ID: 329739
Sample Name: Pictures.bat
Cookbook: default.jbs
Time: 09:00:18
Date: 13/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

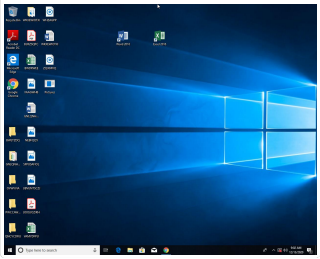
Analysis Report Pictures.bat

Overview

General Information

Sample Name:	Pictures.bat (renamed file extension from bat to exe)
Analysis ID:	329739
MD5:	97df3062b2fda05..
SHA1:	3b373ce09cad26..
SHA256:	99cc3ed45ab5f25..
Tags:	bat HawkEye

Most interesting Screenshot:



Detection

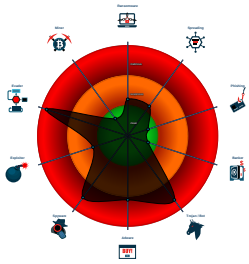
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Changes the view of files in windows…
- Connects to a pastebin service (like…
- Contains functionality to log keystro…

Classification



Startup

- **System is w10x64**
- Pictures.exe (PID: 1492 cmdline: 'C:\Users\user\Desktop\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - cmd.exe (PID: 1380 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 4.769 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 616 cmdline: timeout 4.769 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Pictures.exe (PID: 6464 cmdline: C:\Users\user\Desktop\Pictures.exe MD5: 97DF3062B2FDA05A79936B955CFF4351)
    - WerFault.exe (PID: 5748 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 1840 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6804 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1492 -s 928 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Pictures.exe (PID: 6988 cmdline: 'C:\Users\user\Desktop\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - cmd.exe (PID: 7116 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 4.769 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6488 cmdline: timeout 4.769 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Pictures.exe (PID: 5868 cmdline: C:\Users\user\Desktop\Pictures.exe MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - WerFault.exe (PID: 6772 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6988 -s 1092 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Pictures.exe (PID: 3984 cmdline: 'C:\Users\user\Desktop\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - cmd.exe (PID: 4684 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 4.769 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5712 cmdline: timeout 4.769 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Pictures.exe (PID: 1572 cmdline: C:\Users\user\Desktop\Pictures.exe MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - WerFault.exe (PID: 4928 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3984 -s 1652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Pictures.exe (PID: 4604 cmdline: 'C:\Users\user\Desktop\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - cmd.exe (PID: 6208 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 4.769 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6524 cmdline: timeout 4.769 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- Pictures.exe (PID: 6836 cmdline: 'C:\Users\user\Desktop\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
  - cmd.exe (PID: 6012 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 4.769 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5932 cmdline: timeout 4.769 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- Pictures.exe (PID: 6576 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe' MD5: 97DF3062B2FDA05A79936B955CFF4351)
- **cleanup**

Malware Configuration

Threatname: HawkEye

```
{
  "Modules": [
    "Mail PassView",
    "mailpv",
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x145cb7:$key: HawkEyeKeylogger • 0x147efb:$salt: 099u787978786 • 0x1462f8:$string1: HawkEye_Keylogger • 0x14714b:$string1: HawkEye_Keylogger • 0x147e5b:$string1: HawkEye_Keylogger • 0x1466e1:$string2: holdermail.txt • 0x146701:$string2: holdermail.txt • 0x146623:$string3: wallet.dat • 0x14663b:$string3: wallet.dat • 0x146651:$string3: wallet.dat • 0x147a1f:$string4: Keylog Records • 0x147d37:$string4: Keylog Records • 0x147f53:$string5: do not script --> • 0x145c9f:$string6: \pidloc.txt • 0x145d2d:$string7: BSPLIT • 0x145d3d:$string7: BSPLIT
0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x146350:$hawkstr1: HawkEye Keylogger • 0x147191:$hawkstr1: HawkEye Keylogger • 0x1474c0:$hawkstr1: HawkEye Keylogger • 0x14761b:$hawkstr1: HawkEye Keylogger • 0x14777e:$hawkstr1: HawkEye Keylogger • 0x1479f7:$hawkstr1: HawkEye Keylogger • 0x145ede:$hawkstr2: Dear HawkEye Customers! • 0x147513:$hawkstr2: Dear HawkEye Customers! • 0x14766a:$hawkstr2: Dear HawkEye Customers! • 0x1477d1:$hawkstr2: Dear HawkEye Customers! • 0x145fff:$hawkstr3: HawkEye Logger Details:
Click to see the 81 entries				

Unpacked PEs

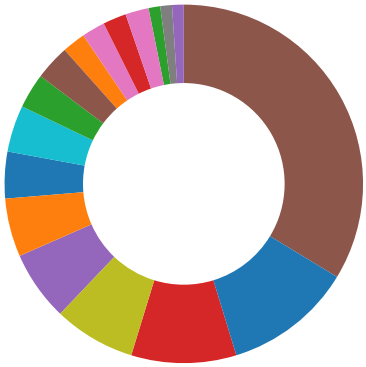
Source	Rule	Description	Author	Strings
35.2.Pictures.exe.400000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8f7:$key: HawkEyeKeylogger • 0x7db3b:$salt: 099u787978786 • 0x7bf38:$string1: HawkEye_Keylogger • 0x7cd8b:$string1: HawkEye_Keylogger • 0x7da9b:$string1: HawkEye_Keylogger • 0x7c321:$string2: holdermail.txt • 0x7c341:$string2: holdermail.txt • 0x7c263:$string3: wallet.dat • 0x7c27b:$string3: wallet.dat • 0x7c291:$string3: wallet.dat • 0x7d65f:$string4: Keylog Records • 0x7d977:$string4: Keylog Records • 0x7db93:$string5: do not script --> • 0x7b8df:$string6: \pidloc.txt • 0x7b96d:$string7: BSPLIT • 0x7b97d:$string7: BSPLIT
35.2.Pictures.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
35.2.Pictures.exe.400000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
35.2.Pictures.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
35.2.Pictures.exe.400000.0.unpack	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bf90:$hawkstr1: HawkEye Keylogger • 0x7cdd1:$hawkstr1: HawkEye Keylogger • 0x7d100:$hawkstr1: HawkEye Keylogger • 0x7d25b:$hawkstr1: HawkEye Keylogger • 0x7d3be:$hawkstr1: HawkEye Keylogger • 0x7d637:$hawkstr1: HawkEye Keylogger • 0x7bb1e:$hawkstr2: Dear HawkEye Customers! • 0x7d153:$hawkstr2: Dear HawkEye Customers! • 0x7d2aa:$hawkstr2: Dear HawkEye Customers! • 0x7d411:$hawkstr2: Dear HawkEye Customers! • 0x7bc3f:$hawkstr3: HawkEye Logger Details:
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 dropped file

Multi AV Scanner detection for submitted file

Networking:

Connects to a pastebin service (likely for C&C)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Creates autostart registry keys with suspicious names

Creates multiple autostart registry keys

Drops PE files to the startup folder

Hooking and other Techniques for Hiding and Protection:

Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

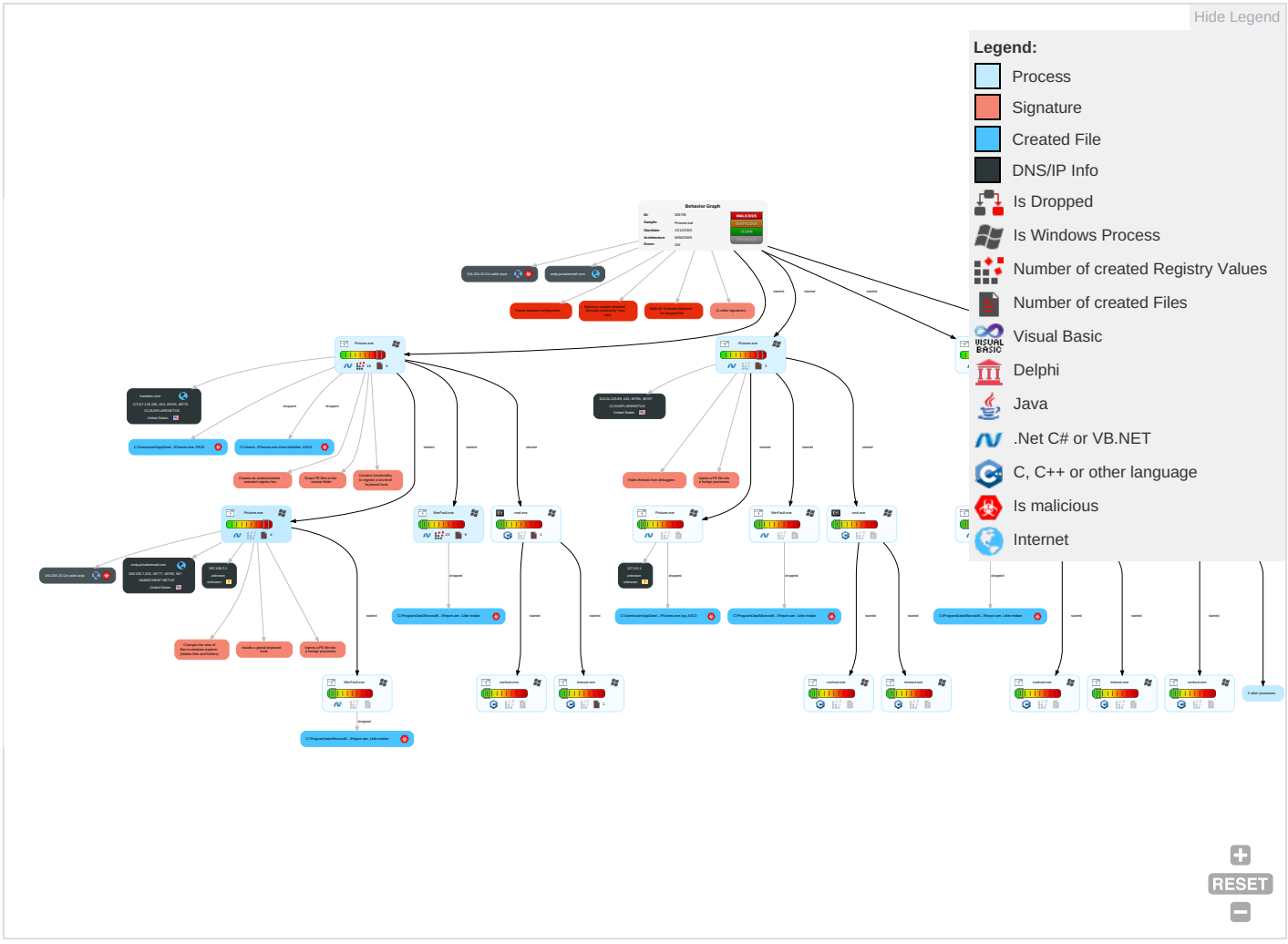
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 3 1 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Network Medium
Default Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 3 1 1	Exfiltration Over Bluetooth

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 4 2 1	Process Injection 1 1 1	Obfuscated Files or Information 2 1	Security Account Manager	System Information Discovery 2 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltr
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 4 2 1	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Trans
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 5 1	SSH	Keylogging	Data Transfer Siz Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 6	VNC	GUI Input Capture	Exfiltration Over C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 6	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encry Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encr Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obf Non-C2 Protocol

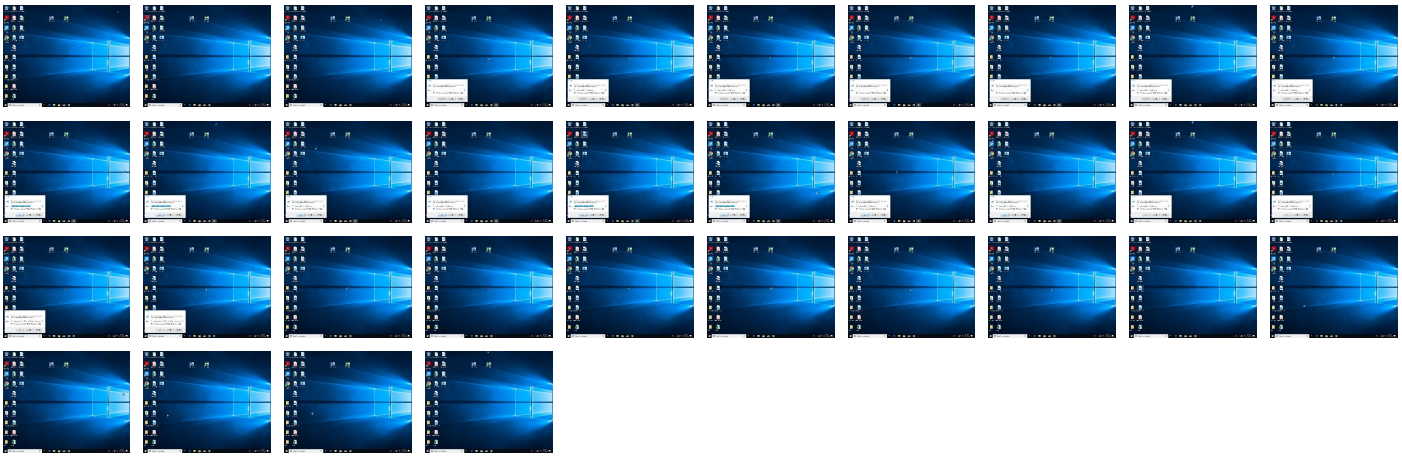
Behavior Graph



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
Pictures.exe	30%	Virustotal		Browse
Pictures.exe	16%	Metadefender		Browse
Pictures.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe	16%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.Pictures.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
23.2.Pictures.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.2.Pictures.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.2.Pictures.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
35.2.Pictures.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
35.2.Pictures.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
164.204.10.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn=I	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceom	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	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.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com6	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sandoll.co.krY5RI	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.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://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	

Source	Detection	Scanner	Label	Link
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnMIr4	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krP	0%	Avira URL Cloud	safe	
http://www.sakkal.coml	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krM	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://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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn//wS5IH..	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.urwpp.deP	0%	Avira URL Cloud	safe	
http://www.urwpp.deve	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krk5	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krN.TTF	0%	Avira URL Cloud	safe	
http://www.sakkal.com7	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sakkal.com-u	0%	Avira URL Cloud	safe	
http://wI5CH./	0%	Avira URL Cloud	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://www.carterandcone.comx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.urwpp.dee	0%	Avira URL Cloud	safe	
http://www.carterandcone.comopsz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hastebin.com	172.67.143.180	true	false		high
smtp.privateemail.com	199.193.7.228	true	false		high
164.204.10.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn=I	Pictures.exe, 00000007.0000000 3.688773365.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhh ttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://https://hastebin.com	Pictures.exe, 00000000.0000000 2.744682493.0000000002D51000.0 0000004.00000001.sdmp, Pictures.exe, 0000000C.00000002.860590575.00000 00002501000.00000004.00000001. sdmp, Pictures.exe, 00000012.0 0000002.880252420.0000000002D1 1000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.comceom	Pictures.exe, 00000007.0000000 2.812029938.00000000018C7000.0 0000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Pictures.exe, 00000007.0000000 2.826255301.0000000008016000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddres sxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html6	Pictures.exe, 00000007.0000000 3.699262389.0000000006368000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com6	Pictures.exe, 00000007.0000000 3.690314858.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovin ce	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Pictures.exe, 00000007.0000000 3.688216115.000000000636E000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddres szhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/authenticatio n	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krY5RI	Pictures.exe, 00000007.0000000 3.688216115.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.carterandcone.comF	Pictures.exe, 00000007.0000000 3.690314858.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://https://hastebin.com/raw/yonozilace	Pictures.exe, 00000000.0000000 2.744682493.0000000002D51000.0 0000004.00000001.sdmp, Pictures.exe, 0000000C.00000002.860590575.00000 00002501000.00000004.00000001. sdmp, Pictures.exe, 00000012.0 0000002.880252420.0000000002D1 1000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnMIr4	Pictures.exe, 00000007.0000000 3.688698853.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krP	Pictures.exe, 00000007.0000000 3.688148286.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.coml	Pictures.exe, 00000007.0000000 3.690845267.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	Pictures.exe, 00000000.0000000 2.746517106.0000000003E88000.0 0000004.00000001.sdmp, Pictures.exe, 00000007.00000002.807250814.00000 00000402000.00000040.00000001. sdmp, Pictures.exe, 0000000C.0 0000002.874949951.00000000043A C000.00000004.00000001.sdmp, P ictures.exe, 00000012.00000002 .888849131.00000000041D6000.00 000004.00000001.sdmp, WerFault.exe, 00000013.00000003.746755143.000000 00058A0000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krM	Pictures.exe, 00000007.0000000 3.688148286.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Pictures.exe, 00000007.0000000 3.688216115.000000000636E000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	Pictures.exe, 00000007.0000000 2.813738725.000000000333B000.0 0000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	Pictures.exe, 00000012.0000000 2.888849131.00000000041D6000.0 0000004.00000001.sdmp	false		high
http://www.urwpp.de	Pictures.exe, 00000007.0000000 3.695329896.0000000006365000.0 0000004.00000001.sdmp, Pictures.exe, 00000007.00000003.700552872.00000 00006368000.00000004.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Pictures.exe, 00000000.0000000 2.744682493.0000000002D51000.0 0000004.00000001.sdmp, Pictures.exe, 00000007.00000002.812978942.00000 00003281000.00000004.00000001. sdmp, WerFault.exe, 0000000A.0 0000003.706265727.0000000005CF 0000.00000004.00000001.sdmp, P ictures.exe, 0000000C.00000002 .860590575.0000000002501000.00 000004.00000001.sdmp, Pictures.exe, 00000012.00000002.880252420.000000 0002D11000.00000004.00000001.sdmp, WerFault.exe, 00000013.00000003.743 322819.0000000005BA0000.000000 04.00000001.sdmp	false		high
http://www.sakkal.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn//wS5IH..	Pictures.exe, 00000007.0000000 3.688626211.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Pictures.exe, 00000007.0000000 2.826255301.0000000008016000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Pictures.exe, 00000007.0000000 3.703414982.0000000006368000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Pictures.exe, 00000007.0000000 2.826255301.0000000008016000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deP	Pictures.exe, 00000007.0000000 3.693500062.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.urwpp.deve	Pictures.exe, 00000007.0000000 3.700382243.0000000006368000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krk5	Pictures.exe, 00000007.0000000 3.688216115.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krN.TTF	Pictures.exe, 00000007.0000000 3.688148286.000000000636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com7	Pictures.exe, 00000007.0000000 3.690845267.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://smtp.privateemail.com	Pictures.exe, 00000007.0000000 2.813515212.0000000003300000.0 0000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Pictures.exe, 00000007.0000000 3.688584334.0000000006365000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	Pictures.exe, 00000007.0000000 3.698812159.0000000006367000.0 0000004.00000001.sdmp, Pictures.exe, 00000007.00000002.823160870.00000 000064B0000.00000002.00000001. sdmp	false		high
http://www.sakkal.com-u	Pictures.exe, 00000007.0000000 3.690785551.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://wI5CH./	Pictures.exe, 00000007.0000000 3.688626211.000000006636E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micro	WerFault.exe, 00000013.0000000 3.772377584.0000000003485000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Pictures.exe, 00000007.0000000 3.699262389.0000000006368000.0 0000004.00000001.sdmp	false		high
http://www.carterandcone.comx	Pictures.exe, 00000007.0000000 3.690314858.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	Pictures.exe, 00000007.0000000 3.689287299.0000000006368000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Pictures.exe, 00000007.0000000 2.823160870.00000000064B0000.0 0000002.00000001.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrh ttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000A.0000000 3.706265727.0000000005CF0000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	Pictures.exe, 00000007.0000000 3.695701608.0000000006365000.0 0000004.00000001.sdmp	false		high
http://www.urwpp.dee	Pictures.exe, 00000007.0000000 3.693500062.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comopsz	Pictures.exe, 00000007.0000000 3.690314858.0000000006365000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.193.7.228	unknown	United States		22612	NAMECHEAP-NETUS	false
104.24.126.89	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.143.180	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	329739
Start date:	13.12.2020
Start time:	09:00:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pictures.bat (renamed file extension from bat 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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@49/21@10/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 31.7% • Quality standard deviation: 29.3%
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): taskhostw.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 51.11.168.160, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 52.255.188.83, 104.43.193.48, 93.184.220.29 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, crl3.digicert.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing behavior and disassembly information. • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile 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 NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:01:23	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\Pictures.exe
09:01:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Pictures.exe C:\Users\user\Desktop\Pictures.exe
09:01:39	API Interceptor	28x Sleep call for process: Pictures.exe modified
09:01:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\Pictures.exe
09:01:44	API Interceptor	4x Sleep call for process: WerFault.exe modified
09:01:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Pictures.exe C:\Users\user\Desktop\Pictures.exe
09:01:57	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.193.7.228	7iZX0KCH4C.exe	Get hash	malicious	Browse	
	Al-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	
	SIWFT refTRF08463473 20201611.exe	Get hash	malicious	Browse	
	Pictures_Designs_images_Dragram on.exe	Get hash	malicious	Browse	
	pictures of me and factory haw on.exe	Get hash	malicious	Browse	
	#U6807#U51c6#U7684#U6837#U672c#U683c#U5f0f #U66f4#U65b0.xlsx.exe	Get hash	malicious	Browse	
	PROFOMA INVOICE LPO-682768286830.exe	Get hash	malicious	Browse	
	payment issue.docx	Get hash	malicious	Browse	
	32IY5Rn02W.exe	Get hash	malicious	Browse	
	I6Sk8JcGLp.exe	Get hash	malicious	Browse	
	vm13rtE9ua.exe	Get hash	malicious	Browse	
	Urgent (0998 R1) ST PO1805140.exe	Get hash	malicious	Browse	
	T21 Orders - Quotation 309-Ref-284.exe	Get hash	malicious	Browse	
	G6pOfA1Ly3.exe	Get hash	malicious	Browse	
	tQAb4zwepD.rtf	Get hash	malicious	Browse	
	e05JLHdiva.exe	Get hash	malicious	Browse	
	swift transfer copy 639082020.exe	Get hash	malicious	Browse	
	dWSU.exe	Get hash	malicious	Browse	
	NBUSpRGwKqFfAcoxptdwkgXyGpxRqE.exe	Get hash	malicious	Browse	
	company certificate.exe	Get hash	malicious	Browse	
104.24.126.89	http://freexyg.imghpoers.pw/north-east-dairies.html	Get hash	malicious	Browse	• freexyg.imghpoers.pw/favicon.ico
172.67.143.180	ORDER #0622.exe	Get hash	malicious	Browse	
	01_extracted.exe	Get hash	malicious	Browse	
	02_extracted.exe	Get hash	malicious	Browse	
	PO122020.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.MSIL.Basic.10.Gen.5064.exe	Get hash	malicious	Browse	
	Le8z5e90IO.exe	Get hash	malicious	Browse	
	vHWqKRYpan.exe	Get hash	malicious	Browse	
	8cXVAdvZhh.exe	Get hash	malicious	Browse	
	ENS004.xls	Get hash	malicious	Browse	
	LA99293P02.xls	Get hash	malicious	Browse	
	IN.986434.exe	Get hash	malicious	Browse	
	ORDER # 00246XF.exe	Get hash	malicious	Browse	
	DHL CUSTOMER FORM.jpg.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader35.57660.10998.exe	Get hash	malicious	Browse	
	SC Inquiry.exe	Get hash	malicious	Browse	
	Dec purchase order.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.MSIL.Basic.10.Gen.4020.exe	Get hash	malicious	Browse	
	Documento de transferencia de Scotiabank7497574730 084doc.exe	Get hash	malicious	Browse	
	Document N0-BR1702Q667420_12.exe	Get hash	malicious	Browse	
	Bank paymentcopy001#pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hastebin.com	ORDER #0622.exe	Get hash	malicious	Browse	• 172.67.143.180
	01_extracted.exe	Get hash	malicious	Browse	• 104.24.127.89
	02_extracted.exe	Get hash	malicious	Browse	• 104.24.127.89
	payment document.exe	Get hash	malicious	Browse	• 104.24.126.89
	PO122020.exe	Get hash	malicious	Browse	• 172.67.143.180
	#PO-NX--LI-2-12-20.jpg.exe	Get hash	malicious	Browse	• 104.24.126.89
	GkNa5RLWZn.exe	Get hash	malicious	Browse	• 104.24.127.89
	archivierter Katalog.exe	Get hash	malicious	Browse	• 104.24.127.89
	New Order document.exe	Get hash	malicious	Browse	• 104.24.127.89
	SecuriteInfo.com.Trojan.MSIL.Basic.10.Gen.5064.exe	Get hash	malicious	Browse	• 172.67.143.180
	O8Ii8MW7rn.exe	Get hash	malicious	Browse	• 104.24.126.89
	Le8z5e90IO.exe	Get hash	malicious	Browse	• 172.67.143.180
	vHWqKRYpan.exe	Get hash	malicious	Browse	• 104.24.127.89
	8cXVAdvZhh.exe	Get hash	malicious	Browse	• 172.67.143.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ENS004.xls	Get hash	malicious	Browse	• 172.67.143.180
	LA99293P02.xls	Get hash	malicious	Browse	• 104.24.126.89
	Invoices.exe	Get hash	malicious	Browse	• 104.24.126.89
	ENS003.xls	Get hash	malicious	Browse	• 104.24.127.89
	xDDWr9lEuo.exe	Get hash	malicious	Browse	• 104.24.126.89
	IN.986434.exe	Get hash	malicious	Browse	• 172.67.143.180
smtp.privateemail.com	7iZX0KCH4C.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order.exe	Get hash	malicious	Browse	• 199.193.7.228
	AI-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	• 199.193.7.228
	SIWFT refTRF08463473 20201611.exe	Get hash	malicious	Browse	• 199.193.7.228
	Pictures_Designs_images_Dragram on.exe	Get hash	malicious	Browse	• 199.193.7.228
	pictures of me and factory haw on.exe	Get hash	malicious	Browse	• 199.193.7.228
	#U6807#U51c6#U7684#U6837#U672c#U683c#U5f0f #U66f4#U65b0.xlsx.exe	Get hash	malicious	Browse	• 199.193.7.228
	PROFOMA INVOICE LPO-682768286830.exe	Get hash	malicious	Browse	• 199.193.7.228
	payment issue.docx	Get hash	malicious	Browse	• 199.193.7.228
	32IY5Rn02W.exe	Get hash	malicious	Browse	• 199.193.7.228
	I6Sk8JcGLp.exe	Get hash	malicious	Browse	• 199.193.7.228
	vm13rtE9ua.exe	Get hash	malicious	Browse	• 199.193.7.228
	Urgent (0998 R1) ST PO1805140.exe	Get hash	malicious	Browse	• 199.193.7.228
	T21 Orders - Quotation 309-Ref-284.exe	Get hash	malicious	Browse	• 199.193.7.228
	G6pOfA1Ly3.exe	Get hash	malicious	Browse	• 199.193.7.228
	tQAb4zwepD.rtf	Get hash	malicious	Browse	• 199.193.7.228
	e05JLHdiva.exe	Get hash	malicious	Browse	• 199.193.7.228
	swift transfer copy 639082020.exe	Get hash	malicious	Browse	• 199.193.7.228
	xtKCPPNMhz.rtf	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.BackDoor.SpyBotNET.25.23177.exe	Get hash	malicious	Browse	• 199.193.7.228

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	http://https://u920579.ct.sendgrid.net/ls/click?upn=Cq4RbLQjlFZUayowJ9tEN6gixmb7UKhyXAXCvMsmbICjFD5DhJprkszpFOyNbgNmq7-2Bq9gyOkpQCauiiQYtKUuzuhRkDdVY3iYQlbf85PPIex1qg1iCLXLRCmn62egy7Kd2WI-2FZe6QjrykO-2BkxUIwg-3D-3Da0Ze_tSu-2BgbrFGsICLGVaAGPqAvBa4uzmGUZNhZ55boO3KRTzNu4GGZepxUqpMzDNq41wULstJA35t6JtnVf2vFtHlmz2-2B31tSDfiBobK3sk93ifRCie1NHPaL2KnBxyzl2a1K3xUYPE-2FZxt6LXV-2FOq7Qf7BGwhC5mooDbh2JB86GzKa1gkvDcq2SJ7XHDp7jJpNK-2FgzsQi2DReRUeTh8TNbzxPb03EO0c0GUBrVxC04FuSc-3D	Get hash	malicious	Browse	• 104.219.248.102
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 192.64.118.140
	http://https://firebasestorage.googleapis.com/v0/b/suga-23109.appspot.com/o/owa%2Findex2isq.html?alt=media&token=37a2b62e-b1f7-4e6b-90a6-c624a30a6a95#centralbilling@opisnet.com	Get hash	malicious	Browse	• 198.54.120.22
	http://amar.alwani.xalia-outlet.com/exr/amar.alwani@centrica.com	Get hash	malicious	Browse	• 199.188.206.8
	D00974974-xls.exe	Get hash	malicious	Browse	• 198.54.117.211
	#Ud83d#Udcdevmshares_msgs.htm	Get hash	malicious	Browse	• 198.54.115.249
	zISJXAAewo.exe	Get hash	malicious	Browse	• 198.54.117.218
	http://amar.alwani.xalia-outlet.com/exr/amar.alwani@centrica.com	Get hash	malicious	Browse	• 199.188.206.8
	CLxJeVvzMA.exe	Get hash	malicious	Browse	• 198.54.117.216
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	reciept.xls	Get hash	malicious	Browse	• 68.65.122.159
	http://https://activingo.org/sanitaryequipment	Get hash	malicious	Browse	• 198.54.116.237
	Statement_9505_of_12_09_2020.xlsm	Get hash	malicious	Browse	• 198.187.29.233
	PURCHASE ORDER-SNDK521036.exe	Get hash	malicious	Browse	• 162.0.232.137
	MSC printouts of outstanding as of 73221_12_09_2020.xlsm	Get hash	malicious	Browse	• 198.187.31.225
	anthony.exe	Get hash	malicious	Browse	• 63.250.41.49

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://voicenotes.eternalallureco.com/screen.php?New_tWfgGGT____soppdYTW_____opUtyDheGWWeQiWJDD___fhfhKLHJSfCxsD=justyna.parzych@ocs.com&fCCjdhRWyryCCSXW____fjfhDFHHFhsh=SFI7SW1wLiAjOTQ5NTMgUHJvZC5wZGY=	Get hash	malicious	Browse	• 162.0.239.153
	tDuLlLosre.exe	Get hash	malicious	Browse	• 192.64.119.113
	uqAU5Vneod.exe	Get hash	malicious	Browse	• 198.54.117.210
	tDuLlLosre.exe	Get hash	malicious	Browse	• 198.54.117.212
CLOUDFLARENETUS	ORDER #0622.exe	Get hash	malicious	Browse	• 172.67.143.180
	MOT_507465.xls	Get hash	malicious	Browse	• 172.67.8.238
	PO_01312.xls	Get hash	malicious	Browse	• 104.22.0.232
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 162.159.130.233
	Confirmation transfer Ref No-MT103-003567865300.exe	Get hash	malicious	Browse	• 104.23.98.190
	01_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180
	02_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180
	oxygen.exe	Get hash	malicious	Browse	• 104.27.159.152
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMonakc5abwzYkjZwuJJIdpTUfwxS3-2FAx2Gg6cNlydrr3lSyhbQTpfJekghaGpBvYb34VwHegANFETS-2FFd170CzXgnUntkFmes-2BUYVWS7isVSQ-2BbQcyOyt4f-2Bdn-2BlFnZ-2Bqc-3DTWzB_2IBYBvCQdAsKAURptGS99dQMFBKrK1wN4XnxMdJ0cXIh9nYwGT3Xwu-2BJ4yf9Ega2-2Fb4aBZPIv-2F3Uh6pUJMakz0TzeZTX0xl7pOsgfOO7FI6CvgBpGnBWoUQlNzcwTa1LKYuValVrvKiMxY1ZNZHP-2BwhweO-2FZEg0fuZ6oQdKpkhXMgoW3oLYapFkguRBnE85xKgVHSn2GJnx3Lso6MZ9nDxeiqulUm-2FFAzZN-2BDV7xlDk-3D	Get hash	malicious	Browse	• 104.16.19.94
	vrptY10F5d.exe	Get hash	malicious	Browse	• 172.67.203.151
	http://https://nelleinletapt.buzz/CD/office365.htm	Get hash	malicious	Browse	• 104.31.89.138
	Your File Is Ready To Download_817649.exe	Get hash	malicious	Browse	• 172.67.73.185
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fin0038847990.sn.am%2fIfCk7ZE6GWq&c=E,1,XbwqZlmKwFAf_trFhDdV9wkuU6vutPEIQqN4IhE8jUbxLD3wnPPXDvKp8Jibjk9HngPAI5iRQWnG4vU_DQMKfMGkzgCqkZ-4BfRprMNSl9Nr7VoPQEtWNft5&typo=1	Get hash	malicious	Browse	• 104.16.19.94
	Your File Is Ready To Download_817649.exe	Get hash	malicious	Browse	• 104.31.89.28
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 104.20.185.68
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 104.18.12.5
	http://https://evenfair.com/Doc.htm	Get hash	malicious	Browse	• 104.20.21.239
	http://https://timcoulson.com/mailer-daemon/?mail=james.dean@ahtd.ar.gov	Get hash	malicious	Browse	• 104.16.123.175
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 104.20.185.68
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMoDOwszjVyyAYaDT-2FHLoDdyO6UKIM2nszToDBLH-2F-2BNBrM6YQWQ3fPgFgPdQQKS7kqDF4HAaq-2Fr6xARUzkvrAsaEOKHpwbrn6MO6h-2FVQHqp3WyMFrzO-2FMB03yvlq5NFbbAuXPdxXXNisWAoifgesDs3QJMZE_MTQeFU9OGQYuK17CNM-2FHMO1to19MQZslfTzkvxZNPLbcqMHTFg465yb8XLd5b0rgockrJEbP9S-2BmH6yrcb6D2Cedv8q0zDKvCKHjkGBdm0VSLiKWxvNJFHYTC9Iu2wUuCoFD26NSM7oM4H1ilEuKaivLf23AP7umZUdZ2jjs6dVp5S47XHieCaV16dvBQPvHZmuEMRH0w6XX1JETA-2BLpCr8JmDoRvBBZSGH-2FQaexfGo-3D	Get hash	malicious	Browse	• 104.16.18.94
CLOUDFLARENETUS	ORDER #0622.exe	Get hash	malicious	Browse	• 172.67.143.180
	MOT_507465.xls	Get hash	malicious	Browse	• 172.67.8.238
	PO_01312.xls	Get hash	malicious	Browse	• 104.22.0.232
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 162.159.130.233
	Confirmation transfer Ref No-MT103-003567865300.exe	Get hash	malicious	Browse	• 104.23.98.190
	01_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180
	02_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180
	oxygen.exe	Get hash	malicious	Browse	• 104.27.159.152

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMonakc5abwzYkjZwuJJIdpTUfwxS3-2FAx2Gg6cNlydrr3lSyhbQTpfJekghaGpBvYb34VwHegANFETS-2FFd170CzXgnUntkFmes-2BUYVWS7isVSQ-2BbQcyOyt4f-2Bdn-2BlFnZ-2Bqc-3DTWzB_2lBYBvCQdAsKAURptGS99dQMFBKrK1wN4XnxMdJ0cXIh9nYwGT3Xwu-2BJ4yf9Ega2-2Fb4aBZPIv-2F3Uh6pUJMakz0TzeZTX0xl7pOsgfOO7FI6CvgBpGnBWoUQlNzcwTa1LKYuValVrvKiMxY1ZNZHP-2BwhweO-2FZEg0fuZ6oQdKpkhXMgoW3oLYapFkguRBnE85xKgVHSn2GJnx3Lso6MZ9nDxeiqulUm-2FFAzZN-2BDV7xlDk-3D	Get hash	malicious	Browse	• 104.16.19.94
	vrptY10F5d.exe	Get hash	malicious	Browse	• 172.67.203.151
	http://https://nelleinletapt.buzz/CD/office365.htm	Get hash	malicious	Browse	• 104.31.89.138
	Your File Is Ready To Download_817649.exe	Get hash	malicious	Browse	• 172.67.73.185
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fin0038847990.sn.am%2fIfCk7ZE6GWq&c=E,1,XbwqZlmKwFAf_trFhDdV9wkuU6vutPEIQqN4IhE8jUbxLD3wnPPXDvKp8Jibjk9HngPAI5iRQWnG4vU_DQMKfMGkzgCqkZ-4BfRprMNSl9Nr7VoPQEtWNft5&typo=1	Get hash	malicious	Browse	• 104.16.19.94
	Your File Is Ready To Download_817649.exe	Get hash	malicious	Browse	• 104.31.89.28
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 104.20.185.68
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 104.18.12.5
	http://https://evenfair.com/Doc.htm	Get hash	malicious	Browse	• 104.20.21.239
	http://https://timcoulson.com/mailer-daemon/?mail=james.dean@ahtd.ar.gov	Get hash	malicious	Browse	• 104.16.123.175
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 104.20.185.68
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMoDOwszjVyyAYaDT-2FHLoDdyO6UKIM2nszToDBLH-2F-2BNBrM6YQWQ3fPgFgPdQQKS7kqDF4HAaq-2Fr6xARUzkvrAsaEOKHpwbrn6MO6h-2FVQHqp3WyMFrzO-2FMB03yvlq5NFbbAuXPdxXXNisWAoifgesDs3QJMZE_MTQeFU9OGQYuK17CNM-2FHMO1to19MQZsIfTzkvxZNPLbcqMHTFg465yb8XLd5b0rgockrJEbP9S-2BmH6yrcb6D2Cedv8q0zDKvCKHjkGBdm0VSLiKWxvNJFHYTC9Iu2wUuCoFD26NSM7oM4H1iIEuKaivLf23AP7umZUdZ2jjs6dVp5S47XHieCaV16dvBQPvHZmuEMRH0w6XX1JETA-2BLpCr8JmDoRvBBZSGH-2FQaexfGo-3D	Get hash	malicious	Browse	• 104.16.18.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	ORDER #0622.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	Confirmation transfer Ref No-MT103-003567865300.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	01_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	02_extracted.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	payment document.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	Zorka-Keramika Order.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	6GLK5.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	PO122020.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	#PO-NX--LI-2-12-20.jpg.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	http://https://tinyurl.com/yyvbwpxk	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	Eh80gQF5vU.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	UNAUTHORIZED SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	New Order document.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	secnc.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nocryt.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	inter.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	SecuriteInfo.com.Exploit.Siggen3.5122.15519.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	6AzBNcJ7GS.docm	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	SecuriteInfo.com.Trojan.MSIL.Basic.10.Gen.5064.exe	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89
	file.xls	Get hash	malicious	Browse	• 172.67.143.180 • 104.24.126.89

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_132ed53a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16862
Entropy (8bit):	3.758598470756162
Encrypted:	false
SSDEEP:	192:KC+mHBUZMXSaPcenu8Nqt/u7swS274ItlJ:pPBUZMXSaZ7A/u7swX4ItlJ
MD5:	DE792DA42617B5CED570EDF810CF25B0
SHA1:	F58161A03FFF393FB2C1F74DA6D321BB82FF70BA
SHA-256:	1670138F0529C121DDAAFE72769B0A345130CA975FBC9437815E66DA2861DDF1
SHA-512:	3ED5719EE8ACE6F3F6D42DFD031FD8C84D5372F1EC78112506D223A320E92DA4E85594E7DB489F76E82A4000712533D22D804FD3E96B03294827688F4E55234B
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.2.3.2.0.1.3.6.4.7.3.6.6.2.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.2.3.2.0.1.6.7.1.1.4.1.8.6.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.4.9.6.2.0.b.8.-.0.d.8.4.-.4.3.e.9.-.a.d.0.0.-.d.6.2.7.b.5.c.a.c.8.4.8.....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.=.8.f.0.1.d.5.3.7.-.9.8.3.2.-.4.b.4.6.-.b.d.6.6.-.f.d.0.1.4.b.b.4.0.8.4.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.i.c.t.u.r.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.9.0.-.0.0.0.1.-.0.0.1.b.-.2.c.c.c.-.3.f.3.0.2.6.d.1.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.2.5.c.d.e.6.6.4.5.7.7.b.8.5.8.a.3.5.2.f.3.8.6.c.c.3.a.c.5.1.0.0.0.0.f.f.f.f.!.0.0.0.0.3.b.3.7.3.c.e.0.9.c.a.d.2.6.8.b.3.a.e.8.6.4.5.4.f.4.b.a.2.3.d.7.0.e.5.9.7.7.0.f.!.P.i.c.t.u.r.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1a1a2321\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16864
Entropy (8bit):	3.7593514119223754
Encrypted:	false
SSDEEP:	192:AJJgg7kOmHBUZMXSaPcenu8Nqt/u7swS274ItlS:E7A/BUZMXSaZ7A/u7swX4ItlS
MD5:	106E93C4ECD9BDF6B7A28300B6960DFA
SHA1:	D2AF39A0F320481E440B322FA9389F4AA75A40AE
SHA-256:	BAD2F590F612CD7C9892E087D49370828E696A3EBB01721B4268F8AEAAF5B20D
SHA-512:	776DBC67597C08EC2A25A9390E1CE92B1A918BCE659005ADA3C0135A00760C00BE2196B73E591C04AA7CF052D091376C7D71E81BCD62C1D4233C5BF9183766F
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.2.3.2.0.1.1.5.1.1.4.3.5.4.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.2.3.2.0.1.5.1.1.6.1.1.0.8.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.f.0.4.9.a.7.7.-.5.6.e.0.-.4.7.a.4.-.9.f.3.d.-.5.1.2.0.f.9.5.9.f.1.6.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.=.f.5.7.f.c.f.b.9.-.6.c.3.0.-.4.2.5.1.-.b.9.0.7.-.f.4.6.8.3.6.5.c.d.4.f.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.i.c.t.u.r.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.4.c.-.0.0.0.1.-.0.0.1.b.-.d.1.b.b.-.5.b.2.b.2.6.d.1.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.2.5.c.d.e.6.6.4.5.7.7.b.8.5.8.a.3.5.2.f.3.8.6.c.c.3.a.c.5.1.0.0.0.0.f.f.f.f.!.0.0.0.0.3.b.3.7.3.c.e.0.9.c.a.d.2.6.8.b.3.a.e.8.6.4.5.4.f.4.b.a.2.3.d.7.0.e.5.9.7.7.0.f.!.P.i.c.t.u.r.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\Report.wer	
Category:	dropped
Size (bytes):	17060
Entropy (8bit):	3.7575296258793593
Encrypted:	false
SSDEEP:	192:6/Q3mHBUZMXSaKsUAip36A/u7sLS274ItI2:KQOBUZMXSalit/u7sLX4ItI2
MD5:	E00BB640DCF08EB94F53FB84D80B2475
SHA1:	D457FF16FF927F94F1C9985C95F61616399C01FA
SHA-256:	CF0CCC6932EB0EE1454BD7FEDF40FF4D8FDE30F3EB4705B36E6ABA1A8A26D2CA
SHA-512:	69E8FED4762FB5F09644594DD57C618EFA9349E67B2B28D326CA5D9FAEA666795A8367AB8A8EC31D13DDFF3006DB59E3979B5595D5F54348835A713C9404A93
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.2.3.2.0.0.8.8.0.9.8.8.2.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.2.3.2.0.1.0.2.5.9.8.7.6.2.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.c.2.1.4.e.f.9.-.4.8.2.1.-.4.5.2.c.-.a.9.9.7.-.3.1.a.3.d.1.9.4.e.c.b.9.....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.=.1.7.6.e.6.0.9.8.-.d.b.a.a.-.4.f.2.e.-.9.7.8.d.-.c.5.5.9.4.3.c.3.0.a.1.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.i.c.t.u.r.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.d.4.-.0.0.0.1.-.0.0.1.b.-.d.f.4.f.-.c.b.1.f.2.6.d.1.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.2.5.c.d.e.6.6.4.5.7.7.b.8.5.8.a.3.5.2.f.3.8.6.c.c.3.a.c.5.1.0.0.0.0.f.f.f.f.!.0.0.0.0.3.b.3.7.3.c.e.0.9.c.a.d.2.6.8.b.3.a.e.8.6.4.5.4.f.4.b.a.2.3.d.7.0.e.5.9.7.7.0.f.!.P.i.c.t.u.r.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_c3cdff3dc5b833acfdddbc409e2196a711873b15_d8cb31ed_1619b505\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16366
Entropy (8bit):	3.7578941116600286
Encrypted:	false
SSDEEP:	192:gWurVHBUZMXSaPXUlXK8zIUGyG/u7sLS274ItI5Xl:zuJBUZMXSasVG/u7sLX4ItI51
MD5:	CBB3FCBBFA1AEB30C25E805AAF9D1C95
SHA1:	A33AB9833EBF6761BB6013109D9396309767FBB5
SHA-256:	0E24AA1162C7AD9FC20F95DFA5970031D830BC0C79A02244A96E352065DC7D7D
SHA-512:	1737D32753F9CA57A85D8AD4DF78811852DF40F321F9C5D4677313D87BD196D1EDB5389CB33A9AB1E73880047F8BDC216D85A361E3F65D8629762E6C6EFD29D
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.2.3.2.0.1.0.4.9.2.6.8.8.0.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.2.3.2.0.1.2.2.9.7.3.7.0.3.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.a.4.a.c.f.0.4.-.4.d.6.7.-.4.3.7.c.-.b.8.f.c.-.2.1.6.7.0.9.8.a.4.3.e.6.....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.=.c.7.e.2.5.4.c.e.-.f.a.4.d.-.4.7.e.9.-.a.d.f.8.-.9.0.6.4.8.2.7.7.4.b.e.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.i.c.t.u.r.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.4.0.-.0.0.0.1.-.0.0.1.b.-.e.c.c.2.-.0.1.2.6.2.6.d.1.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.2.5.c.d.e.6.6.4.5.7.7.b.8.5.8.a.3.5.2.f.3.8.6.c.c.3.a.c.5.1.0.0.0.0.f.f.f.f.!.0.0.0.0.3.b.3.7.3.c.e.0.9.c.a.d.2.6.8.b.3.a.e.8.6.4.5.4.f.4.b.a.2.3.d.7.0.e.5.9.7.7.0.f.!.P.i.c.t.u.r.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Dec 13 08:01:35 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	328688
Entropy (8bit):	3.6198580288230544
Encrypted:	false
SSDEEP:	3072:UU70g2yHjd+pymQZs9gIOgF5g5HY0rXkuyRUCgUj9bC9+5oyd8:j0BJpv9RpDg5HYITj8M5T6
MD5:	C1AF10322B03C9F8A552BB28ECC13EBA
SHA1:	B1E18D8CA8A2361DC45FA1603680EBF23F7E0AEA
SHA-256:	541F2C2A060E8EEFE0E706CC93484CAEF467DF2F10BAD7A71F0DAA2776379176
SHA-512:	056633FC940CF31020A24BB0F0CFD0ED23C6CA71455A897E894B79B435406C379D7808DA1B3757887A79CA245654C14BC1972B9D3EA1EA0C19FB2C177CFB8C2
Malicious:	false
Preview:	MDMP..... ....._..._.....U.....B.....L0.....GenuineIntelW.....T.....H..._.....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...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8400
Entropy (8bit):	3.693980759879209
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAp6Gh6YrUSU7zlEgmfZGS1+prx89b/Gsfi1m:RrlsNim6Gh6Y4SU7zlEgmfkSv/lf5

C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CF.tmp.WERInternalMetadata.xml	
MD5:	CC590D48C5CCFF82C612DD4A30FDB619
SHA1:	CD062A7F98FAC1F901ED03552DAE4563ACD88321
SHA-256:	1CE2767EEFEB35F881F4A8A083E9F2FDF6ECF43C28B96B63C11C3E22A5314113
SHA-512:	266C8ED5E632A3004F1FB54ECDD6B920168D02F7A8F4EA9E35959824317D8A472FB9FA600E57FBD27D566620F85E89826F9B6E6DF4DBA5357D1CD4B9E61D212
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.9.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER313C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.455788378170149
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9GijWSC8BtEf8fm8M4Jwg4FF66+q8ve4VD8mvkAd:uITfjYSSN77Jwm6K3D8mvkAd
MD5:	702332268A87B1C5FCCAC63C33BDEB52
SHA1:	FEFDAD318BFE3A66C26486899AF0165E59CE55D4
SHA-256:	9D1961E84D2434C0D5E698A2D8268F4C558DE8617B201AF13C59DA8EFC886296
SHA-512:	DB08853ADF9F80EAC6AA671B1A05CDF0DC9941F36B8E17944A4D81EEE9BE82609B60739187DC60FB7F66082DECB26ADE8EE7FC120AAB9B45ED079B322B2BBEC1
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="769993" />.. <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\WER4499.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8402
Entropy (8bit):	3.693007348357344
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigM6FvQoiu6YrFSU2zfsOgmfZGS1+prh89bXYsfddm:RrlsNij6R6YJSU2zfsOgmfkSPXLfW
MD5:	97C927519055AE16BFA194BC91C770A2
SHA1:	E6DE1F6BCE5358F3C220A8DDC2B3150A10E19827
SHA-256:	AB03A854F269EC89C89C3CE6513FC8D6B10D745F93417F2D66BF49467E63628B
SHA-512:	1C4CBB6B219AAAA9DBE8388C0B099D98B3C2B198A2C815920782624C907D5F1483B21EDC95F2F11CB9AE3022A72EE39CF79B44C6395038034B892203FD4BBC0
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.4.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.453885994431024
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9GijWSC8Bs8fm8M4Jwg4FFV+q8ve4iD8mvkid:uITfYYSSNXJwJKYD8mvkid
MD5:	6587BF881C2BBC1539A0A73761FB09BF
SHA1:	8E275A66F04346C0B37DF82A1B4310E9E24BD127
SHA-256:	EE6CA846D2DC06F3DDE61784CD9734C4019CD4C25C01751BC37E8FA518C0A557
SHA-512:	AC58651647A9E03431A71A74F3E755D54280D8F8FFF3A851B7396E5A727CAE1D6E610250B1C7AA7659C8601201A0195400C572AA743125906F081EC4019D368E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp.xml	
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="769992" />.. <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\WER66E5.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Dec 13 08:01:53 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	381235
Entropy (8bit):	3.726369952694676
Encrypted:	false
SSDEEP:	3072:Krc70C11jd+pcxQPItf8tXuTqeYE9gIOgF5Bs40pnUCgUr1YTEZoZkVUf5:Z0C1KpcxoId9RpDB5kTjtZke0
MD5:	DCAF4A763463093572CF3413F2DB0631
SHA1:	A19832FE081B35F97815CFFDA1F95896C8F88E5F
SHA-256:	D75A0EEEE5811A1E97DFDFAA729E57141489CF522C778BABB6D7C59B44AEF3A4
SHA-512:	9176F61480FF799FEF3BB8003BBC647D473A7BB5C7EAA34E07E8EBB3AD81BD8C88A715FF90BDFEE06CDD20F4644A074EE84933DADC1F8DA1FCDB1309BE0DA CC9
Malicious:	false
Preview:	MDMP..... .....q..._.....U.....B.....+.....GenuineIntelW.....T.....@...S.._.....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...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C31.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.692160405786034
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiOW6X96YQA6I2gmfZNSS1+prC89bD8sf6hm:RrlsNiX6N6YP6hgmfTSSaDPfl
MD5:	F12D43E7375BD532C4160953F93680BB
SHA1:	C001EFAFE2B476EF477678376F657D8CBCE1D141
SHA-256:	92AE90B0A2F9D21F9CABF09AB7FC00B4EE9C8DF780A5DED4C7E2E33D8BB4311D
SHA-512:	ADB73A899122BF5542BADFB4982F030A3975C56379DD7A9B73811354A255C721A188F781E997273FBC17AC17BFECF8F2B54C41FFF2BCFA276B700058C3470B08
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.6.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EB1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Dec 13 08:02:08 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	319716
Entropy (8bit):	3.6635484587549323
Encrypted:	false
SSDEEP:	3072:3xOpn0q+3rMjd+pDYQLmVmXEKIPZ9gIOgF5Ux0fXtHu8tUCgUBxPVQSMHyou27T:30n0qA9pUQLAPZ9RpD0ktTjLVPkyjaT
MD5:	FD292877F5D1C6C40F173F046962F324
SHA1:	C48A58D1E97C95F47ABBF359349EDB5E65248CC6
SHA-256:	65964A546E09E061E6393A4DB1871CD162209D2F2F1BF4CA8C63E23CDC8B8742
SHA-512:	810164407F01F013273941A83FA575CD05C238AD6138B0E78F7B29D9C5AB70B4635751E52EE6093DBA2D3F4E1DDCCAE4EB08352F3E0A6EF63C8599FD06871AC
Malicious:	false
Preview:	MDMP..... ....._.....U.....B.....D/.....GenuineIntelW.....T.....L...\._.....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...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9143.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4662
Entropy (8bit):	4.450150440567069
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9GijWSC8BtJ8fm8M4JwIwFN+q8v6cLD8mvkyd:uITfYYSSN7uJwnKhD8mvkyd
MD5:	7E4D714F5FC07D4F82F0AAD6A5EDC59D
SHA1:	94819B569BB4D96B5394FB57A261AD69063734F4
SHA-256:	AAA058483D7780AB315361D87C1D3892F591E90D35E10F54A4D80F0F2E0EB120
SHA-512:	F5A7D2D505E07177064000BC625BF4079BA89D2BDF985B2F78563F3C4F5D8DF77A96DB346365AA224A09F164AA78D04B1B1E1D3786ED09735EC0278D2DBECBF D
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="769992" />.. <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\WERD37B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8400
Entropy (8bit):	3.6941514372776383
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJH6zG6YrbSUbzVugmfZGS1+prR89brFsftJk5m:RrlsNiJ6y6Y3SUbzVugmfkSfreftp
MD5:	0478538EFB2FE16D22BEFE4F0E81A643
SHA1:	8D70E3CE33BEB589559A91DE4B246EED25DAC4CE
SHA-256:	A32332DDD34E09FC7F8695271FC5A657971FA05C9C2D7C41A4A49EE45396AF91
SHA-512:	5378571C4D05C630A134A5483CDE1508BA15ADA9A429404494D61BE51E7423A7DDE212334D7BA070E139F55A648CCF50E5F2043DC21C41A54B00ECB29C0E87F
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.8.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDBAA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.457511622378531
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9GijWSC8BtU8fm8M4Jwg4FFyiP+q8ve4dtD8mvkYd:uITfYYSSN7ZJwBPKftD8mvkYd
MD5:	10B2CF41DEAE8A8351371EF0DB2D2648
SHA1:	538C64F46C1D74BA896C905A04EC7E82A1CA160E
SHA-256:	F9218ED3D67A057DF5FB56B675A9C7714E2834F21DAEEE9CF38DCADF54D482E2
SHA-512:	290195C62C9694F418F51DCEB5FD29A80B5F61ED836804363B88DD1BA04FF9F83C34C9A1B5E822B589993573F16424338F40BA284025376676F400DCC9EB6156
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="769992" />.. <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\WERE24F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Dec 13 08:02:32 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	325888
Entropy (8bit):	3.6285567212926466
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE24F.tmp.dmp	
SSDEEP:	3072:1SG80/q8jd+p8NXdWhXLbbGY9glOgF5n80XXEuX8UCgUkNcEujRaBjok189aK:UB0up8jA2Y9RpDn8BTjkKjcBjxHK
MD5:	8E46E3CF56138D21CB385B9640E8B283
SHA1:	5CD89F01AE0863906382C7BDC0117BC4F5E85C55
SHA-256:	617E4F1CD17E9B245552AFF0DEC6EE25B30558B31A6EE84D2186AF92C46D03CF
SHA-512:	A77FE7FB51BB2AF51875D91338F82929810A26735233151E814CEF182E70F0D3CEF5D93A2F6607D94B6A71F54C0A54E9E189EF2E047C5A0C0E73AC29697AEF3B
Malicious:	false
Preview:	MDMP..... ....._.....U.....B.....t/.....GenuineIntelW.....T.....d.._.....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...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Pictures.exe.log	
Process:	C:\Users\user\Desktop\Pictures.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe	
Process:	C:\Users\user\Desktop\Pictures.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23560
Entropy (8bit):	6.2301111727309255
Encrypted:	false
SSDEEP:	384:BHeKiySeg7HNUqYabYBTzlly6LjCOnjNBLUJfl5RxVtFlwJGuYetXnFNS6PDgf2C:BH9ihegDSqYabST5UsJLGflvx/FlwJGp
MD5:	97DF3062B2FDA05A79936B955CFF4351
SHA1:	3B373CE09CAD268B3AE86454F4BA23D70E59770F
SHA-256:	99CC3ED45AB5F25CC7131DE81F5084D476B04AFA9DEF647A0A7D20F1BEB95ADB
SHA-512:	1674B36C55FF1A438627BD73C92C2BD8A88B00F8D3459C94132B5410802359746 70DC8532F4E0D786AC27DCD1822FE6521DE298AFC23E2B097A35966616496CD
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K+._.....D.....b... .....@.. .....f.. ..@.....b..O.....H..... ....H.....text....C... ...D..... ..`.reloc.....F.....@..B..... .....b.....H.....3.....*.r...p.....%.r...p.%.r...p.%.r...p.%.r!..p.(6...*.r...p.....%.r...p.%.r...p.%.r...p.%.rY..p.(6...*.r...p .....%.r...p.%.r...p.%.r...p.(6...**....(7...*..0..R.....r...p.....(.....(....(....#.....@.@[#.....@X(.....8....+.....*...0.....r...p(.....s.....+.....o....(....o.....o....rY..p(....(....o.....o.... ....o.....o.... ....o.....o.... ....o.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Pictures.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\Pictures.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:3:3
MD5:	894A9B94BCC5969B60BD18E8EA9C0DDC
SHA1:	F04A8305CF42ECB7BD5B110ADAB57CE9F68AF30C
SHA-256:	7EE3819BF62F7E4563A2A9476DF6E18A6CD17CCEB30B92F00A24A6C8175E3740
SHA-512:	56088DA0021FBDB8F45EC54B65B929FF335DC38DE3532911125F7783D5FC04142DF54CAA595CBF666E74EE9CF414F8AE8811E4CA3C1AFB14DDE49B15F57CC55
Malicious:	false
Preview:	6464

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\Pictures.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.9544425746945726
Encrypted:	false
SSDEEP:	3:oNt+WfW1M3N:oNwvG3N
MD5:	07404D15FD6211796ACE5BB35AAA3EAB
SHA1:	22854F5FC0F005772FA41B8B3816E08468AD00C8
SHA-256:	E7F738FB66E5FEC38DC7DE9778750EA4AE2C33ECC12ABECD3F8A1D62D42C83FE
SHA-512:	6E0B802303646D08F9BCF327D1FB493C57FD83435E920DDD87136044E047484A8EBCEFBE88C018B539A1A876B754A461ADDDA8865B99BCF329CFCED2E294D7E
Malicious:	false
Preview:	C:\Users\user\Desktop\Pictures.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.2301111727309255
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Pictures.exe
File size:	23560
MD5:	97df3062b2fda05a79936b955cff4351
SHA1:	3b373ce09cad268b3ae86454f4ba23d70e59770f
SHA256:	99cc3ed45ab5f25cc7131de81f5084d476b04afa9def647a0a7d20f1beb95adb
SHA512:	1674b36c55ff1a438627bd73c92c2bd8a88b00f8d3459c94132b5410802359746 70dc8532f4e0d786ac27dcd1822fe6521de298afc23e2b097a35966616496cd
SSDEEP:	384:BHeKiySeg7HNUqYabYBTzlly6LjCOnjNBLUJfl5RxVtFlwJGuYetXnFNS6PDgf2C:BH9ihegDSqYabST5UsJLGflvx/FlwJGp

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K+._.....D.....b... .....@.. .....f....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4062fe
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FD42B4B [Sat Dec 12 02:30:35 2020 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=US, L=New York, OU=Edadebedfbfbdf, O=Bdcbfdcccbeecbabbacdedecdf, CN=Ceefaccdedbfbbaaaadacdbf
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/12/2020 3:30:35 AM 12/12/2021 3:30:35 AM
Subject Chain	• C=US, L=New York, OU=Edadebedfbfbdf, O=Bdcbfdcccbeecbabbacdedecdf, CN=Ceefaccdedbfbbaaaadacdbf
Version:	3
Thumbprint MD5:	DA559288943C5E541A1413DCD339D0D5
Thumbprint SHA-1:	9D5B6BC86775395992A25D21D696D05D634A89D1
Thumbprint SHA-256:	57738207D610994A6136D361387FDBB248EEC709FD3DCBA74EC8A330A9A56ED9
Serial:	00AEC009984FA957F3F48FE3104CA9BABC

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x62ac	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x4800	0x1408	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	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

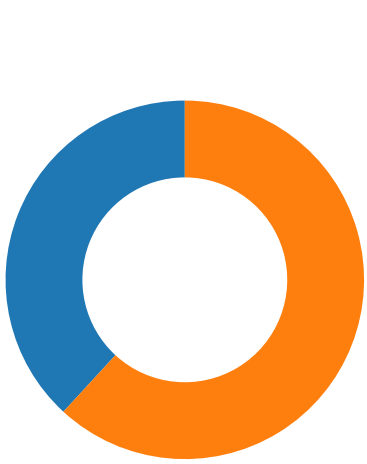
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x4304	0x4400	False	0.415096507353	data	5.84634593861	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.041015625	data	0.0611628522412	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 09:01:16.487791061 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.510068893 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.510797024 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.566931009 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.589230061 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.592657089 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.592685938 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.592804909 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.604289055 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.626605988 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.626746893 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.681402922 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.695121050 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.717421055 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924024105 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924063921 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924094915 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924114943 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924139977 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.924144030 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924171925 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924185038 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.924200058 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924237013 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924248934 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924263954 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924266100 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.924273968 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924289942 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924299955 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924314022 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924323082 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924338102 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924348116 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924361944 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924376011 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:16.924470901 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:16.924544096 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010344028 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010400057 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010453939 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010488987 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010535002 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010562897 CET	443	49749	172.67.143.180	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 09:01:17.010565042 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010582924 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010606050 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010657072 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010689974 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010726929 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010735035 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010740995 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010771990 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010803938 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010833025 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010867119 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.010870934 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010910988 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010950089 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.010994911 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011001110 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011023998 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011054039 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011091948 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011094093 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011096954 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011132956 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011169910 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011215925 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011236906 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011240959 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011249065 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011286974 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011317015 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011324883 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011363029 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011392117 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.011399031 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.011430979 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.013441086 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.056524992 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.094012976 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094034910 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094048023 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094055891 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094070911 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094086885 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094105005 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094125032 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094134092 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.094142914 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094161034 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094183922 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094197989 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094219923 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094237089 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094249964 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.094259024 CET	49749	443	192.168.2.4	172.67.143.180
Dec 13, 2020 09:01:17.094261885 CET	443	49749	172.67.143.180	192.168.2.4
Dec 13, 2020 09:01:17.094285965 CET	443	49749	172.67.143.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 09:01:07.117855072 CET	51726	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:07.144911051 CET	53	51726	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:07.780612946 CET	56794	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:07.804809093 CET	53	56794	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 09:01:08.583662987 CET	56534	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:08.619175911 CET	53	56534	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:09.278830051 CET	56627	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:09.315783024 CET	53	56627	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:10.104551077 CET	56621	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:10.137147903 CET	53	56621	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:12.246356010 CET	63116	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:12.273403883 CET	53	63116	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:13.063663006 CET	64078	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:13.099335909 CET	53	64078	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:13.982692957 CET	64801	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:14.006998062 CET	53	64801	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:14.875528097 CET	61721	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:14.899744987 CET	53	61721	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:15.870129108 CET	51255	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:15.894267082 CET	53	51255	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:16.433238029 CET	61522	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:16.465677023 CET	53	61522	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:16.781209946 CET	52337	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:16.805493116 CET	53	52337	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:17.429711103 CET	55046	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:17.453968048 CET	53	55046	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:34.059462070 CET	49612	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:34.083739042 CET	53	49612	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:38.094436884 CET	49285	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:38.130075932 CET	53	49285	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:39.192804098 CET	50601	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:39.227588892 CET	53	50601	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:43.690452099 CET	60875	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:43.723305941 CET	53	60875	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:50.819103956 CET	56448	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:50.851902008 CET	53	56448	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:55.112220049 CET	59172	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:55.146486044 CET	53	59172	8.8.8.8	192.168.2.4
Dec 13, 2020 09:01:58.418241978 CET	62420	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:01:58.442744970 CET	53	62420	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:04.271701097 CET	60579	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:04.296154976 CET	53	60579	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:09.147290945 CET	50183	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:09.214890003 CET	53	50183	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:09.634826899 CET	61531	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:09.685215950 CET	53	61531	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:10.038877010 CET	49228	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:10.074387074 CET	53	49228	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:10.445342064 CET	59794	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:10.478070021 CET	53	59794	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:11.405864000 CET	55916	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:11.443872929 CET	53	55916	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:11.771887064 CET	52752	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:11.804393053 CET	53	52752	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:12.120671034 CET	60542	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:12.147738934 CET	53	60542	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:12.558737993 CET	60689	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:12.574285984 CET	64206	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:12.585782051 CET	53	60689	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:12.609813929 CET	53	64206	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:13.054713011 CET	50904	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:13.090099096 CET	53	50904	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:13.354191065 CET	57525	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:13.387249947 CET	53	57525	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:14.419780016 CET	53814	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:14.443931103 CET	53	53814	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:15.163750887 CET	53418	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:15.196762085 CET	53	53418	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 09:02:16.313414097 CET	62833	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:16.358726978 CET	53	62833	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:17.037868977 CET	59260	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:17.071844101 CET	53	59260	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:18.221879005 CET	49944	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:18.257651091 CET	53	49944	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:30.878645897 CET	63300	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:30.902821064 CET	53	63300	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:32.494139910 CET	61449	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:32.518338919 CET	53	61449	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:37.862979889 CET	51275	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:37.896147966 CET	53	51275	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:39.831494093 CET	63492	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:39.866903067 CET	53	63492	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:44.319679976 CET	58945	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:44.344043970 CET	53	58945	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:48.099230051 CET	60779	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:48.123490095 CET	53	60779	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:52.501990080 CET	64014	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:52.537776947 CET	53	64014	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:53.513276100 CET	57091	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:53.537516117 CET	53	57091	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:54.773585081 CET	55904	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:54.821656942 CET	53	55904	8.8.8.8	192.168.2.4
Dec 13, 2020 09:02:58.513851881 CET	52109	53	192.168.2.4	8.8.8.8
Dec 13, 2020 09:02:58.546385050 CET	53	52109	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 13, 2020 09:01:16.433238029 CET	192.168.2.4	8.8.8.8	0xf901	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:38.094436884 CET	192.168.2.4	8.8.8.8	0xe00a	Standard query (0)	164.204.10.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Dec 13, 2020 09:01:39.192804098 CET	192.168.2.4	8.8.8.8	0x7fe2	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:50.819103956 CET	192.168.2.4	8.8.8.8	0xfb36	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:58.418241978 CET	192.168.2.4	8.8.8.8	0xa51c	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:12.574285984 CET	192.168.2.4	8.8.8.8	0x2f26	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:15.163750887 CET	192.168.2.4	8.8.8.8	0x3fb8	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:17.037868977 CET	192.168.2.4	8.8.8.8	0xaa21	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:39.831494093 CET	192.168.2.4	8.8.8.8	0x328a	Standard query (0)	164.204.10.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Dec 13, 2020 09:02:58.513851881 CET	192.168.2.4	8.8.8.8	0x1cf8	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 13, 2020 09:01:16.465677023 CET	8.8.8.8	192.168.2.4	0xf901	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:16.465677023 CET	8.8.8.8	192.168.2.4	0xf901	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:16.465677023 CET	8.8.8.8	192.168.2.4	0xf901	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:38.130075932 CET	8.8.8.8	192.168.2.4	0xe00a	Name error (3)	164.204.10.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Dec 13, 2020 09:01:39.227588892 CET	8.8.8.8	192.168.2.4	0x7fe2	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 13, 2020 09:01:39.227588892 CET	8.8.8.8	192.168.2.4	0x7fe2	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:39.227588892 CET	8.8.8.8	192.168.2.4	0x7fe2	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:50.851902008 CET	8.8.8.8	192.168.2.4	0xfb36	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:50.851902008 CET	8.8.8.8	192.168.2.4	0xfb36	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:50.851902008 CET	8.8.8.8	192.168.2.4	0xfb36	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:58.442744970 CET	8.8.8.8	192.168.2.4	0xa51c	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:58.442744970 CET	8.8.8.8	192.168.2.4	0xa51c	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:01:58.442744970 CET	8.8.8.8	192.168.2.4	0xa51c	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:12.609813929 CET	8.8.8.8	192.168.2.4	0x2f26	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:12.609813929 CET	8.8.8.8	192.168.2.4	0x2f26	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:12.609813929 CET	8.8.8.8	192.168.2.4	0x2f26	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:15.196762085 CET	8.8.8.8	192.168.2.4	0x3fb8	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:15.196762085 CET	8.8.8.8	192.168.2.4	0x3fb8	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:15.196762085 CET	8.8.8.8	192.168.2.4	0x3fb8	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:17.071844101 CET	8.8.8.8	192.168.2.4	0xaa21	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Dec 13, 2020 09:02:39.866903067 CET	8.8.8.8	192.168.2.4	0x328a	Name error (3)	164.204.10.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Dec 13, 2020 09:02:58.546385050 CET	8.8.8.8	192.168.2.4	0x1cf8	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

HTTPS Packets

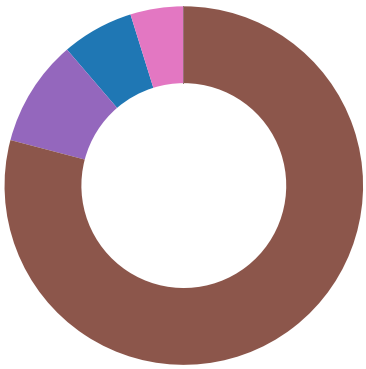
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 13, 2020 09:01:16.592685938 CET	172.67.143.180	443	192.168.2.4	49749	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 25 02:00:00 CEST 2020	Sun Jul 25 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 13, 2020 09:01:39.361706018 CET	104.24.126.89	443	192.168.2.4	49755	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 25 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 25 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



- Pictures.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Pictures.exe
- WerFault.exe
- Pictures.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Pictures.exe
- WerFault.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Pictures.exe
- Pictures.exe
- WerFault.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Pictures.exe
- cmd.exe
- conhost.exe
- timeout.exe
- Pictures.exe
- WerFault.exe
- Pictures.exe

Click to jump to process

System Behavior

Analysis Process: Pictures.exe PID: 1492 Parent PID: 5912

General

Start time:	09:01:12
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pictures.exe'

Imagebase:	0x960000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.746517106.0000000003E88000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.746517106.0000000003E88000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.746517106.0000000003E88000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.746517106.0000000003E88000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.746517106.0000000003E88000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D02CF06	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	6D02CF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.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	6BE7DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BE7DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe	0	23560	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 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 02 00 4b 2b d4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 44 00 00 00 02 00 00 00 00 00 00 fe 62 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 04 00 00 00 00 00 00 00 00 a0 00 00 00 02 00 00 ff 66 00 00 02 00 40 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...K+._.......... ....D...........b... ....@.. ....f....@................	success or wait	1	6BE7DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6BE7DD66	CopyFileW

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	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D005705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D00CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE71B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Users\user\Desktop\Pictures.exe	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Users\user\Desktop\Pictures.exe	unknown	512	success or wait	1	6CFED72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	<Unknown>	unicode	C:\Users\user\Desktop\Pictures.exe	success or wait	1	6BE7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	shell	unicode	explorer.exe,"C:\Users\user\Desktop\Pictures.exe"	success or wait	1	6BE7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Pictures.exe	unicode	C:\Users\user\Desktop\Pictures.exe	success or wait	1	6BE7646A	RegSetValueExW

Analysis Process: cmd.exe PID: 1380 Parent PID: 1492

General

Start time:	09:01:13
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 4.769
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: 3220 Parent PID: 1380

General

Start time:	09:01:14
Start date:	13/12/2020
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: timeout.exe PID: 616 Parent PID: 1380

General

Start time:	09:01:14
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe

Wow64 process (32bit):	true
Commandline:	timeout 4.769
Imagebase:	0x1190000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: Pictures.exe PID: 6464 Parent PID: 1492

General

Start time:	09:01:23
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pictures.exe
Imagebase:	0xef0000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.817381181.0000000004281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.817381181.0000000004281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.814621175.000000000351A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.814621175.000000000351A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000002.807250814.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.807250814.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.807250814.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.807250814.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.807250814.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.812978942.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.812978942.0000000003281000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.814706345.000000000352A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D02CF06	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	6D02CF06	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE71E60	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE71E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	6BE76A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	6BE76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 34 36 34	6464	success or wait	1	6BE71B4F	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	35	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 50 69 63 74 75 72 65 73 2e 65 78 65	C:\Users\user\Desktop\Pictures.exe	success or wait	1	6BE71B4F	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	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D005705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D00CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE71B4F	ReadFile
C:\Users\user\Desktop\Pictures.exe	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Users\user\Desktop\Pictures.exe	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFED72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	6BE71B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	6BE71B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	6BE71B4F	ReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	6BE7C075	RegSetValueExW

Analysis Process: WerFault.exe PID: 6804 Parent PID: 1492

General

Start time:	09:01:25
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1492 -s 928
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F361717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F35497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	success or wait	1	6F354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	success or wait	1	6F354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp.xml	success or wait	1	6F354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4861.tmp.csv	success or wait	1	6F354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CD6.tmp.txt	success or wait	1	6F354BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 5f ca d5 5f a4 05 12 00 00 00 00 00	MDMP..... ....._.._.....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 4c 30 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 d4 05 00 00 48 ca d5 5f 00 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......L0.... ..GenuineIntelW...........T... ....H.._................. ....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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 08 ed cf 00 05 00 00 00 00 00 00 00 05 00 00 00 48 ec cf 00 a0 ec cf 00 22 d7 ae 74 23 00 00 00 16 02 00 00 48 ec cf 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........................H... ...."..t#.......H...+.........	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	168	14 06 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 ae 74 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e9 6c 00 00 00 00 f0 27 ef 00 00 00 00 00 88 ed cf 00 00 00 00 00 00 01 00 00 00 00 00 00 00 10 ed cf 00 00 00 00 00 08 ed cf 00 00 00 00 00 f4 76 ea 6c 00 00 00 00 d4 e9 b1 07 00 00 00 00 f0 27 ef 00 00 00 00 00 7a 77 ea 6c 00 00 00 00 68 ec cf 00 00 00 00 00 cc 02 00 00 b0 3a 00 00	........RCC............."..t.. ....l.....'........ .... .v.l............'......zw.l.. ..h............:..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	20	02 03 00 00 84 12 29 05 00 00 00 00 01 00 00 00 60 9a 00 00	......).........`...	success or wait	770	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	1	f8	.	success or wait	769	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	72	48 00 00 00 02 00 05 00 50 e7 02 00 60 31 05 00 09 00 00 00 00 00 00 00 b0 18 08 00 c0 91 00 00 70 aa 08 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	H.......P...`1................ ..p......................................	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	4	10 00 00 00	....	success or wait	16	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 e0 dd cf 00 bc 9a 11 77 23 00 00 00 16 02 00 00 50 dc cf 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... ....w#.......P...+.........	success or wait	16	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	48	b4 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 60 a3 00 00 00 00 00 88 f9 97 06 00 00 00 00 78 06 00 00 27 a8 03 00 cc 02 00 00 70 67 00 00	....`..... ..x...'.....pg..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	4	54 00 00 00	T...	success or wait	84	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	30	18 00 00 00 50 00 69 00 63 00 74 00 75 00 72 00 65 00 73 00 2e 00 65 00 78 00 65 00 00 00	....P.i.c.t.u.r.e.s...e.x.e...	success or wait	84	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	120	00 00 3a 6f 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 30 3a 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..:o.....`.Z0:..... .....?..... .....) ..@A.....	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	668	00 00 f2 72 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 92 3a 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 a3 02 00 00 00 00 00 10 2d 03 00 00 00 00 c5 60 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 f3 6b 03 00 00 00 00 00 36 7b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 6f 1a 00 00 00 00 00 d8 8f 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 08 a1 05 00 00 00 00 00 b6 17 d8 3f 01 00 00 00 eb fe 2b 17 00 00 00 00 fa 01 00 0e 00 00 00 00 00 85 03 f1 00 00 00 00 00 19 a7 00 00 1b d5 00 00 56 50 05 00 bc 54 0a 00 d8 8f 05 00 fb 7e 15 00 08 a1 05 00 a9 f2 23 00 6e 4b 01 00 a2 71 12 00 00 00 00 00 70 42 11 00 fa b5 04	...r.....*,..:.....Zb ....0.....- .....`.....k.. ....6{.....ho..... .....@.....?.... ..+..... ..VP...T.....~.....#.nK.. .q.....pB.....	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	34706	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 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 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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2558.tmp.dmp	unknown	120	03 00 00 00 04 03 00 00 08 07 00 00 04 00 00 00 74 23 00 00 18 0a 00 00 0e 00 00 00 3c 00 00 00 8c 2d 00 00 05 00 00 00 24 30 00 00 3c 6a 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 48 54 00 00 f0 af 04 00 15 00 00 00 ec 01 00 00 c8 2d 00 00 16 00 00 00 98 00 00 00 b4 2f 00 00	.....t#.....<....-.....$0..<j.....`....8.....T.....HT.....-...../..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 34 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.4.9.2.<./.P.i.d.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 50 00 69 00 63 00 74 00 75 00 72 00 65 00 73 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.>.P.i.c.t.u.r.e.s...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 36 00 31 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.3.6.1.6.<./.U.p.t.i.m.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 34 00 37 00 39 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.6.4.7.9.8.2.0.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 34 00 37 00 39 00 30 00 30 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.6.4.7.9.0.0.1.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 32 00 36 00 32 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.2.7.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 38 00 34 00 35 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.8.8.4.5.5.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 36 00 38 00 37 00 35 00 33 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.6.8.7.5.3.9.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 35 00 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.3.5.4.4.5.6.<./.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 35 00 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.4.4.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 32 00 33 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.32.3.4.9.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 32 00 33 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.3.2.2.4.<./.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 35 00 33 00 35 00 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.3.5.6.3.3.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 35 00 39 00 31 00 33 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.1.3.3.9.5.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 35 00 33 00 35 00 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.3.5.6.3.3.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 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	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 36 00 30 00 30 00 35 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.>.7.1.6.0.0.5.3.<./.U.p.t.i.m.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 34 00 39 00 32 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.9.2.8.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 30 00 36 00 39 00 32 00 36 00 30 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.9.2.6.0.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 30 00 36 00 32 00 37 00 38 00 39 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.2.7.8.9.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 35 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.1.5.1.1.2.<./.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	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 31 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.0.1.6.6.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.7.5.3.2.8.<./.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 30 00 38 00 38 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.>.7.4.0.8.8.<./.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 35 00 36 00 35 00 35 00 36 00 38 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.>.3.5.6.5.5.6.8.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 34 00 38 00 31 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.4.8.1.9.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 33 00 35 00 36 00 35 00 35 00 36 00 38 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.>.3.5.6.5.5.6.8.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 50 00 69 00 63 00 74 00 75 00 72 00 65 00 73 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.P.i.c.t.u.r.e.s...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 68 00 6c 00 71 00 62 00 78 00 67 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.>.h.l.q.b.x.g.,. .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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 68 00 6c 00 71 00 62 00 78 00 67 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.>.h.l.q.b.x.g.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 35 00 33 00 32 00 31 00 32 00 32 00 33 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.3.2.1.2.2.3.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 30 00 2d 00 31 00 32 00 2d 00 31 00 33 00 54 00 30 00 38 00 3a 00 30 00 31 00 3a 00 33 00 36 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.2.-.1.3.T.0.8.:.0.1.:.3.6.Z.".>.	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 34 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 31 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.6.3.". .P.I.D.=.".1.4.9.2.". .U.p.t.i.m.e.M.S.=.".1.1.1.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.1.1.7.1.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 63 00 32 00 31 00 34 00 65 00 66 00 39 00 2d 00 34 00 38 00 32 00 31 00 2d 00 34 00 35 00 32 00 63 00 2d 00 61 00 39 00 39 00 37 00 2d 00 33 00 31 00 61 00 33 00 64 00 31 00 39 00 34 00 65 00 63 00 62 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.c.2.1.4.e.f.9.-.4.8.2.1.-.4.5.2.c.-.a.9.9.7.-.3.1.a.3.d.1.9.4.e.c.b.9.<./.G.u.i.d.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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 30 00 2d 00 31 00 32 00 2d 00 31 00 33 00 54 00 30 00 38 00 3a 00 30 00 31 00 3a 00 33 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.2.-.1.3.T.0.8.:.0.1.:.3.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4499.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	6F35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4853.tmp.xml	unknown	4678	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\Report.wer	unknown	2	ff fe	..	success or wait	1	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\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	216	6F35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Pictures.exe_8de45086902aa2ba8efa51809173eaf73c535_065d0aef_1af963d8\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 39 00 35 00 37 00 37 00 34 00 30 00 39 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.4.9.5.7.7.4.0.9.5.	success or wait	1	6F35497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe\ada2a7b2	success or wait	1	6F3736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F371FB2	RegCreateKeyExW
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe\ada2a7b2	ProgramId	unicode	00069c25cde664577b858a352f386cc3ac510000ffff	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe\ada2a7b2	FileId	unicode	00003b373ce09cad268b3ae86454f4ba23d70e59770f	success or wait	1	6F3736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	LowerCaseLongPath	unicode	c:\users\user\desktop\pictures.exe	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	LongPathHash	unicode	pictures.exe|ada2a7b2	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	Name	unicode	pictures.exe	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	Publisher	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	Version	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	BinFileVersion	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	BinaryType	unicode	pe32_clr_32	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	ProductName	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	ProductVersion	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	LinkDate	unicode	12/12/2020 02:30:35	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	BinProductVersion	unicode		success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	Size	B	08 5C 00 00 00 00 00 00	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	Language	dword	0	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	IsPeFile	dword	1	success or wait	1	6F3736BF	unknown
\REGISTRY\A\{d2f5d555-dc90-92e2-0fb3-c62b1c949584}\Root\InventoryApplicationFile\pictures.exe|ada2a7b2	IsOsComponent	dword	0	success or wait	1	6F3736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 AE 74 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E9 6C F0 27 EF 00 88 ED CF 00 01 00 00 00 10 ED CF 00 08 ED CF 00 F4 76 EA 6C D4 E9 B1 07 F0 27 EF 00 7A 77 EA 6C 68 EC CF 00	success or wait	1	6F371FE8	RegSetValueExW

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

Analysis Process: Pictures.exe PID: 6988 Parent PID: 3424

General

Start time:	09:01:32
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pictures.exe'
Imagebase:	0x180000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000C.00000002.874949951.00000000043AC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000C.00000002.882295269.00000000061BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.882295269.00000000061BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000C.00000002.882295269.00000000061BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000002.882295269.00000000061BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000C.00000002.882295269.00000000061BC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D02CF06	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	6D02CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D005705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D00CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D005705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE71B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFED72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6CFED72F	unknown
C:\Users\user\Desktop\Pictures.exe	unknown	4096	success or wait	1	6CFED72F	unknown
C:\Users\user\Desktop\Pictures.exe	unknown	512	success or wait	1	6CFED72F	unknown

Analysis Process: cmd.exe PID: 7116 Parent PID: 6988

General

Start time:	09:01:33
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 4.769
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

Analysis Process: conhost.exe PID: 4600 Parent PID: 7116

General

Start time:	09:01:34
Start date:	13/12/2020
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: timeout.exe PID: 6488 Parent PID: 7116

General

Start time:	09:01:34
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4.769
Imagebase:	0x1190000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Pictures.exe PID: 3984 Parent PID: 3424

General

Start time:	09:01:40
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pictures.exe'
Imagebase:	0x780000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.888849131.00000000041D6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.888849131.00000000041D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.888849131.00000000041D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.888849131.00000000041D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.888849131.00000000041D6000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: WerFault.exe PID: 5748 Parent PID: 6464

General

Start time:	09:01:40
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 1840
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000013.00000003.746755143.00000000058A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000003.746755143.00000000058A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000003.746755143.00000000058A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: cmd.exe PID: 4684 Parent PID: 3984

General

Start time:	09:01:42
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 4.769
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

Analysis Process: conhost.exe PID: 5048 Parent PID: 4684

General

Start time:	09:01:42
Start date:	13/12/2020
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: timeout.exe PID: 5712 Parent PID: 4684

General

Start time:	09:01:43
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4.769
Imagebase:	0x1190000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Pictures.exe PID: 5868 Parent PID: 6988

General

Start time:	09:01:48
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pictures.exe
Imagebase:	0x8f0000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000017.00000002.780102732.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000002.780102732.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.780102732.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000002.780102732.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000017.00000002.780102732.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: Pictures.exe PID: 4604 Parent PID: 3424

General

Start time:	09:01:49
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pictures.exe'
Imagebase:	0x910000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000018.00000002.837966470.0000000003F76000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000018.00000002.837966470.0000000003F76000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000018.00000002.837966470.0000000003F76000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000018.00000002.837966470.0000000003F76000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000018.00000002.837966470.0000000003F76000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000018.00000002.841324147.00000000040A2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000018.00000002.841324147.00000000040A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000018.00000002.841324147.00000000040A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000018.00000002.841324147.00000000040A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000018.00000002.841324147.00000000040A2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: WerFault.exe PID: 6772 Parent PID: 6988

General

Start time:	09:01:51

Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6988 -s 1092
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: 6208 Parent PID: 4604

General

Start time:	09:01:51
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 4.769
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6964 Parent PID: 6208

General

Start time:	09:01:52
Start date:	13/12/2020
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

Analysis Process: timeout.exe PID: 6524 Parent PID: 6208

General

Start time:	09:01:52
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4.769
Imagebase:	0x1190000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Pictures.exe PID: 6836 Parent PID: 3424

General

Start time:	09:01:57
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pictures.exe'
Imagebase:	0xde0000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001F.00000002.988442141.0000000004250000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001F.00000002.988442141.0000000004250000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001F.00000002.988442141.0000000004250000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001F.00000002.988442141.0000000004250000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001F.00000002.988442141.0000000004250000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: cmd.exe PID: 6012 Parent PID: 6836

General

Start time:	09:02:00
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 4.769
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1424 Parent PID: 6012

General

Start time:	09:02:00
Start date:	13/12/2020
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

Analysis Process: timeout.exe PID: 5932 Parent PID: 6012

General

Start time:	09:02:01
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4.769
Imagebase:	0x1190000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Pictures.exe PID: 1572 Parent PID: 3984

General

Start time:	09:02:01
Start date:	13/12/2020
Path:	C:\Users\user\Desktop\Pictures.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pictures.exe
Imagebase:	0xd50000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000023.00000002.780175587.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000023.00000002.780175587.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000023.00000002.780175587.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000023.00000002.780175587.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000023.00000002.780175587.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: WerFault.exe PID: 4928 Parent PID: 3984

General

Start time:	09:02:04
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3984 -s 1652
Imagebase:	0x1150000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Pictures.exe PID: 6576 Parent PID: 3424

General

Start time:	09:02:06
Start date:	13/12/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Pictures.exe'
Imagebase:	0x1e0000
File size:	23560 bytes
MD5 hash:	97DF3062B2FDA05A79936B955CFF4351
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.869677007.0000000003FC6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.869677007.0000000003FC6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.869677007.0000000003FC6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.869677007.0000000003FC6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.869677007.0000000003FC6000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.866236197.000000000399A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 16%, Metadefender, Browse • Detection: 41%, ReversingLabs

Disassembly

Code Analysis