

ID: 626423
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.39649730.16343.2439
Cookbook: default.jbs
Time: 00:37:32
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Trojan.GenericKD.39649730.16343.2439 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 5
System Summary 5
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 12
Public IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.log 14
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies 15
Static File Info 15
General 15
File Icon 15
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 21
DNS Answers 21
SMTP Packets 21
Statistics 21
Behavior 21
System Behavior 22

Copyright Joe Security LLC 2022

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exePID: 3692, Parent PID: 4968 22
General 22
File Activities 22
File Created 22
File Written 23
File Read 23
Analysis Process: SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exePID: 2560, Parent PID: 3692 23
General 23
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 25
Disassembly 25

Copyright Joe Security LLC 2022

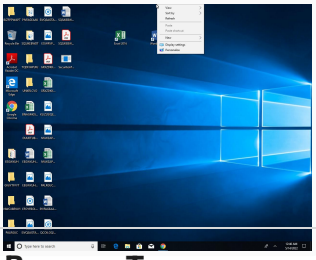
Windows Analysis Report

SecuriteInfo.com.Trojan.GenericKD.39649730.16343.2439

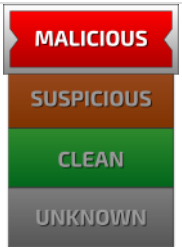
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.2439 (renamed file extension from 2439 to exe)
Analysis ID:	626423
MD5:	351a6ff6c8aef2f…
SHA1:	86b49c51155b6e..
SHA256:	6099e48acdfc2f1..
Tags:	exe
Infos:	



Detection



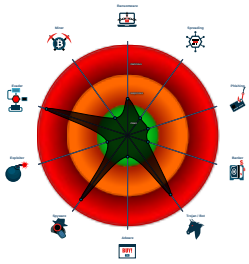
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe (PID: 3692 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe" MD5: 351A6FF6C8AEF2F1F3FCC9CD8C0DFD8E)
  - SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe (PID: 2560 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe MD5: 351A6FF6C8AEF2F1F3FCC9CD8C0DFD8E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "v.saniuk@ibc.by",
  "Password": "QWErty654321",
  "Host": "webmail.active.by"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.272202502.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.272202502.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.272808462.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000004.00000000.272808462.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000002.510960801.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32d6f:$s10: logins • 0x327d6:$s11: credential • 0x2ed99:$g1: get_Clipboard • 0x2eda7:$g2: get_Keyboard • 0x2edb4:$g3: get_Password • 0x300af:$g4: get_CtrlKeyDown • 0x300bf:$g5: get_ShiftKeyDown • 0x300d0:$g6: get_AltKeyDown
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 32 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Copyright Joe Security LLC 2022

Data Obfuscation



.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion



Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

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

HIPS / PFW / Operating System Protection Evasion



.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality



Yara detected AgentTesla

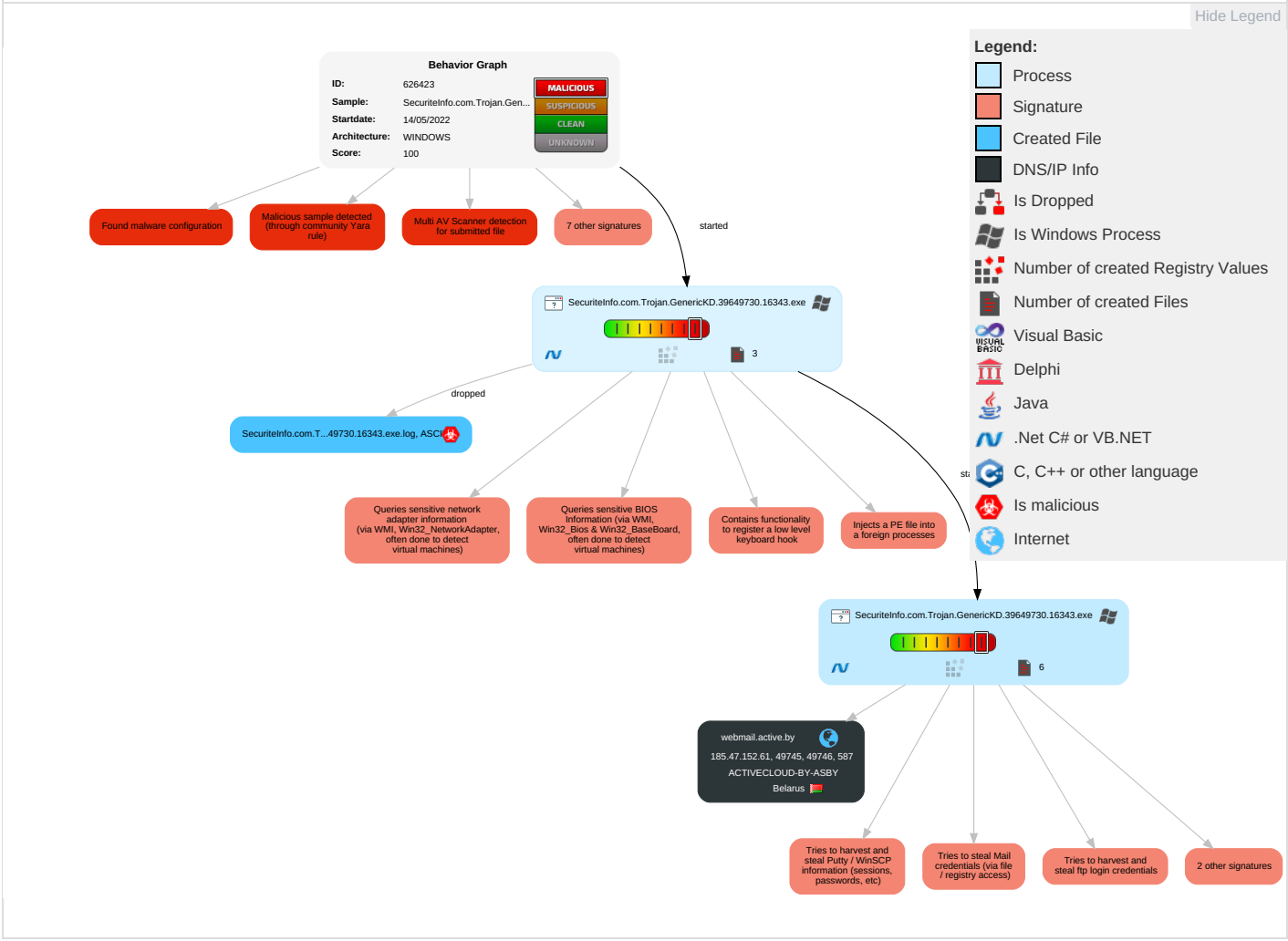
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	2 1 1 Input Capture	1 Process Discovery	Remote Desktop Protocol	2 1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

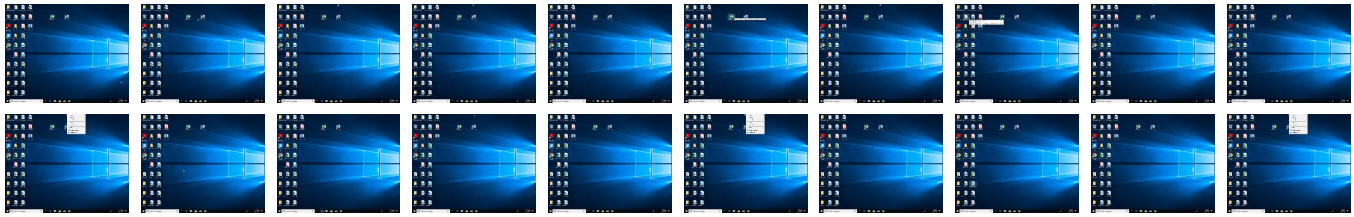
Behavior Graph



Screenshots

Thumbnails

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



Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe	33%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Copyright Joe Security LLC 2022

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kry	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krN.TTFp	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://WuEWlY.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.sandoll.co.krl	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.fontbureau.comoitu3	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.goodfont.co.krFT	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://SF7VJVWyAkXSzaT8.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr&	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://https://SF7VJVWyAkXSzaT8.com8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.active.by	185.47.152.61	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.0000 0000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.0000 0000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.2522489 30.0000000005351000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kry	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.00000000 05346000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krN.TTFp	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.00000000 05346000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://WuEWlY.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krl	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.00000000 05346000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.253829018.00000000 05342000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://webmail.active.by	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.514453925.00000000 03227000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.514578396.000000000326D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.typography.netD	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comoitu3	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.288764673.00000000 05340000.00000004.00000800.00020000.0000 0000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.259518998.00000000 0537E000.00000004.00000800.00020000.0000 0000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649 730.16343.exe, 00000000.00000003.2591301 81.000000000537E000.00000004.00000800.00 020000.00000000.sdmp, SecuriteInfo.com.T rojan.GenericKD.39649730.16343.exe, 0000 0000.00000003.259303763.000000000537E000 .00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.1634 3.exe, 00000000.00000003.260320170.00000 0000537D000.00000004.00000800.00020000.0 0000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39 649730.16343.exe, 00000000.00000003.2597 91661.000000000537E000.00000004.00000800 .00020000.00000000.sdmp, SecuriteInfo.co m.Trojan.GenericKD.39649730.16343.exe, 0 0000000.00000003.259701206.000000000537E 000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.1 6343.exe, 00000000.00000003.259471979.00 0000000537E000.00000004.00000800.0002000 0.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD .39649730.16343.exe, 00000000.00000003.2 59344901.000000000537E000.00000004.00000 800.00020000.00000000.sdmp, SecuriteInfo.com.Troja n.GenericKD.39649730.16343.exe, 00000000 .00000003.259609928.000000000537E000.000 00004.00000800.00020000.00000000.sdmp, S ecuriteInfo.com.Trojan.GenericKD.39649730.16343.ex e, 00000000.00000003.259911250.000000000 537D000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Trojan.GenericKD.396497 30.16343.exe, 00000000.00000003.25905667 2.000000000537E000.00000004.00000800.000 20000.00000000.sdmp, SecuriteInfo.com.Tr ojan.GenericKD.39649730.16343.exe, 00000 000.00000003.259200492.000000000537E000. 00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16343 .exe, 00000000.00000003.259281371.000000 000537E000.00000004.00000800.00020000.00 000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.396 49730.16343.exe, 00000000.00000003.26018 2995.000000000537D000.00000004.00000800. 00020000.00000000.sdmp, SecuriteInfo.com .Trojan.GenericKD.39649730.16343.exe, 00 000000.00000003.259547743.000000000537E0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16 343.exe, 00000000.00000003.259577319.000 000000537E000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD. 39649730.16343.exe, 00000000.00000003.25 9756828.000000000537E000.00000004.000008 00.00020000.00000000.sdmp, SecuriteInfo. com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.259947152.00000000053 7D000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730 .16343.exe, 00000000.00000003.260104307. 000000000537D000.00000004.00000800.00020 000.00000000.sdmp, SecuriteInfo.com.Trojan.Generic KD.39649730.16343.exe, 00000000.00000003 .258994813.000000000537E000.00000004.000 00800.00020000.00000000.sdmp, SecuriteIn fo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.260143045.00000000 0537D000.00000004.00000800.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.0000 0000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp//	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.253829018.00000000 05342000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.253829018.00000000 05342000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.0000000006552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.krFT	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.00000000 05346000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.0000000005346000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.289013797.00000000 06552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://SF7VJVWyAkXSzaT8.com	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr&	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000003.251445922.00000000 05346000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com=	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000000.00000002.288764673.00000000 05340000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://SF7VJVWyAkXSzaT8.com8	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe, 00000004.00000002.513468896.00000000 02ED1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.47.152.61	webmail.active.by	Belarus		202090	ACTIVECLOUD-BY-ASBY	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626423
Start date and time: 14/05/202200:37:32	2022-05-14 00:37:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.2439 (renamed file extension from 2439 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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1.1%) • Quality average: 65.1% • Quality standard deviation: 39.4%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:38:43	API Interceptor	735x Sleep call for process: SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu

MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.751594485393351
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
File size:	675840
MD5:	351a6ff6c8aef2f1f3fcc9cd8c0dfd8e
SHA1:	86b49c51155b6e3997a45e0ad1adef77722d4f6e
SHA256:	6099e48acdfc2f116c21d55e3aff1a1b7bc0d4c5841ee5506f762cd66935ca2e
SHA512:	c4f7c6857b511e50ada9fcc4ccd149a39dce2903f8e58ab38126794847f264ba9069c4de64a46a9f5065ba3781b1a61380a653799d3cd31aca57220c4b2853e6
SSDEEP:	12288:s/RR9cMw+idI0lWyrzmdcRURevzuVKane+jQ+oEvf7p97QbW:4qAOzlZemuVBne3Zap
TLSH:	8BE4F17DF2E78E63CB2522B6C0EB590403A05A5BD673E3AA2B4151E54D03BD39D42BC7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~b.....0..H.....f... .....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a660e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627E0DE1 [Fri May 13 07:50:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Copyright Joe Security LLC 2022

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

Copyright Joe Security LLC 2022

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa65c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x3bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa655f	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa4614	0xa4800	False	0.872511101349	SysEx File -	7.76001062943	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x3bc	0x400	False	0.380859375	data	3.02433380393	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa8058	0x364	data		

Imports

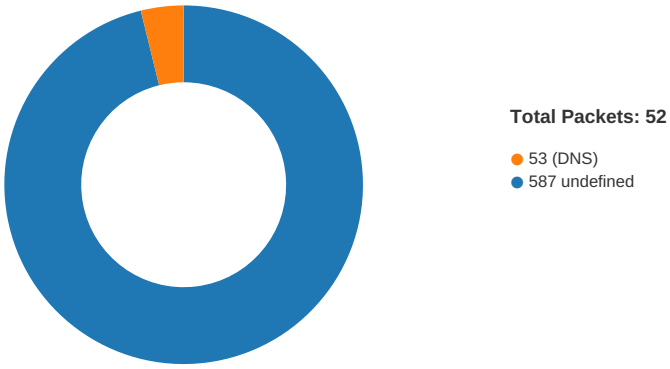
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	AssemblyAlgorithmIdAttrib.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ResetEvent
ProductVersion	1.0.0.0
FileDescription	ResetEvent
OriginalFilename	AssemblyAlgorithmIdAttrib.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 00:38:59.679438114 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:38:59.746223927 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:38:59.746365070 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:38:59.813838005 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:38:59.814126968 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:38:59.881165981 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:38:59.881213903 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:38:59.881433010 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:38:59.956746101 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.032051086 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.096976995 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.097007990 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.097033978 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.097047091 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.097119093 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.097150087 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.103696108 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.171617985 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.242981911 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.307900906 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.308996916 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.373702049 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.381966114 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.487729073 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.568512917 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.570369959 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.635299921 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.635354996 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.636518955 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.701631069 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.705959082 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.779897928 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.782213926 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.782655954 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.783776999 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.784034014 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:00.847397089 CEST	587	49745	185.47.152.61	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 00:39:00.848531961 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:00.848915100 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:01.067194939 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:01.125231028 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:01.125559092 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:01.997858047 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.062716007 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.062747002 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.062959909 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.063410044 CEST	587	49745	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.063486099 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.074456930 CEST	49745	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.128956079 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.194772959 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.194957018 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.261580944 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.261873960 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.328174114 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.328217030 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.328465939 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.404619932 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.405039072 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.470732927 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.470784903 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.470824003 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.470853090 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.470880985 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.470935106 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.472127914 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.540873051 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.542937994 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.608890057 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.609313011 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.675415039 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.675900936 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.785697937 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.895184040 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.895605087 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:02.961004019 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.961025953 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:02.961328030 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.026959896 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.027287960 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.101412058 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.103316069 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.103444099 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.103621960 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.103800058 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.103874922 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.103952885 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.104023933 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.104096889 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:39:03.168987989 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.169133902 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.169300079 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.169759989 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:39:03.259846926 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:40:39.611948013 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:40:39.677751064 CEST	587	49746	185.47.152.61	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 00:40:39.677792072 CEST	587	49746	185.47.152.61	192.168.2.3
May 14, 2022 00:40:39.677942991 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:40:39.678169012 CEST	49746	587	192.168.2.3	185.47.152.61
May 14, 2022 00:40:39.678837061 CEST	587	49746	185.47.152.61	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 00:38:59.641088963 CEST	49316	53	192.168.2.3	8.8.8.8
May 14, 2022 00:38:59.660692930 CEST	53	49316	8.8.8.8	192.168.2.3
May 14, 2022 00:39:02.108280897 CEST	56417	53	192.168.2.3	8.8.8.8
May 14, 2022 00:39:02.127830029 CEST	53	56417	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 00:38:59.641088963 CEST	192.168.2.3	8.8.8.8	0x9f7d	Standard query (0)	webmail.active.by	A (IP address)	IN (0x0001)
May 14, 2022 00:39:02.108280897 CEST	192.168.2.3	8.8.8.8	0xfb9d	Standard query (0)	webmail.active.by	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 00:38:59.660692930 CEST	8.8.8.8	192.168.2.3	0x9f7d	No error (0)	webmail.active.by		185.47.152.61	A (IP address)	IN (0x0001)
May 14, 2022 00:39:02.127830029 CEST	8.8.8.8	192.168.2.3	0xfb9d	No error (0)	webmail.active.by		185.47.152.61	A (IP address)	IN (0x0001)

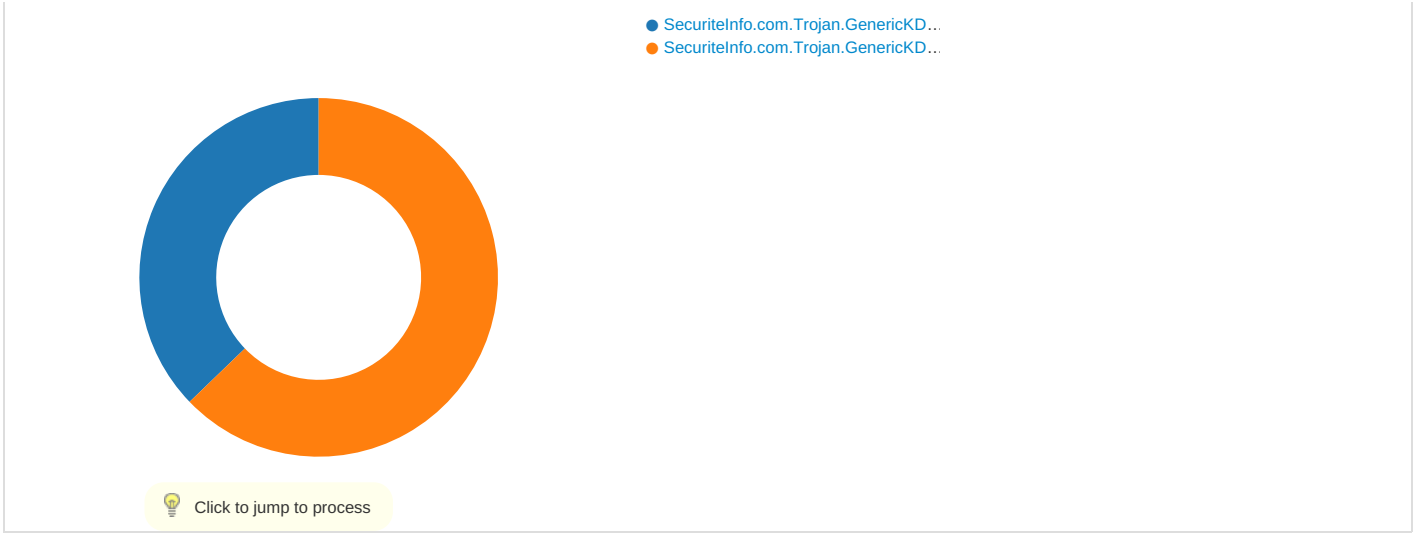
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 00:38:59.813838005 CEST	587	49745	185.47.152.61	192.168.2.3	220 webmail.active.by ESMTP Exim
May 14, 2022 00:38:59.814126968 CEST	49745	587	192.168.2.3	185.47.152.61	EHLO 760639
May 14, 2022 00:38:59.881213903 CEST	587	49745	185.47.152.61	192.168.2.3	250-webmail.active.by Hello 760639 [84.17.52.36] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 00:38:59.881433010 CEST	49745	587	192.168.2.3	185.47.152.61	STARTTLS
May 14, 2022 00:38:59.956746101 CEST	587	49745	185.47.152.61	192.168.2.3	220 TLS go ahead
May 14, 2022 00:39:02.261580944 CEST	587	49746	185.47.152.61	192.168.2.3	220 webmail.active.by ESMTP Exim
May 14, 2022 00:39:02.261873960 CEST	49746	587	192.168.2.3	185.47.152.61	EHLO 760639
May 14, 2022 00:39:02.328217030 CEST	587	49746	185.47.152.61	192.168.2.3	250-webmail.active.by Hello 760639 [84.17.52.36] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 00:39:02.328465939 CEST	49746	587	192.168.2.3	185.47.152.61	STARTTLS
May 14, 2022 00:39:02.404619932 CEST	587	49746	185.47.152.61	192.168.2.3	220 TLS go ahead

Statistics

Behavior

Copyright Joe Security LLC 2022



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe PID: 3692, Parent PID: 4968

General

Target ID:	0
Start time:	00:38:33
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe"
Imagebase:	0x90000
File size:	675840 bytes
MD5 hash:	351A6FF6C8AEF2F1F3FCC9CD8C0DFD8E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.286867007.0000000003710000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.286867007.0000000003710000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.286449493.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.286449493.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284509153.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	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	6DC1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF2C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe.log	0	1308	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF2C907	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	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe PID: **2560**, Parent PID: **3692**

General

Target ID:	4
Start time:	00:38:45
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.39649730.16343.exe
Imagebase:	0xcb0000
File size:	675840 bytes
MD5 hash:	351A6FF6C8AEF2F1F3FCC9CD8C0DFD8E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.272202502.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.272202502.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.272808462.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.272808462.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.510960801.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.510960801.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.273600180.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.273600180.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.274625372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.274625372.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.513468896.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.513468896.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	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	6DC1CF06	unknown
C:\Users\user\AppData\Roaming\dexqxm4g.x3e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CA6DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies	success or wait	1	6CA66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C g 8	success or wait	1	6CA6DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Roaming\dexqxm4g.x3e\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CA61B4F	ReadFile

Disassembly

No disassembly