20.697467089 CET	50601	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:20.773297071 CET	53	50601	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:21.516798019 CET	60875	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:21.576582909 CET	53	60875	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:22.527643919 CET	56448	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:22.587239027 CET	53	56448	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:24.613257885 CET	59172	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:24.664139986 CET	53	59172	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:25.417870045 CET	62420	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:25.474555016 CET	53	62420	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:26.287581921 CET	60579	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:26.348815918 CET	53	60579	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:27.186872005 CET	50183	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:27.245357037 CET	53	50183	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:28.412652969 CET	61531	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:28.463732958 CET	53	61531	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:30.456523895 CET	49228	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:30.521622896 CET	53	49228	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:31.110861063 CET	59794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:31.169318914 CET	53	59794	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:32.605475903 CET	55916	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:32.665482044 CET	53	55916	8.8.8.8	192.168.2.4
Jan 26, 2021 19:16:43.212677002 CET	52752	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:16:43.263365030 CET	53	52752	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:11.886284113 CET	60542	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:11.937151909 CET	53	60542	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:20.125094891 CET	60689	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:20.197899103 CET	53	60689	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 19:17:20.284976959 CET	64206	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:20.334652901 CET	53	64206	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:33.544280052 CET	50904	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:33.613106966 CET	53	50904	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:46.438988924 CET	57525	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:46.487060070 CET	53	57525	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:53.906111956 CET	53814	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:53.976504087 CET	53	53814	8.8.8.8	192.168.2.4
Jan 26, 2021 19:17:55.874610901 CET	53418	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:17:55.935830116 CET	53	53418	8.8.8.8	192.168.2.4
Jan 26, 2021 19:18:02.336050034 CET	62833	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:18:02.385848999 CET	53	62833	8.8.8.8	192.168.2.4
Jan 26, 2021 19:18:16.327147961 CET	59260	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:18:16.391833067 CET	53	59260	8.8.8.8	192.168.2.4
Jan 26, 2021 19:18:29.608736992 CET	49944	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:18:29.656579971 CET	53	49944	8.8.8.8	192.168.2.4
Jan 26, 2021 19:18:36.704664946 CET	63300	53	192.168.2.4	8.8.8.8
Jan 26, 2021 19:18:36.765784025 CET	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 19:17:20.125094891 CET	192.168.2.4	8.8.8.8	0x5a89	Standard query (0)	www.thesun chronical.com	A (IP address)	IN (0x0001)
Jan 26, 2021 19:17:33.544280052 CET	192.168.2.4	8.8.8.8	0x10be	Standard query (0)	www.sereni tyhomedits.com	A (IP address)	IN (0x0001)
Jan 26, 2021 19:17:55.874610901 CET	192.168.2.4	8.8.8.8	0x2879	Standard query (0)	www.g2vies.com	A (IP address)	IN (0x0001)
Jan 26, 2021 19:18:16.327147961 CET	192.168.2.4	8.8.8.8	0x706c	Standard query (0)	www.edu4go.com	A (IP address)	IN (0x0001)
Jan 26, 2021 19:18:36.704664946 CET	192.168.2.4	8.8.8.8	0xd061	Standard query (0)	www.infomgt.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 19:17:20.197899103 CET	8.8.8.8	192.168.2.4	0x5a89	Name error (3)	www.thesun chronical.com	none	none	A (IP address)	IN (0x0001)
Jan 26, 2021 19:17:33.613106966 CET	8.8.8.8	192.168.2.4	0x10be	Name error (3)	www.sereni tyhomedits.com	none	none	A (IP address)	IN (0x0001)
Jan 26, 2021 19:17:55.935830116 CET	8.8.8.8	192.168.2.4	0x2879	No error (0)	www.g2vies.com	g2vies.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 19:17:55.935830116 CET	8.8.8.8	192.168.2.4	0x2879	No error (0)	g2vies.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 26, 2021 19:18:16.391833067 CET	8.8.8.8	192.168.2.4	0x706c	No error (0)	www.edu4go .com	edu4go.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 19:18:16.391833067 CET	8.8.8.8	192.168.2.4	0x706c	No error (0)	edu4go.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 26, 2021 19:18:36.765784025 CET	8.8.8.8	192.168.2.4	0xd061	No error (0)	www.infomgt.net		188.166.214.231	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.g2vies.com
- www.edu4go.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49775	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 19:17:55.980583906 CET	5680	OUT	GET /bsl/?2d=hxlpdRkxCvtTgBzP&mt=B72SzM4OK6YheLE+tS6SAH+1fBRAvDBThfWED1RPUqC7thw4cowf+3ukjA/mpLG53kNi HTTP/1.1 Host: www.g2vies.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 19:17:56.119247913 CET	5681	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 26 Jan 2021 18:17:56 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

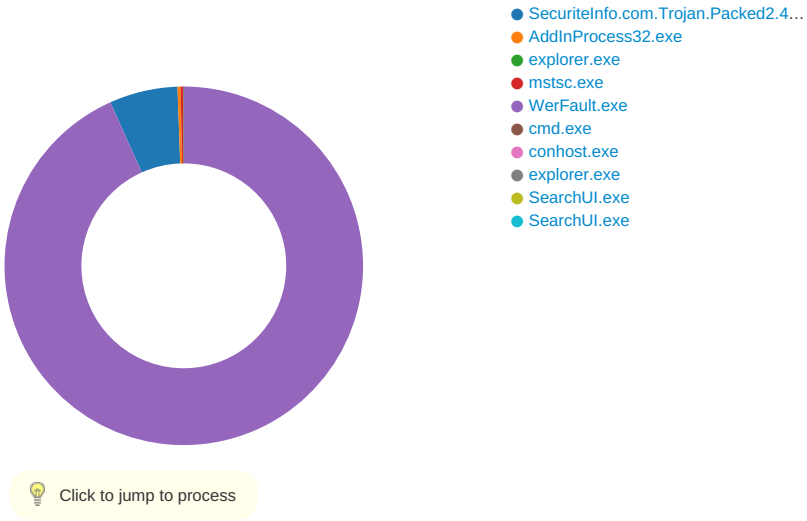
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49777	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 19:18:16.435353041 CET	5713	OUT	GET /bsl/?mt=meRO04KZ+tRueejEQ1mKApUC+xiZQAGZPTeO6WstMPZoEBgumINoRWRpGBFK3WkMjtLu&2d=hxlpdRkxCvtTgBzP HTTP/1.1 Host: www.edu4go.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 19:18:16.574495077 CET	5714	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 26 Jan 2021 18:18:16 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d54-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Packed2.42783.14936.exe PID: 5980
Parent PID: 5864

General

Start time:	19:15:30
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe'
Imagebase:	0x10000
File size:	775168 bytes
MD5 hash:	25FCC01067CABBF5D1AA3A2F8B18ED50
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.686008623.0000000003DFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.686008623.0000000003DFA000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.686008623.0000000003DFA000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.686170457.0000000003F66000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.686170457.0000000003F66000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.686170457.0000000003F66000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D41CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D41CF06	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4ABE29B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D72C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1d 5a 8e 5a 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 9a 77 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 dc 8d 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..X...........w... ....@.. ....`.................	success or wait	1	4ABE29B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.42783.14936.exe.log	unknown	1873	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6D72C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C261B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C261B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: AddInProcess32.exe PID: 6476 Parent PID: 5980

General

Start time:	19:15:36
Start date:	26/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x710000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.721240186.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.721240186.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.721240186.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.721927497.0000000001090000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.721927497.0000000001090000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.721927497.0000000001090000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.722073173.00000000010C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.722073173.00000000010C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.722073173.00000000010C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6476

General

Start time:	19:15:41
Start date:	26/01/2021
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

Reputation:	high

Analysis Process: mstsc.exe PID: 3476 Parent PID: 3424

General

Start time:	19:15:54
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0xab0000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1028284186.0000000000A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1027686906.00000000008F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1027686906.00000000008F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1027686906.00000000008F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1025912109.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1025912109.0000000000140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1025912109.0000000000140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	159E57	NtReadFile

Analysis Process: WerFault.exe PID: 7108 Parent PID: 3424

General

Start time:	19:15:56
Start date:	26/01/2021
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3424 -s 8832
Imagebase:	0x7ff708910000
File size:	494488 bytes

MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	7FFA9AB3527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA9AB2E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp.xml	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12CF.tmp.csv	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER164A.tmp.txt	success or wait	1	7FFA9AB2E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 10 00 00 00 20 00 00 00 00 00 00 00 69 5c 10 60 a4 05 12 00 00 00 00 00	MDMP..... .....i\.`.....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 1c 7d 00 00 00 01 00 00 4c 77 c2 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 02 c8 ed 01 00 00 54 05 00 00 f7 03 00 00 60 0d 00 00 c0 40 10 60 01 00 00 00 01 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00	..... U..... B.....}.... ..Lw..... T... ....`....@.`..... .....0..... 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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	1232	38 ad 7d 00 00 00 00 00 23 00 00 00 00 00 00 00 00 08 98 5d bd fa 7f 00 00 6c 68 48 bd fa 7f 00 00 3c 56 e6 bb fa 7f 00 00 00 00 00 00 ed a4 57 f9 4f 00 10 00 a0 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 00 00 c8 e5 df 58 eb 35 1f 8c ac 19 2f bc fa 7f 00 00 ac 19 2f bc fa 7f 00 00 ac 19 2f bc fa 7f 00 00 42 59 fc 66 8f 7c 36 9a b8 cd ec 48 ba 91 c0 7d 05 30 47 34 2c 39 d3 3e 03 00 00 00 00 00 00 00 ba 66 48 bd fa 7f 00 00 74 03 00 c0 00 00 00 00 00 b2 7d 00 00 00 00 00 a8 02 91 02 00 00 00 00 01 00 00 00 00 00 00 00 b0 97 5d bd fa 7f 00 00 00 00 00 00 00 00 00 00 00 0b 8b 19 b2 5b 85 aa a1 4f 74 e7 e8 ad b9 3b 04 00 09 14 a1 07 00 00 00 e0 0d 91 02 00 00 00 00 00 00 91 02 00 00 00 00 c0 0c 91 02 00 00 00 00 8d 00 00 00 00 00 00 00 eb 4e 57 bd fa 7f 00	8.}.....#.....].....lhH..... <V.....W.O.....3.+. +.S.+.+.....X.5..../..... /...../.....BY.f.|6....H...} .0G4,9.>.....fH.....t..... ....}.....]. .....[...Ot...;... ....NW....	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	168	64 0d 00 00 00 00 00 00 74 03 00 c0 01 00 00 00 00 00 00 00 00 00 00 00 eb 4e 57 bd fa 7f 00 00 01 00 00 00 00 00 00 00 b0 97 5d bd fa 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b c9 57 bd fa 7f 00 00 94 a1 49 ea 64 a4 00 00 00 00 00 00 00 00 00 00 8d 00 00 00 00 00 00 00 c0 0c 91 02 00 00 00 00 00 00 00 00 00 00 00 00 e0 0d 91 02 00 00 00 00 20 00 00 00 00 00 00 00 5d f6 57 bd fa 7f 00 00 dc f8 83 e1 00 00 00 00 d0 04 00 00 f0 9f 00 00	d.......t.................NW... ....].................. ....[.W....... I.d........................... ....].W...	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	20	a1 01 00 00 00 80 8f 00 00 00 00 00 00 20 00 00 24 1e 02 00	....$...	success or wait	417	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	8192	00 00 00 00 00 00 00 00 00 00 d7 07 00 00 00 00 00 20 d6 07 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 8f 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0d 00 00 00 00 00 00 10 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 97 71 06 00 00 00 00 00 f0 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....`......................... q.............................	success or wait	416	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	888	9d 02 24 bb fa 7f 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 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 d4 e1 61 a6 fa 7f 00 00 a0 d6 bc 02 00 00 00 00 90 fd d4 05 00 00 00 00 90 d6 bc 02 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa 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 a4 d7 61 a6 fa 7f 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa 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 aa aa aa aa aa aa aa aa c8 fd d4 05 00 00 00 00 aa aa aa aa aa aa aa	..$........................... ....a....................... ....a.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	4	49 00 00 00	I...	success or wait	73	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	1232	aa aa aa aa aa aa aa aa 20 00 00 00 00 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 1f 00 10 00 a0 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa aa aa aa aa aa aa aa aa aa c0 99 7d 00 00 00 00 00 60 0d 00 00 00 00 00 00 88 99 7d 00 00 00 00 00 b0 22 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 00 00 00 00 00 00 00 00 00 00 00 50 b2 7d 00 00 00 00 00 68 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 aa 51 bd fa 7f 00	....3.+. +.S.+.+.F..................... ....}.....`..... ....}......".................. ....P.}......h....... ....Q....	success or wait	73	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	48	28 13 00 00 02 00 00 00 20 00 00 00 00 00 00 00 00 60 9d 00 00 00 00 00 28 f9 3d 11 00 00 00 00 d8 06 00 00 46 1f 0a 00 d0 04 00 00 40 ff 01 00	(....... ....`......(.=... ......F.......@...	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	4	ec 00 00 00	....	success or wait	236	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	30	18 00 00 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 00 00	....e.x.p.l.o.r.e.r...e.x.e...	success or wait	236	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	120	00 00 a7 9a fa 7f 00 00 00 b0 03 00 5a 12 04 00 bd 7d 8b 35 a0 9d 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 0f 00 00 00	...........Z....}.5.......... ....B.......B?........... ....-............. ..`A.........................	success or wait	15	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	40	22 00 00 00 42 00 6c 00 75 00 65 00 74 00 6f 00 6f 00 74 00 68 00 41 00 70 00 69 00 73 00 2e 00 64 00 6c 00 6c 00 00 00	"...B.l.u.e.t.o.o.t.h.A.p.i.s. ..d.l.l...	success or wait	15	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	48	00 00 c1 9a fa 7f 00 00 00 10 1e 00 fa 81 1e 00 c6 5d 75 70 d2 9f 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 04 00 00 00	................]up........ . ..p..............	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	156	00 00 65 a9 f4 7d 00 00 e0 11 65 a9 f4 7d 00 00 00 00 65 a9 f4 7d 00 00 01 00 00 00 04 00 00 00 a8 f2 5e bd fa 7f 00 00 a8 f2 5e bd fa 7f 00 00 00 00 65 a9 f4 7d 00 00 45 8c bf ca fb 96 d6 01 00 00 65 a9 f4 7d 00 00 e0 11 65 a9 f4 7d 00 00 00 00 65 a9 f4 7d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 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 10 00 00 e0 11 00 00 0c 00 00 00	..e..}....e..}....e..}........ ....^.......^.......e..}..E... ......e..}....e..}....e..}....	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	644	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 ff ff 7f 00 00 0f 00 00 00 00 00 00 00 00 04 00 00 00 00 70 b8 02 00 00 00 00 00 30 3b 03 00 00 00 00 0b 6a 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 3f 9c 03 00 00 00 00 00 40 9c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ae d3 1a 00 00 00 00 00 92 2b 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 fe 4a 05 00 00 00 00 00 86 0b e1 45 01 00 00 00 f3 e9 8a 19 00 00 00 00 f7 bf e9 0d 00 00 00 00 98 ec fc 00 00 00 00 00 e0 b0 00 00 c7 d6 00 00 0a 97 05 00 c2 5e 0a 00 92 2b 05 00 fb 7e 15 00 fe 4a 05 00 ca 2d 28 00 6e 4c 01 00 5e 41 14 00 00 00 00 00 75 d9 13 00 77 10 05 00 90 c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 02 00	....Zb..... .....p.. .....0;.....j..... ..?.....@..... .....+.....@.....J..... .E..... .....^...+...~...J...- (.nL..^A.....u...w..... .....U..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	153388	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	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61D.tmp.dmp	unknown	132	03 00 00 00 b4 0d 00 00 14 07 00 00 04 00 00 00 94 63 00 00 d4 14 00 00 0e 00 00 00 74 01 00 00 68 78 00 00 0d 00 00 00 bc 00 00 00 dc 79 00 00 05 00 00 00 14 1a 00 00 10 04 02 00 06 00 00 00 a8 00 00 00 6c 06 00 00 07 00 00 00 38 00 00 00 e0 00 00 00 0f 00 00 00 54 05 00 00 18 01 00 00 0c 00 00 00 70 5d 01 00 0a 1b 0f 00 15 00 00 00 ec 01 00 00 98 7a 00 00 16 00 00 00 98 00 00 00 84 7c 00 00	.....c.....t. ..hx.....y..... .....l.....8.....T. .....p].....z.. .....|..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 38 00 31 00 34 00 35 00 34 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.>.7.0.8.1.4.5.4.<./.U.p.t.i.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 38 00 37 00 34 00 30 00 33 00 33 00 36 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.>.2.2.0.3.8.7.4.0.3.3.6.6.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 38 00 35 00 39 00 36 00 33 00 36 00 32 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.0.3.8.5.9.6.3.6.2.2.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 31 00 31 00 33 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.>.7.1.1.3.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 36 00 37 00 35 00 31 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.9.6.7.5.1.3.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 36 00 37 00 35 00 31 00 33 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.9.6.7.5.1.3.6.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 38 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.8.5.1.2.<./.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	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 30 00 39 00 39 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.>.9.6.0.9.9.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 31 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.8.1.7.5.2.<./.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 31 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.8.1.4.8.0.<./.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 33 00 36 00 34 00 32 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.3.6.4.2.2.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 31 00 30 00 35 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.1.0.5.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 33 00 36 00 34 00 32 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.3.6.4.2.2.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.0.4.<./.P.i.d.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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.>.(.u.n.a.b.l.e. .t.o. .r.e.t.r.i.e.v.e.).<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	56	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 32 00 33 00 33 00 38 00 37 00 37 00 35 00 31 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.>.1.0.2.3.3.8.7.7.5.1.3.<./.U.p.t.i.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 33 00 37 00 35 00 35 00 35 00 32 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.>.2.2.0.3.4.0.3.7.5.5.5.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	56	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 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 31 00 32 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.2.9.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 35 00 30 00 32 00 39 00 38 00 38 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.>.5.0.2.9.8.8.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 36 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.>.3.6.8.6.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.3.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	88	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 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.9.2.<./.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	100	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 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 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.>.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	72	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 38 00 31 00 39 00 32 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.>.8.1.9.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 31 00 32 00 36 00 31 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.2.6.1.5.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	68	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 38 00 31 00 39 00 32 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.>.8.1.9.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 45 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 45 00 58 00 45 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.>.E.x.p.l.o.r.e.r...E.X.E.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 78 00 65 00 65 00 75 00 75 00 6f 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.>.x.e.e.u.u.o.,. .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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 78 00 65 00 65 00 75 00 75 00 6f 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.>.x.e.e.u.u.o.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 35 00 36 00 37 00 30 00 34 00 37 00 35 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.>.1.5.6.5.6.7.0.4.7.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 31 00 2d 00 32 00 36 00 54 00 31 00 38 00 3a 00 31 00 36 00 3a 00 31 00 30 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.-.0.1.-.2.6.T.1.8.:.1.6.:.1.0.Z.".>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	268	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 38 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 32 00 31 00 37 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 32 00 31 00 37 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65	<.P.r.o.c.e.s.s. .A.s.I.d.=.".8.0.". .P.I.D.=.".3.4.2.4.". .U.p.t.i.m.e.M.S.=.".3.2.1.7.8.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.2.1.7.8.7.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	7	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	21	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	344	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 46 00 6f 00 63 00 75 00 73 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 36 00 37 00 35 00 30 00 32 00 30 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 30 00 31 00 31 00 31 00 31 00 22 00 20 00 54 00 6f 00 74 00 61 00 6c 00 44 00 75 00 72 00 61 00 74	<.T.i.m.e.l.i.n.e. .N.a.m.e.=.".F.o.c.u.s.". .T.i.m.e.l.i.n. e.S.t.a.r.t.D.e.l.t.a.M.S.=.". 6.7.5.0.2.0.8.". .T.i.m.e.l.i. n.e.U.n.i.t.S.h.i.f.t.=.".1.2.". .T.i.m.e.l.i.n.e.=.".1.1.1. 1.1.1.1.1.1.1.1.1.1.1.1.1.1. 1.1.1.1.1.1.1.0.1.1.1.1.". .T.o.t.a.l.D.u.r.a.t	success or wait	7	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 36 00 32 00 63 00 31 00 31 00 31 00 33 00 62 00 2d 00 35 00 61 00 38 00 36 00 2d 00 34 00 34 00 38 00 65 00 2d 00 62 00 37 00 63 00 30 00 2d 00 30 00 30 00 37 00 33 00 38 00 64 00 33 00 38 00 34 00 64 00 32 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.7.6.2.c.1.1.3.b.-.5.a.8.6.-.4.4.8.e.-.b.7.c.0.-.0.0.7.3.8.d.3.8.4.d.2.f.<./.G.u.i.d.>.	success or wait	1	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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 31 00 2d 00 32 00 36 00 54 00 31 00 38 00 3a 00 31 00 36 00 3a 00 31 00 30 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.-.0.1.-.2.6.T.1.8.:.1.6.:.1.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1205.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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12D1.tmp.xml	unknown	4745	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 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	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\Report.wer	unknown	2	ff fe	..	success or wait	1	7FFA9AB2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\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	361	7FFA9AB2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Explorer.EXE_7abfb1f1fbdbd7c2322150249348b63f54b8a170_10665708_1ba816b7\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 34 00 33 00 36 00 35 00 38 00 31 00 37 00 35 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.4.3.6.5.8.1.7.5.3.	success or wait	1	7FFA9AB2E9F7	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA9AB2E3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	FileId	unicode	0000f5d0299140cf98875b07dbd2d892617401dad8b9	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	LowerCaseLongPath	unicode	c:\windows\explorer.exe	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	LongPathHash	unicode	explorer.exe|68e882542b88f3ee	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	Name	unicode	explorer.exe	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	Publisher	unicode	microsoft corporation	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	BinaryType	unicode	pe64_amd64	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	LinkDate	unicode	04/12/2005 02:21:38	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFA9AB51D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	Size	B	00 04 3C 00 00 00 00 00	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	Language	dword	1033	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	IsPeFile	dword	1	success or wait	1	7FFA9AB51D2D	unknown
\REGISTRY\A\{43385ba9-9958-2bc4-7112-3e86839ed654}\Root\InventoryApplicationFile\explorer.exe|68e882542b88f3ee	IsOsComponent	dword	1	success or wait	1	7FFA9AB51D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E D1 58 F9 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	74 03 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 EB 4E 57 BD FA 7F 00 00 01 00 00 00 00 00 00 00 B0 97 5D BD FA 7F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5B C9 57 BD FA 7F 00 00 94 A1 49 EA 64 A4 00 00 00 00 00 00 00 00 00 00 8D 00 00 00 00 00 00 00 C0 0C 91 02 00 00 00 00 00 00 00 00 00 00 00 00 E0 0D 91 02 00 00 00 00 20 00 00 00 00 00 00 00 5D F6 57 BD FA 7F 00 00 DC F8 83 E1 00 00 00 00	success or wait	1	7FFA9AB507CB	RegSetValueExW

Analysis Process: cmd.exe PID: 5992 Parent PID: 3476

General

Start time:	19:15:59
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7116 Parent PID: 5992

General

Start time:	19:16:00

Start date:	26/01/2021
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: explorer.exe PID: 2896 Parent PID: 576

General

Start time:	19:16:12
Start date:	26/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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	Completion	Count	Source Address	Symbol

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: SearchUI.exe PID: 960 Parent PID: 800

General

Start time:	19:16:31
Start date:	26/01/2021
Path:	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe

Wow64 process (32bit):	false
Commandline:	'C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe' -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
Imagebase:	0x7ff676950000
File size:	13606304 bytes
MD5 hash:	C4A9ACE9CDB9E5DB7CBA996CFA9EA7A2
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: SearchUI.exe PID: 6652 Parent PID: 800

General

Start time:	19:17:39
Start date:	26/01/2021
Path:	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe' -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
Imagebase:	0x7ff676950000
File size:	13606304 bytes
MD5 hash:	C4A9ACE9CDB9E5DB7CBA996CFA9EA7A2
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis