ID: 319686
Sample Name: INQUIRY.exe
Cookbook: default.jbs
Time: 15:00:58
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

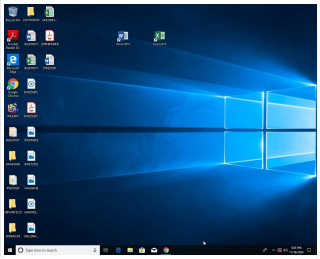
Analysis Report INQUIRY.exe

Overview

General Information

Sample Name:	INQUIRY.exe
Analysis ID:	319686
MD5:	0b940145d7d02e..
SHA1:	53ae0b576f7b362.
SHA256:	bf487ff7cdbbd99…
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

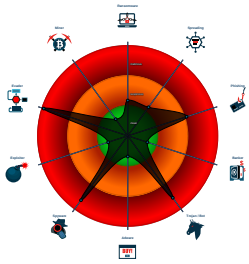
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process

Classification



Startup

- **System is w10x64**
- INQUIRY.exe (PID: 2016 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' MD5: 0B940145D7D02E5B1B975C99DD5197A4)
  - INQUIRY.exe (PID: 5896 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' MD5: 0B940145D7D02E5B1B975C99DD5197A4)
    - dw20.exe (PID: 6868 cmdline: dw20.exe -x -s 2308 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
    - vbc.exe (PID: 6664 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6700 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - WerFault.exe (PID: 6776 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5896 -s 2216 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - INQUIRY.exe (PID: 5788 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' 2 5896 5358953 MD5: 0B940145D7D02E5B1B975C99DD5197A4)
    - INQUIRY.exe (PID: 6076 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
      - INQUIRY.exe (PID: 6808 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
        - dw20.exe (PID: 6936 cmdline: dw20.exe -x -s 2272 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
        - vbc.exe (PID: 5684 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
        - vbc.exe (PID: 4184 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
        - WerFault.exe (PID: 1076 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6808 -s 2324 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - INQUIRY.exe (PID: 6792 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' 2 6808 5404546 MD5: 0B940145D7D02E5B1B975C99DD5197A4)
        - INQUIRY.exe (PID: 6400 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
          - INQUIRY.exe (PID: 240 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
            - dw20.exe (PID: 204 cmdline: dw20.exe -x -s 2100 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
          - INQUIRY.exe (PID: 6428 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' 2 240 5445406 MD5: 0B940145D7D02E5B1B975C99DD5197A4)
            - INQUIRY.exe (PID: 6900 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
              - INQUIRY.exe (PID: 1364 cmdline: C:\Users\user\Desktop\INQUIRY.exe MD5: 0B940145D7D02E5B1B975C99DD5197A4)
                - dw20.exe (PID: 6380 cmdline: dw20.exe -x -s 2284 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
                - vbc.exe (PID: 5396 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
                - vbc.exe (PID: 3064 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
                - WerFault.exe (PID: 7076 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1364 -s 2096 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
              - INQUIRY.exe (PID: 4424 cmdline: 'C:\Users\user\Desktop\INQUIRY.exe' 2 1364 5460187 MD5: 0B940145D7D02E5B1B975C99DD5197A4)
- **cleanup**

Malware Configuration

Threatname: HawkEye

```
{
  "Modules": [
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x59d3e3:$key: HawkEyeKeylogger • 0x59f613:$salt: 099u787978786 • 0x59da24:$string1: HawkEye_Keylogger • 0x59e863:$string1: HawkEye_Keylogger • 0x59f573:$string1: HawkEye_Keylogger • 0x59ddf9:$string2: holdermail.txt • 0x59de19:$string2: holdermail.txt • 0x59dd3b:$string3: wallet.dat • 0x59dd53:$string3: wallet.dat • 0x59dd69:$string3: wallet.dat • 0x59f137:$string4: Keylog Records • 0x59f44f:$string4: Keylog Records • 0x59f66b:$string5: do not script --> • 0x59d3cb:$string6: \pidloc.txt • 0x59d459:$string7: BSPLIT • 0x59d469:$string7: BSPLIT
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x59da7c:$hawkstr1: HawkEye Keylogger • 0x59e8a9:$hawkstr1: HawkEye Keylogger • 0x59ebd8:$hawkstr1: HawkEye Keylogger • 0x59ed33:$hawkstr1: HawkEye Keylogger • 0x59ee96:$hawkstr1: HawkEye Keylogger • 0x59f10f:$hawkstr1: HawkEye Keylogger • 0x59d60a:$hawkstr2: Dear HawkEye Customers! • 0x59ec2b:$hawkstr2: Dear HawkEye Customers! • 0x59ed82:$hawkstr2: Dear HawkEye Customers! • 0x59eee9:$hawkstr2: Dear HawkEye Customers! • 0x59d72b:$hawkstr3: HawkEye Logger Details:
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x5a504d:$key: HawkEyeKeylogger • 0x5a727d:$salt: 099u787978786 • 0x5a568e:$string1: HawkEye_Keylogger • 0x5a64cd:$string1: HawkEye_Keylogger • 0x5a71dd:$string1: HawkEye_Keylogger • 0x5a5a63:$string2: holdermail.txt • 0x5a5a83:$string2: holdermail.txt • 0x5a59a5:$string3: wallet.dat • 0x5a59bd:$string3: wallet.dat • 0x5a59d3:$string3: wallet.dat • 0x5a6da1:$string4: Keylog Records • 0x5a70b9:$string4: Keylog Records • 0x5a72d5:$string5: do not script --> • 0x5a5035:$string6: \pidloc.txt • 0x5a50c3:$string7: BSPLIT • 0x5a50d3:$string7: BSPLIT
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 4 entries				

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b89c:$key: HawkEyeKeylogger • 0x7dacc:$salt: 099u787978786 • 0x7bedd:$string1: HawkEye_Keylogger • 0x7cd1c:$string1: HawkEye_Keylogger • 0x7da2c:$string1: HawkEye_Keylogger • 0x7c2b2:$string2: holdermail.txt • 0x7c2d2:$string2: holdermail.txt • 0x7c1f4:$string3: wallet.dat • 0x7c20c:$string3: wallet.dat • 0x7c222:$string3: wallet.dat • 0x7d5f0:$string4: Keylog Records • 0x7d908:$string4: Keylog Records • 0x7db24:$string5: do not script --> • 0x7b884:$string6: \pidloc.txt • 0x7b912:$string7: BSPLIT • 0x7b922:$string7: BSPLIT
00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bf35:$hawkstr1: HawkEye Keylogger • 0x7cd62:$hawkstr1: HawkEye Keylogger • 0x7d091:$hawkstr1: HawkEye Keylogger • 0x7d1ec:$hawkstr1: HawkEye Keylogger • 0x7d34f:$hawkstr1: HawkEye Keylogger • 0x7d5c8:$hawkstr1: HawkEye Keylogger • 0x7bac3:$hawkstr2: Dear HawkEye Customers! • 0x7d0e4:$hawkstr2: Dear HawkEye Customers! • 0x7d23b:$hawkstr2: Dear HawkEye Customers! • 0x7d3a2:$hawkstr2: Dear HawkEye Customers! • 0x7bbe4:$hawkstr3: HawkEye Logger Details:
Click to see the 197 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
16.1.INQUIRY.exe.400000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x112984:$key: HawkEyeKeylogger • 0x114bb4:$salt: 099u787978786 • 0x112fc5:$string1: HawkEye_Keylogger • 0x113e04:$string1: HawkEye_Keylogger • 0x114b14:$string1: HawkEye_Keylogger • 0x11339a:$string2: holdermail.txt • 0x1133ba:$string2: holdermail.txt • 0x1132dc:$string3: wallet.dat • 0x1132f4:$string3: wallet.dat • 0x11330a:$string3: wallet.dat • 0x1146d8:$string4: Keylog Records • 0x1149f0:$string4: Keylog Records • 0x114c0c:$string5: do not script --> • 0x11296c:$string6: \pidloc.txt • 0x1129fa:$string7: BSPLIT • 0x112a0a:$string7: BSPLIT
16.1.INQUIRY.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
16.1.INQUIRY.exe.400000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
16.1.INQUIRY.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 156 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

Installs a global keyboard hook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

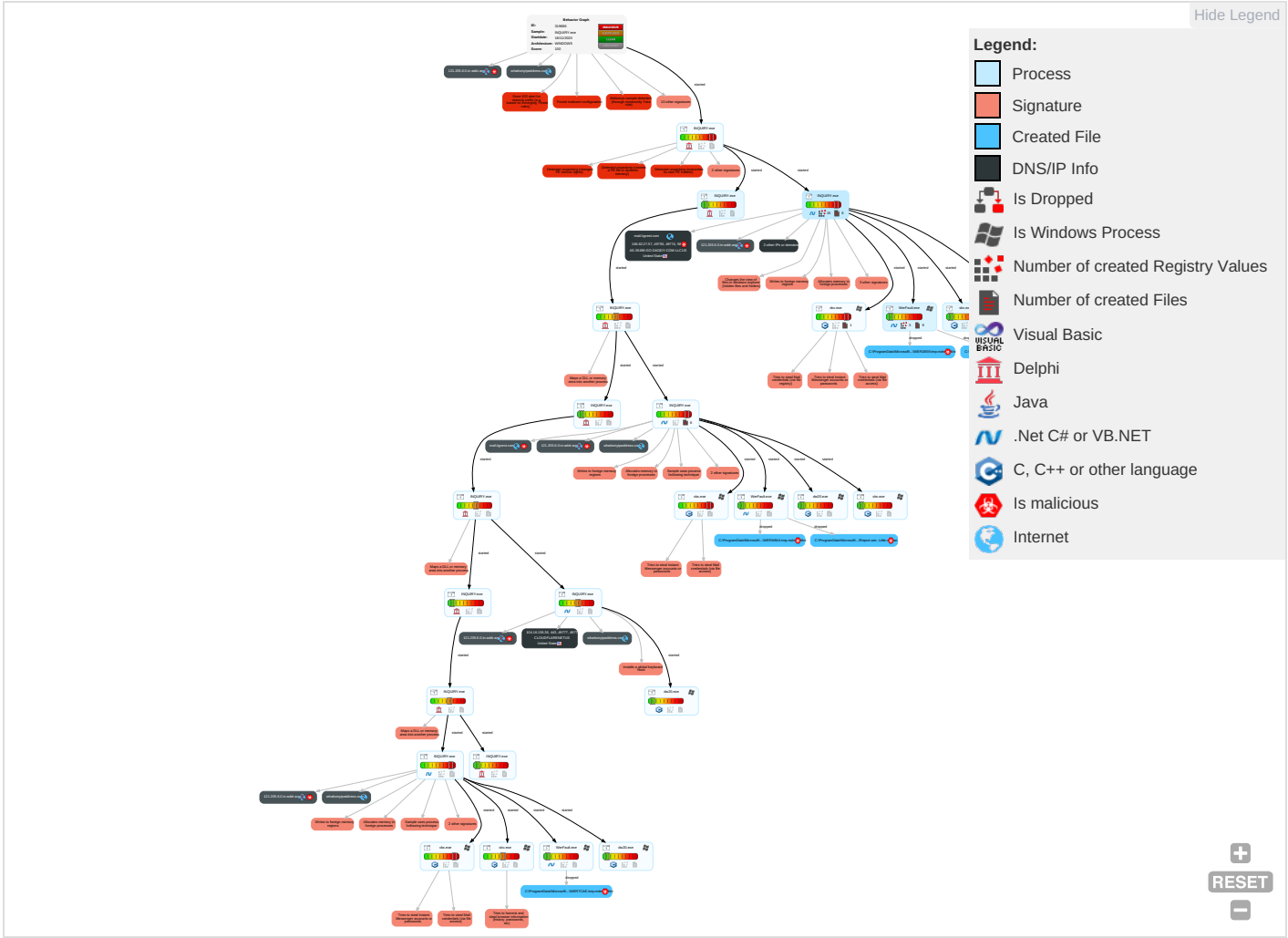
Yara detected HawkEye Keylogger

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	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over C Network Medium
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 5 1 1	Obfuscated Files or Information 2 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 4 1	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 9	SSH	Input Capture 2 1 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Query Registry 1	VNC	Clipboard Data 3	Exfiltration Over C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Security Software Discovery 1 10 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 6	Proc Filesystem	Virtualization/Sandbox Evasion 6	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encryp Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encry Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfu Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over U
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Used P

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
INQUIRY.exe	44%	Virustotal		Browse
INQUIRY.exe	42%	ReversingLabs	Win32.Trojan.Wacatac	
INQUIRY.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File

Source	Detection	Scanner	Label	Link	Download
16.2.INQUIRY.exe.22e0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
32.2.INQUIRY.exe.2680000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
32.2.INQUIRY.exe.2680000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.1.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.INQUIRY.exe.21e0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
33.1.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.INQUIRY.exe.2270000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.INQUIRY.exe.2270000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
13.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
28.1.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.INQUIRY.exe.2370000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.INQUIRY.exe.2370000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.INQUIRY.exe.2640000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.INQUIRY.exe.2640000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
27.2.INQUIRY.exe.2640000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
27.2.INQUIRY.exe.2640000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.INQUIRY.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.1.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
17.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
37.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
6.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.INQUIRY.exe.25f0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.2.INQUIRY.exe.22f0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
28.2.INQUIRY.exe.22f0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.INQUIRY.exe.22f0000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.INQUIRY.exe.22f0000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
27.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
1.2.INQUIRY.exe.2300000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.INQUIRY.exe.2300000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.2.INQUIRY.exe.2490000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.INQUIRY.exe.2490000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.INQUIRY.exe.2210000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
28.2.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
28.2.INQUIRY.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.2.INQUIRY.exe.2660000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.2.INQUIRY.exe.2660000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.INQUIRY.exe.2380000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.INQUIRY.exe.2380000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
20.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
2.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
32.2.INQUIRY.exe.2630000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.2.INQUIRY.exe.7a0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
16.2.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.INQUIRY.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
32.2.INQUIRY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
27.2.INQUIRY.exe.25e0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.2.INQUIRY.exe.2240000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
28.2.INQUIRY.exe.2240000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.INQUIRY.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.INQUIRY.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.iigcest.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/://w	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.jiyu-kobo.co.jp/typo	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiv&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Treb	0%	Avira URL Cloud	safe	
http://www.carterandcone.comandh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp//	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com0p	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/cheV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/=	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.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	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comTCE	0%	Avira URL Cloud	safe	
http://www.carterandcone.comits	0%	Avira URL Cloud	safe	
http://www.carterandcone.comMic	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.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	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	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.comTC(	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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.fontbureau.comTTFF	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtig	0%	Avira URL Cloud	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://www.fontbureau.comnc.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://go.microsoft.	0%	Avira URL Cloud	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comn	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.carterandcone.comle	0%	Avira URL Cloud	safe	
http://www.fontbureau.comk	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm=	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	Avira URL Cloud	safe	
http://www.fontbureau.coms	0%	Avira URL Cloud	safe	
http://www.carterandcone.com$p	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.154.36	true	false		high
mail.iigcest.com	166.62.27.57	true	true	• 0%, Virustotal, Browse	unknown
121.205.6.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/://w	INQUIRY.exe, 00000001.00000003.661005611.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/typo	INQUIRY.exe, 00000001.00000003.661005611.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsiv&	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/Treb	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comandh	INQUIRY.exe, 00000001.00000003.660352640.0000000005011000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp//	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comepko	INQUIRY.exe, 00000001.00000003.670995336.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/s/	INQUIRY.exe, 00000001.00000003.660714589.0000000004FE4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessed	INQUIRY.exe, 00000001.00000003.664511180.0000000004FEF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	INQUIRY.exe, 00000001.00000003.659667033.0000000005016000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.661195055.0000000005011000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com0p	INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/cheV	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

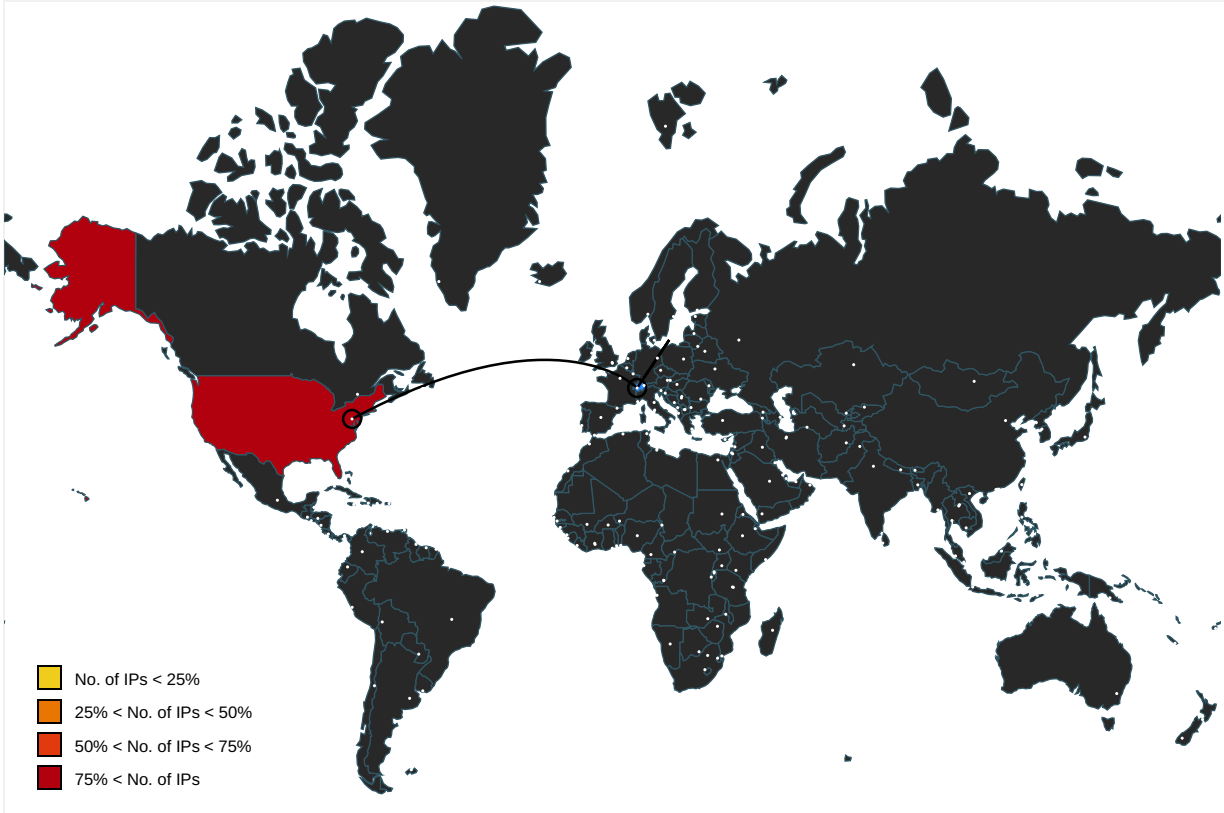
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designerslb	INQUIRY.exe, 00000001.00000003.664066811.0000000005016000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/=	INQUIRY.exe, 00000001.00000003.661005611.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTCE	INQUIRY.exe, 00000001.00000003.660146058.0000000004FEC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comits	INQUIRY.exe, 00000001.00000003.659772843.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comMic	INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersd	INQUIRY.exe, 00000001.00000003.662998950.0000000005011000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com/-	INQUIRY.exe, 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, INQUIRY.exe, 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, WerFault.exe, 00000009.00000002.731445229.0000000005040000.00000004.00000001.sdmp, INQUIRY.exe, 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, INQUIRY.exe, 00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrito	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	INQUIRY.exe, vbc.exe	false		high
http://www.fonts.com	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	INQUIRY.exe, 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	vbc.exe, 00000013.00000002.770041777.0000000000400000.00000040.00000001.sdmp, vbc.exe, 00000014.00000002.774520700.0000000000400000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC(	INQUIRY.exe, 00000001.00000003.660146058.0000000004FEC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.como.	INQUIRY.exe, 00000001.00000003.660146058.0000000004FEC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comTTFF	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	INQUIRY.exe, 00000001.00000003.664511180.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comtig	INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.com/	INQUIRY.exe, 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	INQUIRY.exe, 00000001.00000003.659052456.0000000005013000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.659667033.0000000005016000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	INQUIRY.exe, 00000001.00000003.666565645.0000000004FEF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comnc.	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://whatismyipaddress.com	INQUIRY.exe, 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlu	INQUIRY.exe, 00000001.00000003.664546236.0000000005011000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTC	INQUIRY.exe, 00000001.00000003.661005611.0000000004FEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://go.microsoft.	INQUIRY.exe, 00000010.00000002.825594692.0000000000852000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com	INQUIRY.exe, 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp	false		high
http://go.microsoft.LinkId=42127	INQUIRY.exe, 00000010.00000002.825594692.0000000000852000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	INQUIRY.exe, 00000001.00000003.656578776.0000000004FED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comn	INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.660006267.0000000004FF6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	INQUIRY.exe, 00000001.00000003.659772843.0000000005016000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comle	INQUIRY.exe, 00000001.00000003.660352640.0000000005011000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comk	INQUIRY.exe, 00000001.00000003.664511180.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm=	INQUIRY.exe, 00000001.00000003.670995336.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn	INQUIRY.exe, 00000001.00000003.659052456.0000000005013000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.657519748.0000000005012000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	INQUIRY.exe, 00000001.00000003.664630621.000000000501B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comlvfet	INQUIRY.exe, 00000001.00000003.670995336.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coms	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com$p	INQUIRY.exe, 00000001.00000003.659571445.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designershq	INQUIRY.exe, 00000001.00000003.663957016.0000000005016000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.661257796.0000000004FEB000.00000004.00000001.sdmp, INQUIRY.exe, 00000001.00000003.660714589.0000000004FE4000.00000004.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	INQUIRY.exe, 00000001.00000002.743094862.0000000005150000.00000002.00000001.sdmp, INQUIRY.exe, 00000010.00000002.830353978.0000000005270000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comalsd=	INQUIRY.exe, 00000001.00000003.665416380.0000000004FEF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.comic	INQUIRY.exe, 00000001.00000003.660146058.0000000004FEC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/_	INQUIRY.exe, 00000001.00000003.661599639.0000000004FEB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comsm	INQUIRY.exe, 00000001.00000003.660235609.0000000005016000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.154.36	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
166.62.27.57	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319686
Start date:	18.11.2020
Start time:	15:00:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INQUIRY.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.phis.troj.spyw.evad.winEXE@46/34@17/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 82% (good quality ratio 80.2%) • Quality average: 85.6% • Quality standard deviation: 23.6%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 51.104.144.132, 205.185.216.42, 205.185.216.10, 52.155.217.156, 20.54.26.129, 52.147.198.201, 92.122.213.247, 92.122.213.194, 51.104.139.180, 13.64.90.137 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.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 disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many 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
15:01:59	API Interceptor	70x Sleep call for process: INQUIRY.exe modified
15:02:07	API Interceptor	4x Sleep call for process: dw20.exe modified
15:02:22	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.154.36	c9o0CtTIYT.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	khJdbt0clZ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5Av43Q5lXd.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	8oaZfXDstn.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	pwYhlZGMa6.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	YrHUxpftPs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	cj9weNQmT2.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	lk5M5Q97c3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Enquiry_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	KM4ukzS8ER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	kYr85V73sJ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36
	5Av43Q5lXd.exe	Get hash	malicious	Browse	• 104.16.154.36
	8oaZfXDstn.exe	Get hash	malicious	Browse	• 104.16.154.36
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
	9vdouqRTh3.exe	Get hash	malicious	Browse	• 104.16.154.36
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• 104.16.155.36
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• 104.16.154.36
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• 104.16.154.36
	pwYhlZGMa6.exe	Get hash	malicious	Browse	• 104.16.154.36
mail.iigcest.com	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• 166.62.27.57
	x2rzwu7CQ3.exe	Get hash	malicious	Browse	• 166.62.27.57
	X62RG9z7kY.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT100892220-PDF.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT0079111-pdf.exe	Get hash	malicious	Browse	• 166.62.27.57
	AD1-2001328L_pdf.exe	Get hash	malicious	Browse	• 166.62.27.57

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	ShippingDoc.jar	Get hash	malicious	Browse	• 104.23.98.190
	JmuEmJ4T4r5bc8S.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Mal.Generic-S.5505.exe	Get hash	malicious	Browse	• 172.67.135.77
	Mailbox-Terms&Conditions.jar	Get hash	malicious	Browse	• 104.20.23.46
	ant.exe	Get hash	malicious	Browse	• 104.27.160.64
	List Of Orders.exe	Get hash	malicious	Browse	• 172.67.188.154
	Mailbox-Terms&Conditions.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://aaqkagzimdeymd.nicepage.io/CEREA-PARTNERS.html?version=25fbab78-b58c-47ae-9818-2632bfb7ce1f&uid=a3c290bf-b6ac-425a-b7f8-c2d16638c672	Get hash	malicious	Browse	• 104.16.19.94
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	a66a5257bb6ee2e690450c48a91815d4.exe	Get hash	malicious	Browse	• 104.23.99.190
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.133.233
	u82lb18JnW.exe	Get hash	malicious	Browse	• 104.31.92.240
	http://https://agrabadconventionhall.com/redirect-outlook.com/server%20configuration/?#info@herbertarchitekten.de	Get hash	malicious	Browse	• 104.16.18.94
	http://https://agrabadconventionhall.com/redirect-outlook.com/server configuration/	Get hash	malicious	Browse	• 104.16.19.94
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 172.67.214.161
	http://cricketventures.com	Get hash	malicious	Browse	• 104.26.13.251
	http://https://www.chm-endurance.com/	Get hash	malicious	Browse	• 104.22.24.131
	http://https://bitly.com/35yFnns	Get hash	malicious	Browse	• 104.16.19.94
	http://https://email.ofificeshareserver1.ml/e/c/eyJlbWFpbF9pZCI6IlJPS0xCZ01BQVhYVjZXVUFLRTFaMUpQWmZrTU1mUT09IiwiaHJlZiI6Imh0dHBzOi8vZmlyZWJhc2VzdG9yYWdlLmdvb2dsZWFwaXMuY29tL3YwL2Ivc2l0ZXMtMDAuYXBwc3BvdC5jb20vby9zaGFyZS1wb2ludCUyRnJlZGlyZWN0Lmh0bWw_YWx0PW1lZGlhXHUwMDI2dG9rZW49ZWM5NWIwZjItNTE4Ny00YzA3LWExNGUtMDA2OWE0ZWI0ODcxXHUwMDI2ZW1haWw9bWFya3VzLm5pZXRoQGp1bGl1c2JhZXIuY29tIiwibGlua19pZCI6MSwicG9zaXRpb24iOjB9/1b8972b4385f4f0bcb49ca81c6f33c388775dae940b9f44c90bdf57423203612	Get hash	malicious	Browse	• 104.31.71.251
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 104.27.187.65
AS-26496-GO-DADDY-COM-LLCUS	moses.exe	Get hash	malicious	Browse	• 148.66.138.196
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 184.168.131.241
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 184.168.131.241
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 107.180.26.71
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	anthony.exe	Get hash	malicious	Browse	• 107.180.4.22
	http://https://sailingfloridakeys.com/Guarantee/	Get hash	malicious	Browse	• 104.238.92.18
	oX3qPEgl5x.exe	Get hash	malicious	Browse	• 198.71.232.3
	http://https://rfpforsubmission.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 148.72.93.116
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 198.12.231.132
	4WD28ZoLXN.exe	Get hash	malicious	Browse	• 166.62.110.232
	AgvxMpx2Dv.exe	Get hash	malicious	Browse	• 132.148.26.76
	Untitled 20201030.doc	Get hash	malicious	Browse	• 198.71.233.96
	eLaaw7SqMi.exe	Get hash	malicious	Browse	• 68.178.213.243
	http://https://www.coalesceresearchgroup.com/coalesceinternational.com/acceount/	Get hash	malicious	Browse	• 148.72.22.210
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 107.180.2.103
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 184.168.131.241
	wHRBHjmaGw.exe	Get hash	malicious	Browse	• 132.148.26.76
CLOUDFLARENETUS	ShippingDoc.jar	Get hash	malicious	Browse	• 104.23.98.190
	JmuEmJ4T4r5bc8S.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Mal.Generic-S.5505.exe	Get hash	malicious	Browse	• 172.67.135.77
	Mailbox-Terms&Conditions.jar	Get hash	malicious	Browse	• 104.20.23.46
	ant.exe	Get hash	malicious	Browse	• 104.27.160.64

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	List Of Orders.exe	Get hash	malicious	Browse	• 172.67.188.154
	Mailbox-Terms&Conditions.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://aaqkagzimdeymd.nicepage.io/CEREA-PARTNERS.html?version=25fbab78-b58c-47ae-9818-2632bfb7ce1f&uid=a3c290bf-b6ac-425a-b7f8-c2d16638c672	Get hash	malicious	Browse	• 104.16.19.94
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	a66a5257bb6ee2e690450c48a91815d4.exe	Get hash	malicious	Browse	• 104.23.99.190
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.133.233
	u82lb18JnW.exe	Get hash	malicious	Browse	• 104.31.92.240
	http://https://agrabadconventionhall.com/redirect-outlook.com/server%20configuration/?#info@herbertarchitekten.de	Get hash	malicious	Browse	• 104.16.18.94
	http://https://agrabadconventionhall.com/redirect-outlook.com/server configuration/	Get hash	malicious	Browse	• 104.16.19.94
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 172.67.214.161
	http://cricketventures.com	Get hash	malicious	Browse	• 104.26.13.251
	http://https://www.chm-endurance.com/	Get hash	malicious	Browse	• 104.22.24.131
	http://https://bitly.com/35yFnns	Get hash	malicious	Browse	• 104.16.19.94
	http://https://email.ofificeshareserver1.ml/e/c/eyJlbWFpbF9pZCI6IlJPS0xCZ01BQVhYVjZXVUFLRTFaMUpQWmZrTU1mUT09IiwiaHJlZiI6Imh0dHBzOi8vZmlyZWJhc2VzdG9yYWdlLmdvb2dsZWFwaXMuY29tL3YwL2Ivc2l0ZXMtMDAuYXBwc3BvdC5jb20vby9zaGFyZS1wb2ludCUyRnJlZGlyZWN0Lmh0bWw_YWx0PW1lZGlhXHUwMDI2dG9rZW49NWIwZjItNTE4Ny00YzA3LWExNGUtMDA2OWE0ZWI0ODcxXHUwMDI2ZW1haWw9bWFya3VzLm5pZXRoQGp1bGl1c2JhZXIuY29tIiwibGlua19pZCI6MSwicG9zaXRpb24iOjB9/1b8972b4385f4f0bcb49ca81c6f33c388775dae940b9f44c90bdf57423203612	Get hash	malicious	Browse	• 104.31.71.251
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 104.27.187.65

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_0466ea22\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	19244
Entropy (8bit):	3.7689860404632216
Encrypted:	false
SSDEEP:	192:OYcm0I9+HzHqHBUZMXIjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xT5/u7sSS27P:X4HziBUZMXIjB7vqsSt/u7sSX4It5a8
MD5:	C8F2F641B01A44390EE72AB0291023BB
SHA1:	73DD3194D00A241D6506AC88E94A31C0872AAD9E
SHA-256:	253F7456400E5CD904BCCB71A341A89DDED83968C28A9ECDED505C38833040EE
SHA-512:	D10C15F5E4E81ACB4489DFD0CD212672A3396CF5CCCC38D76A5225B0E68B72EC05B22D9F2C08377CE5736CEAE4D545DB1C0DCF44A99D889EA64C797035DA4E5
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.1.8.1.7.6.8.7.2.5.3.6.8.1.....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.=.1.3.2.5.0.1.8.1.7.8.3.6.3.1.5.7.2.0.....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.=.8.7.4.7.1.9.9.a.-.f.e.7.9.-.4.4.6.d.-.a.c.8.3.-.2.3.0.d.3.d.4.9.4.3.4.4.....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.=.8.2.5.9.2.d.1.2.-.6.6.c.3.-.4.7.1.1.-.b.5.4.7.-.6.5.2.b.0.d.3.e.5.c.b.b.....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.=.I.N.Q.U.I.R.Y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.9.8.-.0.0.0.1.-.0.0.1.b.-.6.1.2.3.-.c.6.7.6.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	19246
Entropy (8bit):	3.7687586959631867
Encrypted:	false
SSDEEP:	192:cg/3+HVHqHBUZMXIjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sSS274ItF:B/uHViBUZMXIjB7vqsSt/u7sSX4It5a0
MD5:	0F2339E59B1382CFEBA7C65E0204DB37
SHA1:	869CD3F293F945FE0B794C50EF4899CCC318B52C
SHA-256:	EBD1A41084A86F927C8E65CD72B32DC6B9A5E16C62205A82F52EC9B364A79947
SHA-512:	1C8564A5E898644CBCF53664A1D39E26ADF5BE1DBA3DB233E2C325BA846520DACDFAC2DF7243F21C9AF1F78A9F2CCB035C1C2BCFB919FD0B1A8CEF54D657I 231
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.1.8.1.7.3.1.8.8.1.7.4.0.9.....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.=.1.3.2.5.0.1.8.1.7.4.1.3.3.4.8.3.4.7.....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.=.4.c.0.d.d.f.0.9.-.6.b.6.0.-.4.1.9.c.-.a.1.3.4.-.4.f.2.8.d.1.1.b.2.7.1.d.....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.=.a.e.f.0.8.8.e.c.-.c.a.5.c.-.4.4.9.4.-.8.6.f.d.-.f.b.f.f.c.f.f.8.d.b.5.3.....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.=.I.N.Q.U.I.R.Y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.0.8.-.0.0.0.1.-.0.0.1.b.-.8.5.b.b.-.c.f.5.b.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_inquiry.exe_e6c573bafb277a8e53b04fdad891cf6b8aba558_00000000_009f3881\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18450
Entropy (8bit):	3.7579185842846132
Encrypted:	false
SSDEEP:	192:EZ+HLTi+VJjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7srS274ItZ:HHLVjB7vqsSt/u7srX4ItZ
MD5:	FBCEA239031271D5FC498B4CCFF7FFC5
SHA1:	A317C75282FB18400F1DA04EE684D29A375F5919
SHA-256:	96D8D97D8A8C4F15EE1E0D1B75A78F8BEEBF3845EDD82E72E8D46F7F92F6B92E
SHA-512:	6DF096B4314D9F1E9E7672055DA379DE2270F970E3F5F2CE1026322C9CD0F52927DC652D3806CCCCA12662BD9121B0A8BC1528306CB63976184EF87AA99F226
Malicious:	false
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.=.1.3.2.5.0.1.8.1.8.0.2.7.7.2.1.3.1.1.....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.=.1.3.2.5.0.1.8.1.8.0.3.9.2.8.3.7.9.3.....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.c.1.4.c.0.8.c.-.3.3.4.9.-.4.a.e.4.-.8.5.a.7.-.e.5.4.9.3.b.5.0.4.7.9.b.....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.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.0.-.0.0.0.1.-.0.0.1.b.-.1.3.6.7.-.d.8.8.e.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.I.N.Q.U.I.R.Y...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.9.1.....I.s.F.a.t.a.l.=.4.2.9.4.9.6.7.2.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_inquiry.exe_e6c573bafb277a8e53b04fdad891cf6b8aba558_00000000_18bf7163\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18448
Entropy (8bit):	3.7581897365137853
Encrypted:	false
SSDEEP:	192:21+H0Ti+VJjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7srS274Itu:VH0VjB7vqsSt/u7srX4Itu
MD5:	5856CBF6D7376E0047754E49722CDE9A
SHA1:	051FCA316BE423B3D5475C843573239C084BB0AE
SHA-256:	AC6415AD3FD401C7E0B4547121023266CF2ABBC2F75A35FCCB2763DB2B36AEF3
SHA-512:	560A4FF5B36ED1ABA6F86856AE12A665208CED8A67893FC36246CC049C7B0DD9872AB2DC26E552D40E24A384B3441555442CE3505138F61EC24DDFE832C1A25
Malicious:	false
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.=.1.3.2.5.0.1.8.1.8.1.5.4.4.3.9.6.7.2.....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.=.1.3.2.5.0.1.8.1.8.1.8.5.0.6.4.5.5.1.....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.=.0.e.3.8.0.2.4.7.-.2.d.d.b.-.4.4.5.7.-.9.b.1.5.-.f.1.3.e.e.5.6.2.1.6.6.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.5.4.-.0.0.0.1.-.0.0.1.b.-.f.b.5.c.-.2.0.9.8.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.I.N.Q.U.I.R.Y...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.9.6.....I.s.F.a.t.a.l.=.4.2.9.4.9.6.7.2.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_inquiry.exe_e6c573bafb277a8e53b04fdad891cf6b8aba558_00000000_1a860a22\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_inquiry.exe_e6c573bafb277a8e53b04fdad891cf6b8aba558_00000000_1a860a22\Report.wer	
Category:	dropped
Size (bytes):	18450
Entropy (8bit):	3.7573567572608084
Encrypted:	false
SSDEEP:	192:2Mlg+HPTi+VJjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xT5/u7stS274Itw:bNHPVjB7vqsSt/u7stX4Itw
MD5:	BEA478764A49288FAE5D2C58DEA9E7F7
SHA1:	8601AF0DC1CFDBA1A6FD96882B78E44800F059AF
SHA-256:	D55EC04B23C4335716973DD1BE81A2285765931885 97B2FF2422E7CA596DAC57
SHA-512:	15AA099538B4D44703D965C393892452B5D204568CFE062308F35741F8C10FC87738AFF0CE2AEE3B2D9C3E2770C774C4216A053554CF554073FD0335AC46035B
Malicious:	false
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.=.1.3.2.5.0.1.8.1.7.2.0.5.3.8.0.2.5.0.....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.=.1.3.2.5.0.1.8.1.7.2.2.1.3.1.7.7.8.2.....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.=.7.7.e.5.1.0.d.1.-.c.c.b.4.-.4.5.8.4.-.8.e.d.d.-.e.d.1.2.8.8.9.c.0.1.1.3.....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.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.0.8.-.0.0.0.1.-.0.0.1.b.-.8.5.b.b.-.c.f.5.b.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.I.N.Q.U.I.R.Y...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.6.2.....I.s.F.a.t.a.l.=.4.2.9.4.9.6.7.2.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_inquiry.exe_e6c573bafb277a8e53b04fdad891cf6b8aba558_00000000_1b4a9849\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18450
Entropy (8bit):	3.7581638227883536
Encrypted:	false
SSDEEP:	192:B8y+H0Ti+VJjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xT5/u7sSS274Itj:kH0VjB7vqsSt/u7sSX4Itj
MD5:	4E9027E389CF59A8E643336BC538513A
SHA1:	5FC1F51DA07FA44C69EF4DC8C46AF896176E76F0
SHA-256:	5E35F7BEAF0E442F1923D24380FE8A32309325B08F6C6815AC221527631AEBEF
SHA-512:	77A94A00184189C927B7EF97D7308D0E5B629B080DF48CA7DB95BF8C0210E2E37F06377AD55CE8187E4E60F07AB2099AAC49A6B52D76EC1BFF39BC666F852C7
Malicious:	false
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.=.1.3.2.5.0.1.8.1.7.6.0.0.6.9.1.4.6.1.....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.=.1.3.2.5.0.1.8.1.7.6.3.0.2.2.2.6.3.2.....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.=.c.5.9.7.0.9.0.f.-.0.7.a.4.-.4.7.5.1.-.b.9.c.9.-.7.e.3.7.7.2.5.9.1.0.a.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.9.8.-.0.0.0.1.-.0.0.1.b.-.6.1.2.3.-.c.6.7.6.b.3.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.9.9.0.e.1.8.8.e.c.d.5.a.7.e.8.7.1.b.9.7.a.6.a.4.c.b.7.b.b.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.3.a.e.0.b.5.7.6.f.7.b.3.6.2.b.9.0.a.2.5.a.c.e.1.4.7.0.d.3.3.0.6.8.d.b.4.4.9.0.!.I.N.Q.U.I.R.Y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.I.N.Q.U.I.R.Y...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.7.8.....I.s.F.a.t.a.l.=.4.2.9.4.9.6.7.2.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 18 14:02:15 2020, 0x60521 type
Category:	dropped
Size (bytes):	7008087
Entropy (8bit):	4.7220376102848896
Encrypted:	false
SSDEEP:	98304:dYMlAY0P5P9Hch291r+VT8b1XanA8ngFYT3bRnCSljd5XSoU+zR8MX:djAYaP9HNgGwFJ/5Xv
MD5:	B959EB0600252402A18BFCF647E10552
SHA1:	0626EAF638F4FEF2920A77E3BC56740E52E126C5
SHA-256:	92E8F1B478C7EB956AD40A33A3739229D6C1ACB0793A32A327CF426C6CCE2A77
SHA-512:	A61C0109EBA44B3ECECA58A5D3DE320553FEE491B820638D50B266122604F6BD3B75660C745BA011C717FEA2E24C15C4AAFC5D49CCF254478E99D55B5A5EF0C
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp, Author: JPCERT/CC Incident Response Group
Preview:	MDMP..... .....g)._!.....U.....B.....8.....GenuineIntelW.....T.....M)._.....0..2.....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\WER2E55.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	3.7043697131252022
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNii06Yb6YPI6Egmf0uuS8+prk89bb9sfnpm:RrlsNiJ6s6Yw6EgmfPuSRb2fE
MD5:	878E1942EA193A0986BDC8426E80F69E
SHA1:	D47C31FC7B12BA957F6D61AB8E0C5FFDCE2585D6
SHA-256:	B31B2972C250517AF12D08CD15DE379C47B1FAA215DF97926D7227400370543A
SHA-512:	BEBD8D8ECEBD5466E4CBC6303EBEC7879A8D6C02057DADCCA7B56E117F426849E56E3E9BBF21F477C3D2EA83ECC2D55D427F756E57942950AA5826416B2B626
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.>.5.8.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3043.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5640
Entropy (8bit):	3.724414552767444
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3i+s6ROcYZtuvUubSfaQgsB+aM1911fH/m:Rrl7r3GLNi+s6ROcYZtuvUubS7+p191g
MD5:	3ACCC42FCA2CB02425C8B5FEB60C324D
SHA1:	2EF2A521BF4C9A6F3FA58C56A803D919B985BBE7
SHA-256:	2ECDDEC9C38A915BD80665FAFBE7779795C1342454EA3C57D8D682FA52A2089E
SHA-512:	B0813E81B0FA83DEF1700D5B4199F8CA0A8148B07319D158FE513094230C2A355E977F31BE21656C0A92D8B6B46B38C523E21582FEC509DEDA162DACEF37ADD
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.>.2.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4587
Entropy (8bit):	4.510625392276364
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI9OK6oWSC8BP8fm8M4JOWjZF5+q89zCpJP6v4HTd:uITfI4aSNKJOgtsCvP6vMTd
MD5:	A8469566DD777304B6389CE1094F7028
SHA1:	E5C9D56772A35FD2D8DCA937B993B3F4C092F9B9
SHA-256:	507E6016E8640ECE9E662D46F13B0C0322C64175A78028E65A471791CF7EB03D
SHA-512:	8B6460D77CE2B91024D10532ABD27E990F723E906AABC28F2EC02F85301A9A37953DE7BACEBFA1AD1D85FB11F2ECDD7A443C03F3598C42EBD7A9A48A5FF51F43
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="734352" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER310F.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4609
Entropy (8bit):	4.454622515385555
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9OK6oWSC8Bw08fm8M4JFKg7FT9P+q8v5bpJP6v4H+d:uITfS4aSNYJFKMKVvP6vM+d

C:\ProgramData\Microsoft\Windows\WER\Temp\WER310F.tmp.xml	
MD5:	E90B24327D824129769567901CF443FD
SHA1:	136452E7C618931A5D39470F24C97B3CE9FB8858
SHA-256:	27C78A3143AFDA038D4939AED93E3CB8B249CC9032C6568D01BAC4B57B298BAE
SHA-512:	BE3CA69E21A0B60EDA1C09659DF6968ADA039FC12791ED077D5E1026E587C40DED3E4FD91A75BAEEE238633622C31D183F440CC241D58E08FF789477FB4098
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="734354" />.. <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\WER6231.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5644
Entropy (8bit):	3.725672845251971
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3i4W6hn/OY6TYZtuvUubSfaQgsB+aM1jM1fohm:Rrl7r3GLNi4W6h/OlTYZtuvUubS7+p1k
MD5:	0EF540DE4DBDF43FBCFEE50AB55FA136
SHA1:	7ECED9AE0FCF5AAC17BF09D4114C09D2285FC38E
SHA-256:	8DAEF505D2FE71360A1544D35C3E1ACBE7AE5A4EFF9617AC844B591E55E9DCB1
SHA-512:	9C771D8C01F602E3732F32990596ED9C8E833AF86C91F507D402CF14B1E5DEBEE53BA9CED202C1BB40F667B4DDB904AB419A4387464F30E5F72D93F60D639D4
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.>.1.3.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6389.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4609
Entropy (8bit):	4.456846137432615
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9OK6oWSC8B48fm8M4JFKg7F98+q8v5epJP6v4Hdd:ulTfS4aSN3JFKDKovP6vMdd
MD5:	2ABC6F088DE2C790C718E4B5C042A11F
SHA1:	663A6B84DE9F3B0284CB8F8F56F68836D59199BA
SHA-256:	B78C0C1912AF53D5A3855576A4F1759E27E916D0CDDEA8F9ECD6B179302BB31D
SHA-512:	2145C163BEF734A90F38DB9ABF56E6EDA5BB1E3CE77AC22F5ABE411C4E98191C4DC8B68588BEE18AA157139F546DECF73A2322C7C2326BFDF2870B94A3638C26
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="734354" />.. <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\WER7CAE.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 18 14:03:43 2020, 0x60521 type
Category:	dropped
Size (bytes):	7022802
Entropy (8bit):	4.717144579527239
Encrypted:	false
SSDEEP:	98304:XYPlBtHP569HBpwU1r+VTnb1XaFA8nPtYT3bMriGfjTsXDaIoUL8Md:X6Btx69HAV4YQhfsXb
MD5:	FEAD06C9C1479F402088C5790CB54810
SHA1:	98E6C5DBB08872323131736E654FA53615B587B4
SHA-256:	E5C77118B53DF48454D8706ADB3AA5E603848B19056510A90343E9C8229EEBC6
SHA-512:	BC34879B56421682EF50B6B1EAA7D8CE9D3120567037B8213FC36ACCAB9218CE55125A98552CF3ED34CA2D1E7D98D8F107C0F286F2345EB138C9C351491C32A
Malicious:	**true**

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7CAE.tmp.mdmp	
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER7CAE.tmp.mdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER7CAE.tmp.mdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WER7CAE.tmp.mdmp, Author: JPCERT/CC Incident Response Group
Preview:	MDMP..... .....)._!.....U.....B.....8.....GenuineIntelW.....T.....T....)._.....0..2.....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\WER8867.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):	6324
Entropy (8bit):	3.732480537668084
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4Z6mY0uuS8+prI89bkcsfrsm:RrlsNi+6mYPuSFkvf1
MD5:	443C182B00527E31B1E4AD64BFFA8241
SHA1:	F1D745B2744B4224FD43AE752DAA83B8E7FB10E8
SHA-256:	25D2AD246A4ACEB2DBF6DD75A5DD3B06CC824F525D990939B860A4E259E71E64
SHA-512:	36978C6151C7001BF4AF5C4D7AB4510EADD05EB048E435BD1C1A61809B4003CB2F6D5AE7F6C9074952C5C121C793F337EF2886D30FE662B18BA622FFE1E1E02
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.>.1.3.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8933.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4587
Entropy (8bit):	4.5076470925802195
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9OK6oWSC8Bn8fm8M4JOWjZFz+q89z8pJP6v4Hud:ulTfS4aSN+JOgns8vP6vMud
MD5:	52FC903ED30F5B61BA8F727424907241
SHA1:	40816AF32399226225A46FA9841CC819A894B75A
SHA-256:	CD4FF732AB018C9AAC4D92F681006C0FB246283D3ADC6A040F8CA7B31F48FF38
SHA-512:	51706A5090F26418194DFC10146F7D906A7E4E203FFDBE7BFB1FDE179C53FAE6B32AE0134F083A50E07B78FA3B020A968C9CA773CCA4A45A8FEB8AEC48BAAC8B
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="734354" />.. <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\WER89A3.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5644
Entropy (8bit):	3.727574879681056
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3iGQA6pOPYZtuvUubSfaQgsB+aM1YC1fYAUom:Rrl7r3GLNiG/6pAYZtuvUubS7+p1YC1S
MD5:	B3060F69B30CC0B7BE8A0EEBBC0F66AE
SHA1:	14ED5EC297764359163C1F4AF27BA5D9CD96F73B
SHA-256:	E42AE8026F9C077C31416C917B6B9EBE48907C17E9D392B0B900FA94CB1F7121
SHA-512:	514FE1126AF8F28F5A2E99DD6D8B441CC185879EF3FC73AEE025356DDCA920109D43E26E994BC43E62AB9A15A0181FFDCA346ACE6F14CC4ED7A1B5B915B252D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A3.tmp.WERInternalMetadata.xml	
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.>.6.8.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B0B.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4609
Entropy (8bit):	4.456792166327963
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9OK6oWSC8BN8fm8M4JFKg7Fi+q8v5mpJP6v4HcHOd:uITfT4aSNwJFK7K0vP6vMiOd
MD5:	18F66061D1D492E5837EDA572C603EF7
SHA1:	09D9099E03FF5F8A1A481E9C16C706253EF312C8
SHA-256:	40F6DA190C8F79EA3E49E49A4FF2165C43FDFA39C281EE54BEC83B22ABAD4810
SHA-512:	2D7BF15CE4CD127233CDF94E19D653B90D9E3CE4AA6DE49D145DC879CF3F7B4559D16F1D2B3118FAD5B7CE89279EB44B69F85F037D125FEB27E82BAAA80C397
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="734353" />.. <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\WERAB44.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 18 14:02:53 2020, 0x60521 type
Category:	dropped
Size (bytes):	7023137
Entropy (8bit):	4.716145709461237
Encrypted:	false
SSDEEP:	98304:XYElKgNP5N9H5ZFx1r+VTJb1XacA8nLqYT3bXUyYjgtXSiqjoUt8MS:XbKgjN9HVsvVrttXS+
MD5:	727EDE66BE753BF43CC3BB8AD0424846
SHA1:	6D36C62C3F02AC08483F5C46ECAE760987320DCF
SHA-256:	790BA9AF55C3D758F27EF0D7863D6CB9A56EAFA041302FF6E05DD97CF97AC35F
SHA-512:	E96B87EEFC7CD22C841C78A61B34466AD208935E6ACAA741204F87FBBFCADA9B9EF12B6E3C4E9379491B5A6BEED83DA044D60F1774519197CFF5A5063603565
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB44.tmp.mdmp, Author: JPCERT/CC Incident Response Group
Preview:	MDMP..... .....).._!.....U.....B.....8.....GenuineIntelW.....T.....z)._.....0..2.....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\WERC3AF.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):	6324
Entropy (8bit):	3.7341230330284576
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGR6OjGY0uuS8+prm89bkasfCCsm:RrlsNiY6DYPuS/k5fCo
MD5:	5D356EEFFF6F12474642A2400398FCD4
SHA1:	51D9FB907FDCABE46A83942DF50444C241FC8F63
SHA-256:	53E30E0481710B622CD95CFADFD2017035084D91E8EFDF6D2BF3EEDF642EF4F5
SHA-512:	B33ACA3565A56D25A75FB3D09CF4E818502C92DA36C13E3277076147DC05F9D9BEF1AAFFCD81E0A2F4831560579BAB3E2688DCB4EC723064BA3576CBEF39A1E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3AF.tmp.WERInternalMetadata.xml	
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.>.6.8.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6FC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4587
Entropy (8bit):	4.511253263073843
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9OK6oWSC8BF8fm8M4JOWjZFI+q89zApJP6v4HcHdd:uITfT4aSNkJOgEsAvP6vMidd
MD5:	4433E23608B8B2A3855C267846E81EA3
SHA1:	20A828E188264B443EC9BF44921A81DADFD4B472
SHA-256:	9632AC9115185AB53965AF43D06F0E22DC58CA6013D9DC82F82F636370757E73
SHA-512:	14C33EF3DA14C74ECEF7CDF5F79CA7C7F89415E714E06A2A5AC643B10BCE2714A44370694F8A69FC241D9547D50101F973E37CB27121CC454DD6865C33B7F75
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="734353" />.. <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\WEREF38.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7616
Entropy (8bit):	3.691270032301233
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiin6E6YPb6EgmfZtuvUubS7+p1ct1fAldUm:RrlsNia6E6Yj6EgmfSvvbSecvfer
MD5:	ACACA69C6A291286C08D46EDABFF5680
SHA1:	D7B1662B910D8FD7961E37DB9E444921E4639EA4
SHA-256:	8EEB4DDDCF0548A987BD4BF9FE0C06E0B2C14C390D2F0F99C49CD1C5C541F745
SHA-512:	A9EB6EE1080F61332325FA1A47A26C6351A3A070B88DDBBE280D70D3C6BE4BE18E3063E83954C8949A6236C251A3B2BD52CA3176A609F3F4C916890330EDEA0
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.>.5.8.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFF4.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4609
Entropy (8bit):	4.455540365553958
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI9OK6oWSC8Bv8fm8M4JFKg7Fflm+q8v5UpJP6v4Hwd:uITfI4aSNCJFKclKGvP6vMwd
MD5:	DF582E1905AE5003E6954E4AD881502D
SHA1:	CA58F2D441FEA0F0EDB1918239EA99A9E579DE90
SHA-256:	DA6CA008EF7A7B3630E4B663CB2A6E8CE38BCC4E32E7E416950FAB100EA1F2FB
SHA-512:	5BC1A1740FC49FB50052C08845A89BFC11D4B87A83AA0B5BFEFC4682A1F9C36F7F26548BF608BF22B78BE23A721C9620E4B2A1D917BF588FF7A2DBE285F716CF
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="734352" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:Pd:F
MD5:	EFFC299A1ADDB07E7089F9B269C31F2F
SHA1:	6AFB24DE207D2E6952BA43F0E5B20BCDF0596CE5
SHA-256:	50E9A8665B62C8D68BCCC77C7C92431A1AA26CCBD38ED4BBA8DD7422A3A4AB70
SHA-512:	BD27269F95DA0217EE0999E12CC2AFC05882C559D55C1660095BB38A7D96ECB5F8210A919B24069C3FCC17CCDAA13844A75948314C74AAAC63B082DF196EA8
Malicious:	false
Preview:	1364

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\INQUIRY.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.0989440037669045
Encrypted:	false
SSDEEP:	3:oNt+WfWsrmC:oNwvsr7
MD5:	4FA80C1B433C83F339F774D6347C74D8
SHA1:	B5F7CA62EFB43F9A32A112C991CE22C07A8908D2
SHA-256:	25E8C1425C844373EBE82F274167A8ADEA6581F5A4F3ABC6B5F4BD0E5AE80092
SHA-512:	514421997E148C08C2BEE3664F660BEAA500881D1683F2DC6680DA7B5038857A9416918711295644027689 70E4463883C17A3CB186B1CCB0DE82714633B7EECF
Malicious:	false
Preview:	C:\Users\user\Desktop\INQUIRY.exe

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.893502354967658
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	INQUIRY.exe
File size:	1009664
MD5:	0b940145d7d02e5b1b975c99dd5197a4
SHA1:	53ae0b576f7b362b90a25ace1470d33068db4490

General

SHA256:	bf487ff7cdbbd998b633b1858a939d8c808bcce65ab9937695475b39deea70a8
SHA512:	f6ea131ca86752edd8163c27ba045ff8ab4fe90a92f923565496e99d8b46ba5e99af14660bcca127a1ff06246ca262456508f6f9de2462e4cd10ba53d1428a92
SSDEEP:	12288:Hl1aMljBMKnw6WJoGPb5FUoRAVyImHlawG0h/XWl2l+klp8OdH+0YxEGIN1QpZrj:jJCKxWfPNFwyIUlawt/3mwe0dn1QT
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	60c8d86cece67c70

Static PE Info

General

Entrypoint:	0x479884
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5113dec31b8616dbad783836e7188783

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00479694h
call 00007F14C893661Dh
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
call 00007F14C89863DDh
mov ecx, dword ptr [00495BC8h]
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00479188h]
call 00007F14C89863DDh
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
call 00007F14C8986451h
call 00007F14C8934114h
lea eax, dword ptr [eax+00h]
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x97000	0x24c4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x57324	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0x7f70	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x9b000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x788cc	0x78a00	False	0.524172198834	data	6.51448811653	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x7a000	0x1bc5c	0x1be00	False	0.171568455717	data	2.71109267168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x96000	0xcb1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x97000	0x24c4	0x2600	False	0.352076480263	data	4.94171972073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x9a000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x9b000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0x7f70	0x8000	False	0.559631347656	data	6.62495186635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x57324	0x57400	False	0.922672479405	data	7.57976248647	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xa4900	0x134	data		
RT_CURSOR	0xa4a34	0x134	data		
RT_CURSOR	0xa4b68	0x134	data		
RT_CURSOR	0xa4c9c	0x134	data		
RT_CURSOR	0xa4dd0	0x134	data		
RT_CURSOR	0xa4f04	0x134	data		
RT_CURSOR	0xa5038	0x134	data		
RT_BITMAP	0xa516c	0x1d0	data		
RT_BITMAP	0xa533c	0x1e4	data		
RT_BITMAP	0xa5520	0x1d0	data		
RT_BITMAP	0xa56f0	0x1d0	data		
RT_BITMAP	0xa58c0	0x1d0	data		
RT_BITMAP	0xa5a90	0x1d0	data		
RT_BITMAP	0xa5c60	0x1d0	data		
RT_BITMAP	0xa5e30	0x1d0	data		
RT_BITMAP	0xa6000	0x539f1	data	English	United States
RT_BITMAP	0xf99f4	0x1d0	data		
RT_BITMAP	0xf9bc4	0xd8	data		
RT_BITMAP	0xf9c9c	0xd8	data		
RT_BITMAP	0xf9d74	0xd8	data		
RT_BITMAP	0xf9e4c	0xd8	data		
RT_BITMAP	0xf9f24	0xd8	data		
RT_BITMAP	0xf9ffc	0xe8	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xfa0e4	0x668	data	English	United States
RT_DIALOG	0xfa74c	0x52	data		
RT_RCDATA	0xfa7a0	0x10	data		
RT_RCDATA	0xfa7b0	0x274	data		
RT_RCDATA	0xfaa24	0x7c3	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xfb1e8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb1fc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb210	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb224	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb238	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb24c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb260	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfb274	0x14	data	English	United States
RT_HTML	0xfb288	0x99	data	English	United States

Imports

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

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/18/20-15:02:26.704911	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49750	587	192.168.2.4	166.62.27.57
11/18/20-15:03:08.289546	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49774	587	192.168.2.4	166.62.27.57

Network Port Distribution

Total Packets: 107

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 15:01:59.031246901 CET	49743	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.047661066 CET	80	49743	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.047848940 CET	49743	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.048484087 CET	49743	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.064749956 CET	80	49743	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.071091890 CET	80	49743	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.108748913 CET	49744	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.117561102 CET	49743	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.125319004 CET	443	49744	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.126780987 CET	49744	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.169167995 CET	49744	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.185825109 CET	443	49744	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.185980082 CET	443	49744	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.186119080 CET	443	49744	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.186583042 CET	49744	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.197808981 CET	49744	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.199700117 CET	49745	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.214375019 CET	443	49744	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.216025114 CET	443	49745	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.216219902 CET	49745	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.216970921 CET	49745	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.233329058 CET	443	49745	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.235097885 CET	443	49745	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.235296011 CET	443	49745	104.16.154.36	192.168.2.4
Nov 18, 2020 15:01:59.235400915 CET	49745	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.236514091 CET	49745	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:01:59.252928972 CET	443	49745	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:23.817213058 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:24.098351955 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:24.098483086 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:24.647198915 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:24.822807074 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:24.825001001 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:25.106144905 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:25.106544971 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:25.388585091 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:25.388873100 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:25.710129023 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:25.858115911 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:25.858395100 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.139451027 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.139874935 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.422636032 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.422939062 CET	49750	587	192.168.2.4	166.62.27.57

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 15:02:26.703771114 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.703959942 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.704910994 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.704945087 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.705151081 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.705218077 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.705363989 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.705427885 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:26.986233950 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.986258984 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:26.999335051 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:27.002060890 CET	587	49750	166.62.27.57	192.168.2.4
Nov 18, 2020 15:02:27.057396889 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:33.383512020 CET	49743	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:33.383887053 CET	49750	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:02:38.505419016 CET	49759	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.521910906 CET	80	49759	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.522161961 CET	49759	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.523021936 CET	49759	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.539441109 CET	80	49759	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.549550056 CET	80	49759	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.597470045 CET	49761	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.613935947 CET	443	49761	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.614130020 CET	49761	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.673311949 CET	49761	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.689773083 CET	443	49761	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.690314054 CET	443	49761	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.690376043 CET	443	49761	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.690885067 CET	49761	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.693752050 CET	49761	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.695373058 CET	49763	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.710299015 CET	443	49761	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.711641073 CET	443	49763	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.711795092 CET	49763	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.712759972 CET	49763	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.714680910 CET	49759	80	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.729115963 CET	443	49763	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.729497910 CET	443	49763	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.729578018 CET	443	49763	104.16.154.36	192.168.2.4
Nov 18, 2020 15:02:38.729635954 CET	49763	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.731683016 CET	49763	443	192.168.2.4	104.16.154.36
Nov 18, 2020 15:02:38.747950077 CET	443	49763	104.16.154.36	192.168.2.4
Nov 18, 2020 15:03:05.906356096 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:06.168962955 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:06.169061899 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:06.695435047 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:06.695717096 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:06.958623886 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:06.959141970 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:07.222193003 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:07.223017931 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:07.495678902 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:07.495965004 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:07.758713007 CET	587	49774	166.62.27.57	192.168.2.4
Nov 18, 2020 15:03:07.758955002 CET	49774	587	192.168.2.4	166.62.27.57
Nov 18, 2020 15:03:08.022917032 CET	587	49774	166.62.27.57	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 15:01:43.623750925 CET	64549	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:43.650897980 CET	53	64549	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:45.449043989 CET	63153	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:45.475955009 CET	53	63153	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 15:01:46.248142004 CET	52991	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:46.275309086 CET	53	52991	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:47.094983101 CET	53700	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:47.122129917 CET	53	53700	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:47.915492058 CET	51726	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:47.943371058 CET	53	51726	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:48.590341091 CET	56794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:48.617573977 CET	53	56794	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:49.659903049 CET	56534	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:49.687086105 CET	53	56534	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:50.457806110 CET	56627	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:50.495663881 CET	53	56627	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:54.680612087 CET	56621	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:54.707959890 CET	53	56621	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:55.514782906 CET	63116	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:55.541924000 CET	53	63116	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:56.319547892 CET	64078	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:56.346719980 CET	53	64078	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:57.273447990 CET	64801	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:57.300653934 CET	53	64801	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:58.292248964 CET	61721	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:58.319410086 CET	53	61721	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:58.704564095 CET	51255	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:58.741070986 CET	53	51255	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:58.971637011 CET	61522	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:59.006939888 CET	53	61522	8.8.8.8	192.168.2.4
Nov 18, 2020 15:01:59.079847097 CET	52337	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:01:59.106956959 CET	53	52337	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:02.765192986 CET	55046	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:02.792345047 CET	53	55046	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:11.437201977 CET	49612	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:11.464301109 CET	53	49612	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:22.060935974 CET	49285	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:22.088042021 CET	53	49285	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:23.770134926 CET	50601	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:23.815956116 CET	53	50601	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:32.777748108 CET	60875	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:32.804969072 CET	53	60875	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:35.306493044 CET	56448	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:35.342278957 CET	53	56448	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:35.996299028 CET	59172	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:36.031609058 CET	53	59172	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:36.529362917 CET	62420	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:36.565490007 CET	53	62420	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:36.900733948 CET	60579	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:36.960184097 CET	53	60579	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:37.449456930 CET	50183	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:37.485517025 CET	53	50183	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:37.910711050 CET	61531	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:37.937813044 CET	53	61531	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:38.128568888 CET	49228	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:38.164376020 CET	53	49228	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:38.443804026 CET	59794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:38.471159935 CET	53	59794	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:38.472012043 CET	55916	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:38.507505894 CET	53	55916	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:38.556760073 CET	52752	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:38.592199087 CET	53	52752	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:38.655498981 CET	60542	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:38.690794945 CET	53	60542	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:39.171142101 CET	60689	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:39.207019091 CET	53	60689	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:39.929310083 CET	64206	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:39.956566095 CET	53	64206	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 15:02:41.034682989 CET	50904	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:41.072463989 CET	53	50904	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:43.444211006 CET	57525	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:43.471467018 CET	53	57525	8.8.8.8	192.168.2.4
Nov 18, 2020 15:02:55.619406939 CET	53814	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:02:55.656312943 CET	53	53814	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:04.388042927 CET	53418	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:04.415371895 CET	53	53418	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:05.854183912 CET	62833	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:05.904856920 CET	53	62833	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:20.956906080 CET	59260	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:20.992511988 CET	53	59260	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:21.287211895 CET	49944	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:21.314351082 CET	53	49944	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:21.386476994 CET	63300	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:21.424304962 CET	53	63300	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:24.213391066 CET	61449	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:24.240730047 CET	53	61449	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:24.378654003 CET	51275	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:24.414350033 CET	53	51275	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:26.271187067 CET	63492	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:26.298304081 CET	53	63492	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:33.447617054 CET	58945	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:33.483230114 CET	53	58945	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:33.766551018 CET	60779	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:33.802285910 CET	53	60779	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:33.881725073 CET	64014	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:33.917220116 CET	53	64014	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:38.988058090 CET	57091	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:39.015259027 CET	53	57091	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:46.905772924 CET	55904	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:46.933022976 CET	53	55904	8.8.8.8	192.168.2.4
Nov 18, 2020 15:03:56.111162901 CET	52109	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:03:56.138288021 CET	53	52109	8.8.8.8	192.168.2.4
Nov 18, 2020 15:04:00.602796078 CET	54450	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:04:00.638335943 CET	53	54450	8.8.8.8	192.168.2.4
Nov 18, 2020 15:04:00.673490047 CET	49374	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:04:00.700529099 CET	53	49374	8.8.8.8	192.168.2.4
Nov 18, 2020 15:04:00.756617069 CET	50436	53	192.168.2.4	8.8.8.8
Nov 18, 2020 15:04:00.791821003 CET	53	50436	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 15:01:58.704564095 CET	192.168.2.4	8.8.8.8	0x7fd8	Standard query (0)	121.205.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:01:58.971637011 CET	192.168.2.4	8.8.8.8	0x27c4	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:01:59.079847097 CET	192.168.2.4	8.8.8.8	0x7cb6	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:23.770134926 CET	192.168.2.4	8.8.8.8	0xb5a3	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.128568888 CET	192.168.2.4	8.8.8.8	0x8bd0	Standard query (0)	121.205.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:02:38.443804026 CET	192.168.2.4	8.8.8.8	0x9673	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.556760073 CET	192.168.2.4	8.8.8.8	0x19c	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:05.854183912 CET	192.168.2.4	8.8.8.8	0x697a	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:20.956906080 CET	192.168.2.4	8.8.8.8	0xa2aa	Standard query (0)	121.205.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:03:21.287211895 CET	192.168.2.4	8.8.8.8	0x557a	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:21.386476994 CET	192.168.2.4	8.8.8.8	0x5ae3	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 15:03:33.447617054 CET	192.168.2.4	8.8.8.8	0x53b6	Standard query (0)	121.205.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:03:33.766551018 CET	192.168.2.4	8.8.8.8	0x5dfb	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:33.881725073 CET	192.168.2.4	8.8.8.8	0x5d23	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.602796078 CET	192.168.2.4	8.8.8.8	0x70c7	Standard query (0)	121.205.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:04:00.673490047 CET	192.168.2.4	8.8.8.8	0x279f	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.756617069 CET	192.168.2.4	8.8.8.8	0x506	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 15:01:58.741070986 CET	8.8.8.8	192.168.2.4	0x7fd8	Name error (3)	121.205.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:01:59.006939888 CET	8.8.8.8	192.168.2.4	0x27c4	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:01:59.006939888 CET	8.8.8.8	192.168.2.4	0x27c4	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:01:59.106956959 CET	8.8.8.8	192.168.2.4	0x7cb6	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:01:59.106956959 CET	8.8.8.8	192.168.2.4	0x7cb6	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:23.815956116 CET	8.8.8.8	192.168.2.4	0xb5a3	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.164376020 CET	8.8.8.8	192.168.2.4	0x8bd0	Name error (3)	121.205.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:02:38.471159935 CET	8.8.8.8	192.168.2.4	0x9673	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.471159935 CET	8.8.8.8	192.168.2.4	0x9673	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.592199087 CET	8.8.8.8	192.168.2.4	0x19c	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:02:38.592199087 CET	8.8.8.8	192.168.2.4	0x19c	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:05.904856920 CET	8.8.8.8	192.168.2.4	0x697a	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:20.992511988 CET	8.8.8.8	192.168.2.4	0xa2aa	Name error (3)	121.205.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:03:21.314351082 CET	8.8.8.8	192.168.2.4	0x557a	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:21.314351082 CET	8.8.8.8	192.168.2.4	0x557a	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:21.424304962 CET	8.8.8.8	192.168.2.4	0x5ae3	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:21.424304962 CET	8.8.8.8	192.168.2.4	0x5ae3	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:33.483230114 CET	8.8.8.8	192.168.2.4	0x53b6	Name error (3)	121.205.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:03:33.802285910 CET	8.8.8.8	192.168.2.4	0x5dfb	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:33.802285910 CET	8.8.8.8	192.168.2.4	0x5dfb	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 15:03:33.917220116 CET	8.8.8.8	192.168.2.4	0x5d23	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:03:33.917220116 CET	8.8.8.8	192.168.2.4	0x5d23	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.638335943 CET	8.8.8.8	192.168.2.4	0x70c7	Name error (3)	121.205.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 15:04:00.700529099 CET	8.8.8.8	192.168.2.4	0x279f	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.700529099 CET	8.8.8.8	192.168.2.4	0x279f	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.791821003 CET	8.8.8.8	192.168.2.4	0x506	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 15:04:00.791821003 CET	8.8.8.8	192.168.2.4	0x506	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49743	104.16.154.36	80	C:\Users\user\Desktop\INQUIRY.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 15:01:59.048484087 CET	348	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 15:01:59.071091890 CET	349	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 14:01:59 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 15:01:59 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067d42940f0000c2810dbe2000000001 Server: cloudflare CF-RAY: 5f423a0018cdc281-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49759	104.16.154.36	80	C:\Users\user\Desktop\INQUIRY.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 15:02:38.523021936 CET	844	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 15:02:38.549550056 CET	844	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 14:02:38 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 15:02:38 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067d432e42000063776eb34000000001 Server: cloudflare CF-RAY: 5f423af6cb926377-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49776	104.16.154.36	80	C:\Users\user\Desktop\INQUIRY.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 15:03:21.354469061 CET	5549	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 15:03:21.376317978 CET	5550	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 14:03:21 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 15:03:21 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067d43d59000002c2ed824b000000001 Server: cloudflare CF-RAY: 5f423c0288692c2e-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49783	104.16.155.36	80	C:\Users\user\Desktop\INQUIRY.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 15:03:33.843103886 CET	5584	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 15:03:33.867271900 CET	5584	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 14:03:33 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 15:03:33 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067d44065900002b95012f5000000001 Server: cloudflare CF-RAY: 5f423c508af42b95-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49790	104.16.155.36	80	C:\Users\user\Desktop\INQUIRY.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 15:04:00.721941948 CET	5624	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 15:04:00.753989935 CET	5624	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 14:04:00 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 15:04:00 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067d446f5c0000d6bda83ec000000001 Server: cloudflare CF-RAY: 5f423cf88d18d6bd-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

SMTP Packets

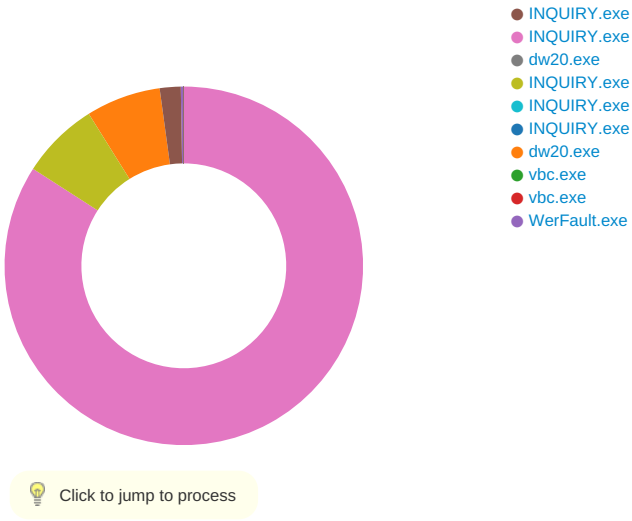
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 18, 2020 15:02:24.647198915 CET	587	49750	166.62.27.57	192.168.2.4	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Wed, 18 Nov 2020 07:02:24 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 18, 2020 15:02:24.825001001 CET	49750	587	192.168.2.4	166.62.27.57	EHLO 445817

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 18, 2020 15:02:25.106144905 CET	587	49750	166.62.27.57	192.168.2.4	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 445817 [84.17.52.40] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 18, 2020 15:02:25.106544971 CET	49750	587	192.168.2.4	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 18, 2020 15:02:25.388585091 CET	587	49750	166.62.27.57	192.168.2.4	334 UGFzc3dvcmQ6
Nov 18, 2020 15:02:25.858115911 CET	587	49750	166.62.27.57	192.168.2.4	235 Authentication succeeded
Nov 18, 2020 15:02:25.858395100 CET	49750	587	192.168.2.4	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 18, 2020 15:02:26.139451027 CET	587	49750	166.62.27.57	192.168.2.4	250 OK
Nov 18, 2020 15:02:26.139874935 CET	49750	587	192.168.2.4	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 18, 2020 15:02:26.422636032 CET	587	49750	166.62.27.57	192.168.2.4	250 Accepted
Nov 18, 2020 15:02:26.422939062 CET	49750	587	192.168.2.4	166.62.27.57	DATA
Nov 18, 2020 15:02:26.703959942 CET	587	49750	166.62.27.57	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 18, 2020 15:02:26.705427885 CET	49750	587	192.168.2.4	166.62.27.57	.
Nov 18, 2020 15:02:27.002060890 CET	587	49750	166.62.27.57	192.168.2.4	250 OK id=1kfO2U-008ZMO-Gu
Nov 18, 2020 15:03:06.695435047 CET	587	49774	166.62.27.57	192.168.2.4	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Wed, 18 Nov 2020 07:03:06 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 18, 2020 15:03:06.695717096 CET	49774	587	192.168.2.4	166.62.27.57	EHLO 445817
Nov 18, 2020 15:03:06.958623886 CET	587	49774	166.62.27.57	192.168.2.4	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 445817 [84.17.52.40] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 18, 2020 15:03:06.959141970 CET	49774	587	192.168.2.4	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 18, 2020 15:03:07.222193003 CET	587	49774	166.62.27.57	192.168.2.4	334 UGFzc3dvcmQ6
Nov 18, 2020 15:03:07.495678902 CET	587	49774	166.62.27.57	192.168.2.4	235 Authentication succeeded
Nov 18, 2020 15:03:07.495965004 CET	49774	587	192.168.2.4	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 18, 2020 15:03:07.758713007 CET	587	49774	166.62.27.57	192.168.2.4	250 OK
Nov 18, 2020 15:03:07.758955002 CET	49774	587	192.168.2.4	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 18, 2020 15:03:08.022917032 CET	587	49774	166.62.27.57	192.168.2.4	250 Accepted
Nov 18, 2020 15:03:08.025825977 CET	49774	587	192.168.2.4	166.62.27.57	DATA
Nov 18, 2020 15:03:08.288832903 CET	587	49774	166.62.27.57	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 18, 2020 15:03:08.290122032 CET	49774	587	192.168.2.4	166.62.27.57	.
Nov 18, 2020 15:03:08.570868969 CET	587	49774	166.62.27.57	192.168.2.4	250 OK id=1kfO3A-008aRf-3m

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: INQUIRY.exe PID: 2016 Parent PID: 5852

General

Start time:	15:01:48
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe'
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.656291540.0000000002642000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.656369760.00000000026D7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.656369760.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.656369760.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.656369760.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.656369760.00000000026D7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 5896 Parent PID: 2016

General

Start time:	15:01:49
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe'
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
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: 00000001.00000002.741822453.0000000003A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.741822453.0000000003A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.737101791.0000000002272000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.735055042.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.735055042.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.735055042.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.735055042.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.735055042.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.735183511.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.735183511.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.735183511.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.735183511.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.735183511.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.736771009.00000000021E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.736771009.00000000021E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.736771009.00000000021E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.736771009.00000000021E0000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.736771009.00000000021E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.739090343.0000000002A41000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.737371268.0000000002302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.737371268.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.737371268.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.737371268.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.737371268.0000000002302000.00000040.00000001.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	722760AC	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	722760AC	unknown
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	722760AC	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	722760AC	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	23ABCAB	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	23ABCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	2685E86	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	2685E86	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	35 38 39 36	5896	success or wait	1	2680093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	34	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 49 4e 51 55 49 52 59 2e 65 78 65	C:\Users\user\Desktop\INQUIRY.exe	success or wait	1	2680093	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2680093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2680093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	2680093	ReadFile
C:\Users\user\Desktop\INQUIRY.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\INQUIRY.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	2680093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	2680093	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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	2685326	RegSetValueExW

Analysis Process: INQUIRY.exe PID: 5788 Parent PID: 2016

General

Start time:	15:01:50
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe' 2 5896 5358953
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 6868 Parent PID: 5896

General

Start time:	15:01:59
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2308
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: vbc.exe PID: 6664 Parent PID: 5896

General

Start time:	15:02:02
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.692418330.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

Analysis Process: vbc.exe PID: 6700 Parent PID: 5896

General

Start time:	15:02:03
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.695692485.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	2	ff fe	..	success or wait	1	407BCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Analysis Process: WerFault.exe PID: 6776 Parent PID: 5896

General

Start time:	15:02:08
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5896 -s 2216

Imagebase:	0x990000
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: 00000009.00000002.731445229.0000000005040000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.731445229.0000000005040000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.731445229.0000000005040000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6CBC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	success or wait	1	6CBB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	success or wait	1	6CBB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp.xml	success or wait	1	6CBB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3134.tmp.csv	success or wait	1	6CBB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34C0.tmp.txt	success or wait	1	6CBB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 67 29 b5 5f 21 05 06 00 00 00 00 00	MDMP........ ....g)._!.......	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	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 88 38 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 08 17 00 00 4d 29 b5 5f 01 00 00 00 06 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 32 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.......8.... ..GenuineIntelW...........T... ....M)._.................. ....0..2...............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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	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 7f 02 00 00 00 01 00 00 ff ff 00 00 9f 29 20 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7c 92 11 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 c4 ed c7 07 a8 ca a9 02 1c ee c7 07 ff ff ff f9 00 00 00 00 a8 ca a9 02 d4 ed c7 07 73 78 4e 02 23 00 00 00 46 02 01 00 9c eb c7 07 2b 00 00 00 7f 02 00 01 00 00 00 00 9f 29 20 72 00 00 00 00 00 00 00 00 00 00 00 00 00 80 1f 00 00 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	....) r................ ....|..@.............+...S...+. ..+........................... ....sxN.#...F.......+............) r.......................................	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	168	a4 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 73 78 4e 02 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 66 5c 00 00	........................sxN... ....f\..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	20	00 03 00 00 00 00 d2 04 00 00 00 00 00 00 01 00 3a d2 00 00	................:...	success or wait	768	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	65536	00 00 00 00 00 00 00 00 3a c6 04 00 00 00 00 00 ff 9d 00 00 00 00 00 00 31 31 2f 31 38 20 31 34 3a 30 31 3a 35 31 2e 33 31 39 2c 32 38 38 34 2c 31 30 30 30 30 32 2c 43 61 63 68 65 43 74 78 2c 61 64 64 45 6c 65 6d 2c 66 61 63 65 0a 31 31 2f 31 38 20 31 34 3a 30 31 3a 35 31 2e 33 31 39 2c 31 35 34 30 2c 31 30 30 30 30 35 2c 41 6c 70 63 53 76 72 2c 73 74 61 74 65 2c 6d 69 73 73 0a 31 31 2f 31 38 20 31 34 3a 30 31 3a 35 31 2e 33 31 39 2c 31 35 34 30 2c 31 30 30 30 30 35 2c 41 6c 70 63 53 76 72 2c 73 74 61 74 65 2c 77 61 69 74 0a 31 31 2f 31 38 20 31 34 3a 30 31 3a 35 31 2e 33 31 39 2c 32 38 38 34 2c 31 30 30 30 30 32 2c 43 61 63 68 65 43 74 78 2c 61 64 64 45 6c 65 6d 2c 66 61 63 65 0a 31 31 2f 31 38 20 31 34 3a 30 31 3a 35 31 2e 33 31 39 2c 31 35 34 30 2c 31	........:...............11/18 14:01:51.319,2884,100002 ,Cache Ctx,addElem,face.11/18 14:01:5 1.319,1540,100005,AlpcSv r,state,miss.11/18 14:01:51.319,1540 ,100005,AlpcSvr,state,wait .11/18 14:01:51.319,2884,100002 ,Ca cheCtx,addElem,face.11/1 8 14:01:51.319,1540,1	success or wait	767	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	524288	cc 3b 26 72 b0 ad 5c 00 00 00 00 00 11 08 00 00 7f 00 00 00 00 00 00 00 40 d6 5c 00 00 00 00 26 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 00 00 00 c0 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 21 00 00 c0 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 10 00 00 c0 02 00 00 00 00 00 00 00 05 00 00 00 00 10 f5 70 00 10 bf 72 00 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 b5 57 39 70 a1 98 39 70 b9 57 39 70 a5 98 39 70 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 18 00 00 c0 00 00 00 00 d8 f8 47 70 d2 08 00 00 c0 00 00 00 2c 07 38 70 00 00 00 00 f4 c8 47 70 a6 02 00 00 3e 00 00	.;&r..\................@.\... .&........................... ....!..... ....p...r.......... ....W9p..9p .W9p..9p..................... ....Gp........,.8p ......Gp....>..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	36	50 5d e4 76 40 a4 e3 76 c0 b3 e3 76 a0 64 e4 76 60 a0 e3 76 00 a3 e3 76 90 b1 e3 76 30 56 e4 76 00 00 00 00	P].v@..v...v.d.v`..v...v...v0V .v....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	4	13 00 00 00	....	success or wait	19	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	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 7f 02 00 00 00 01 00 00 ff ff 00 00 48 9b 20 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff 3f 00 00 00 00 00 00 00 80 ff 3f 00 00 00 00 00 00 00 80 ff 3f 00 00 00 00 00 00 00 00 a0 02 40 00 00 00 00 00 00 00 80 fd 3f 00 00 00 00 00 80 80 fb 06 40 00 00 00 00 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 a0 44 eb 02 ec c7 a8 02 14 2b a4 02 00 00 00 00 00 00 00 00 00 00 00 00 70 ec 19 00 9c 2b 55 74 23 00 00 00 12 02 20 00 e0 eb 19 00 2b 00 00 00 7f 02 00 01 00 00 00 00 48 9b 20 72 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 1f 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	?............................ ....H. r................ ....?.... .....?.........?.........@.... .....?.........@....+...S...+. ..+....D.......+............. p....+Ut#..... .....+...........H. r......................................	success or wait	19	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	48	28 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 00 2d 00 00 00 00 00 a4 e7 8d 07 00 00 00 00 5c 18 00 00 e0 8b 4c 00 cc 02 00 00 8a 91 00 00	(....... ....-........... ..\.....L.........	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	4	5e 00 00 00	^...	success or wait	94	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	74	44 00 00 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 6a 00 6f 00 6e 00 65 00 73 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 5c 00 49 00 4e 00 51 00 55 00 49 00 52 00 59 00 2e 00 65 00 78 00 65 00 00 00	D...C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.D.e.s.k.t.o.p.\.I.N.Q.U.I.R.Y...e.x.e...	success or wait	94	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	64	3a 00 00 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 79 00 73 00 74 00 65 00 6d 00 33 00 32 00 5c 00 6e 00 74 00 64 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 00 00 00	:...C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.n.t.d.l.l...d.l.l...	success or wait	93	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	120	00 00 e4 6c 00 00 00 00 00 d0 03 00 98 9b 03 00 82 62 7f b9 96 5b 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 12 a2 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 04 00 00 00	...l.....b...[.....B.....B?.....$.....@A.....	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	30	18 00 00 00 52 00 69 00 63 00 68 00 45 00 64 00 32 00 30 00 2e 00 64 00 6c 00 6c 00 00 00	....R.i.c.h.E.d.2.0...d.l.l...	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	1516	00 00 05 6d 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 2a 5c 00 00 50 03 00 00 01 00 00 00 10 00 00 00 48 00 00 00 40 03 00 00 08 17 00 00 b0 02 00 00 00 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 24 00 00 00 78 00 00 00 40 01 00 00 b8 01 00 00 20 00 00 00 d8 01 00 00 24 01 00 00 00 03 00 00 38 00 00 00 38 03 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 01 05 00 00 00 00 00 05 15 00 00 00 cf 06 ad e5 49 85 b1 7e bc d2 94 f1 ea 03 00 00 00 00 00 00 0e 00 00 00 74 00 00 00 07 00 00 00 90 00 00 00 07 00 00 00 9c 00 00 00 07 00 00 00 a8 00 00 00 0f 00 00 00 b8 00 00 00 07 00 00 00 c8 00 00 00 07 00 00 00 d4 00 00 00 07 00 00 00 e0 00 00 00 07 00 00 00 ec 00 00 00 07 00 00 00 f8 00 00 00 07 00 00 00 04 01 00 00 07 00 00 c0 18 01 00	...m.....m.*\..P.....H...@.....H....P...$...x...@..... .....$.....8...8.....I..~..t.....	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B59.tmp.mdmp	unknown	120	03 00 00 00 94 03 00 00 fc 06 00 00 04 00 00 00 ac 27 00 00 9c 0a 00 00 0e 00 00 00 6c 00 00 00 48 32 00 00 13 00 00 00 50 03 00 00 b4 32 00 00 05 00 00 00 04 30 00 00 36 a2 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 15 00 00 00 ec 01 00 00 04 36 00 00 16 00 00 00 98 00 00 00 f0 37 00 00	.....'.....I. ..H2.....P....2.....0..6... .....T.....8.....T. .....6.....7..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.8.9.6.<./.P.i.d.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 49 00 4e 00 51 00 55 00 49 00 52 00 59 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.>.I.N.Q.U.I.R.Y...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 37 00 37 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.7.7.2.0.<./.U.p.t.i.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 35 00 30 00 39 00 33 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.5.0.9.3.7.3.4.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 34 00 32 00 36 00 33 00 34 00 37 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.4.2.6.3.4.7.5.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 35 00 39 00 39 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.>.2.5.9.9.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 34 00 39 00 39 00 32 00 32 00 30 00 34 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.>.4.9.9.2.2.0.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 34 00 39 00 39 00 32 00 32 00 30 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.9.9.2.2.0.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 34 00 30 00 33 00 36 00 31 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.>.4.0.3.6.1.6.<./.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 36 00 38 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.8.5.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 31 00 36 00 34 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.4.3.8.4.<./.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 31 00 36 00 31 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.1.9.1.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 33 00 37 00 33 00 34 00 36 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.3.7.3.4.6.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 35 00 37 00 34 00 35 00 37 00 39 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.>.3.5.7.4.5.7.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 33 00 37 00 33 00 34 00 36 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.3.7.3.4.6.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.0.1.6.<./.P.i.d.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.(.u.n.a.b.l.e. .t.o. .r.e.t.r.i.e.v.e.).<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 38 00 33 00 35 00 31 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.>.2.8.3.5.1.<./.U.p.t.i.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 38 00 36 00 39 00 38 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.8.8.6.9.8.8.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 39 00 30 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.9.0.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 32 00 31 00 37 00 37 00 39 00 32 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.>.1.3.2.1.7.7.9.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.0.4.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 33 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.3.0.0.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	88	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.2.1.6.8.<./.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	100	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 30 00 32 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.0.2.7.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 49 00 4e 00 51 00 55 00 49 00 52 00 59 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.>.I.N.Q.U.I.R.Y...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 70 00 75 00 73 00 71 00 75 00 64 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.>.p.u.s.q.u.d.,. .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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 70 00 75 00 73 00 71 00 75 00 64 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.>.p.u.s.q.u.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 39 00 36 00 39 00 33 00 36 00 35 00 32 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.>.1.5.5.9.6.9.3.6.5.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 31 00 2d 00 31 00 38 00 54 00 31 00 34 00 3a 00 30 00 32 00 3a 00 31 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.-.1.1.-.1.8.T.1.4.:.0.2.:.1.6.Z.".>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 38 00 39 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 35 00 33 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 38 00 35 00 33 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 00	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.2.". .P.I.D.=.".5.8.9.6.". .U.p.t.i.m.e.M.S.=.".1.8.5.3.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.8.5.3.1.". .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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 63 00 30 00 64 00 64 00 66 00 30 00 39 00 2d 00 36 00 62 00 36 00 30 00 2d 00 34 00 31 00 39 00 63 00 2d 00 61 00 31 00 33 00 34 00 2d 00 34 00 66 00 32 00 38 00 64 00 31 00 31 00 62 00 32 00 37 00 31 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.4.c.0.d.d.f.0.9.-.6.b.6.0.-.4.1.9.c.-.a.1.3.4.-.4.f.2.8.d.1.1.b.2.7.1.d.<./.G.u.i.d.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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 31 00 2d 00 31 00 38 00 54 00 31 00 34 00 3a 00 30 00 32 00 3a 00 31 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.-.1.1.-.1.8.T.1.4.:.0.2.:.1.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E55.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	6CBB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3106.tmp.xml	unknown	4587	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	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622\Report.wer	unknown	2	ff fe	..	success or wait	1	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622\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	224	6CBB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INQUIRY.exe_9acf60ae8258c649d949998398a696799dd6ab7_31a5ab7c_1a2a4622\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 37 00 34 00 32 00 33 00 38 00 35 00 35 00 32 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.7.4.2.3.8.5.5.2.1.	success or wait	1	6CBB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{50186b35-08f1-6d84-a4fd-998d570f6648}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD36BF	unknown
\REGISTRY\A\{50186b35-08f1-6d84-a4fd-998d570f6648}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CBD1FB2	RegCreateKeyExW
\REGISTRY\A\{50186b35-08f1-6d84-a4fd-998d570f6648}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBB43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 73 78 4E 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBD1FE8	RegSetValueExW

Analysis Process: INQUIRY.exe PID: 6076 Parent PID: 5788

General

Start time:	15:02:33
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.756918468.0000000002662000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.757155287.00000000026F7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.757155287.00000000026F7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.757155287.00000000026F7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.757155287.00000000026F7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.757155287.00000000026F7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 6808 Parent PID: 6076

General

Start time:	15:02:34
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
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: 00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source:

00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.825855451.00000000022E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000001.752146287.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000001.752146287.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000001.752146287.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000001.752146287.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000001.752146287.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.828298688.0000000002E11000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.826009202.0000000002372000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.826009202.0000000002372000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.826009202.0000000002372000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.826009202.0000000002372000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.826009202.0000000002372000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.829490755.0000000003E11000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.829490755.0000000003E11000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.824784026.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.824784026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.824784026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.824784026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.824784026.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.826605147.0000000002492000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.826605147.0000000002492000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.826605147.0000000002492000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.826605147.0000000002492000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.826605147.0000000002492000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.824923724.0000000000497000.00000040.00000001.sdmp, Author:

	Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.824923724.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.824923724.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.824923724.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.824923724.0000000000497000.00000040.00000001.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	722760AC	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	722760AC	unknown
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	722760AC	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	722760AC	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	243BCAB	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	243BCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	success or wait	1	2CA2D8E	DeleteFileW
C:\Users\user\AppData\Roaming\pidloc.txt	success or wait	1	2CA2D8E	DeleteFileW
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	2CA2D8E	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	2CA2D8E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 38 30 38	6808	success or wait	1	2CA0093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	34	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 49 4e 51 55 49 52 59 2e 65 78 65	C:\Users\user\Desktop\INQUIRY.exe	success or wait	1	2CA0093	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2CA0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2CA0093	ReadFile
C:\Users\user\Desktop\INQUIRY.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\INQUIRY.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	2CA0093	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	2CA0093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	2CA0093	ReadFile

Analysis Process: INQUIRY.exe PID: 6792 Parent PID: 6076

General

Start time:	15:02:35
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe' 2 6808 5404546
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 6936 Parent PID: 6808

General

Start time:	15:02:39
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2272
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 5684 Parent PID: 6808

General

Start time:	15:02:42
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.770041777.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 4184 Parent PID: 6808

General

Start time:	15:02:43
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000014.00000002.774520700.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 1076 Parent PID: 6808

General

Start time:	15:02:45
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6808 -s 2324
Imagebase:	0x990000
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: 00000016.00000002.820474176.0000000005470000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000016.00000002.820474176.0000000005470000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000016.00000002.820474176.0000000005470000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: INQUIRY.exe PID: 6400 Parent PID: 6792

General

Start time:	15:03:14
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000002.849214765.00000000026D7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.849214765.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000002.849214765.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000002.849214765.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000002.849214765.00000000026D7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000002.849044012.0000000002642000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.849044012.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000002.849044012.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000002.849044012.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000002.849044012.0000000002642000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 240 Parent PID: 6400

General

Start time:	15:03:14
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
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: 0000001C.00000002.859116925.00000000007A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.859116925.00000000007A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.859116925.00000000007A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected

WebBrowserPassView password recovery tool, Source: 0000001C.00000002.859116925.00000000007A0000.00000004.00000001.sdmp, Author: Joe Security

- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.859116925.00000000007A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.858712668.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.858712668.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.858712668.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.858712668.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.858712668.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.863445427.0000000003961000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.863445427.0000000003961000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000001.839775376.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000001.839775376.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000001.839775376.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000001.839775376.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000001.839775376.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.858806395.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.858806395.0000000000497000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.858806395.0000000000497000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.858806395.0000000000497000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.858806395.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.863200098.0000000002DDA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.863200098.0000000002DDA000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.863232173.0000000002DE0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.859836497.0000000002242000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.859836497.0000000002242000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.859836497.0000000002242000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.859836497.0000000002242000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.859836497.0000000002242000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.860072694.00000000022F2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.860072694.00000000022F2000.00000040.00000001.sdmp, Author:

	Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.860072694.00000000022F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.860072694.00000000022F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.860072694.00000000022F2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 6428 Parent PID: 6400

General

Start time:	15:03:16
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe' 2 240 5445406
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 204 Parent PID: 240

General

Start time:	15:03:22
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2100
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: INQUIRY.exe PID: 6900 Parent PID: 6428

General

Start time:	15:03:29
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000020.00000002.875783315.0000000002717000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000020.00000002.875783315.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000020.00000002.875783315.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000020.00000002.875783315.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000020.00000002.875783315.0000000002717000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000020.00000002.875508614.0000000002682000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000020.00000002.875508614.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000020.00000002.875508614.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000020.00000002.875508614.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000020.00000002.875508614.0000000002682000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 1364 Parent PID: 6900

General

Start time:	15:03:30
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INQUIRY.exe
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
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: 00000021.00000002.929210977.0000000003A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.929210977.0000000003A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.923851920.0000000002210000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.923851920.0000000002210000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.923851920.0000000002210000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.923851920.0000000002210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.923851920.0000000002210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.919336144.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.919336144.0000000000402000.00000040.00000001.sdmp, Author:

	Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.919336144.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.919336144.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.919336144.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000001.871375197.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000001.871375197.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000001.871375197.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000001.871375197.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.927425340.0000000002382000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.927425340.0000000002382000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.927425340.0000000002382000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.927425340.0000000002382000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.927425340.0000000002382000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.924535204.00000000022F2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.924535204.00000000022F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.924535204.00000000022F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.924535204.00000000022F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.924535204.00000000022F2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.919755783.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.919755783.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.919755783.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.919755783.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.919755783.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.928494489.0000000002A21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.928494489.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.928494489.0000000002A21000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: INQUIRY.exe PID: 4424 Parent PID: 6900

General

Start time:	15:03:31
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\INQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INQUIRY.exe' 2 1364 5460187
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	0B940145D7D02E5B1B975C99DD5197A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 6380 Parent PID: 1364

General

Start time:	15:03:34
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2284
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vbc.exe PID: 5396 Parent PID: 1364

General

Start time:	15:03:38
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000024.00000002.888584585.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: vbc.exe PID: 3064 Parent PID: 1364

General

Start time:	15:03:38
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000025.00000002.894159498.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 7076 Parent PID: 1364

General

Start time:	15:03:40
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1364 -s 2096
Imagebase:	0x990000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis