ID: 756116
Sample Name: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Cookbook: default.jbs
Time: 16:49:16
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

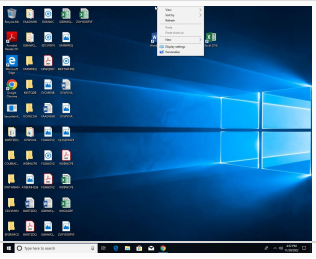
Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe

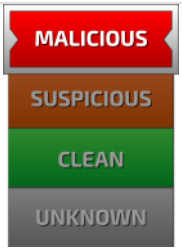
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Analysis ID:	756116
MD5:	fe1aa7fa995970e.
SHA1:	7505b261cc9df8…
SHA256:	655b12a219d0f0..
Tags:	AgentTesla exe
Infos:	



Detection



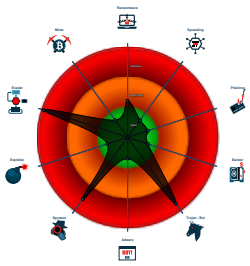
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- 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…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe (PID: 4580 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
  - schtasks.exe (PID: 5756 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nrQtAokXKaSn" /XML "C:\Users\user\AppData\Local\Temp\tmp152E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe (PID: 5688 cmdline: {path} MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
  - SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe (PID: 5900 cmdline: {path} MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
- nrQtAokXKaSn.exe (PID: 5976 cmdline: C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
  - schtasks.exe (PID: 1372 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nrQtAokXKaSn" /XML "C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nrQtAokXKaSn.exe (PID: 2744 cmdline: {path} MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
  - nrQtAokXKaSn.exe (PID: 1008 cmdline: {path} MD5: FE1AA7FA995970EBB34465D5DC0D8CE1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.strictfacilityservices.com",
  "Username": "accounts@strictfacilityservices.com",
  "Password": "SFS!@#321"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31cca:$a13: get_DnsResolver • 0x303f4:$a20: get_LastAccessed • 0x326d7:$a27: set_InternalServerPort • 0x32a20:$a30: set_GuidMasterKey • 0x30506:$a33: get_Clipboard • 0x30514:$a34: get_Keyboard • 0x318b5:$a35: get_ShiftKeyDown • 0x318c6:$a36: get_AltKeyDown • 0x30521:$a37: get_Password • 0x31010:$a38: get_PasswordHash • 0x3210b:$a39: get_DefaultCredentials
0000000B.00000002.532293061.0000000002CF4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000002.533369231.00000000028E4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.3e33c90.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.3e33c90.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.3e33c90.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32bcc:$s10: logins • 0x3264c:$s11: credential • 0x2e906:$g1: get_Clipboard • 0x2e914:$g2: get_Keyboard • 0x2e921:$g3: get_Password • 0x2fca5:$g4: get_CtrlKeyDown • 0x2fcb5:$g5: get_ShiftKeyDown • 0x2fcc6:$g6: get_AltKeyDown
0.2.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.3e33c90.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x300ca:$a13: get_DnsResolver • 0x2e7f4:$a20: get_LastAccessed • 0x30ad7:$a27: set_InternalServerPort • 0x30e20:$a30: set_GuidMasterKey • 0x2e906:$a33: get_Clipboard • 0x2e914:$a34: get_Keyboard • 0x2fcb5:$a35: get_ShiftKeyDown • 0x2fcc6:$a36: get_AltKeyDown • 0x2e921:$a37: get_Password • 0x2f410:$a38: get_PasswordHash • 0x3050b:$a39: get_DefaultCredentials
0.2.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.2cfbae8.0.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0x29ecc:$reg1: SOFTWARE\Microsoft\Windows Defender\Features • 0x29f10:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0x29f58:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0x2a1e4:$s1: Set-MpPreference -SignatureDisableUpdateOnStartupWithoutuser $true • 0x2a248:$s2: Set-MpPreference -DisableArchiveScanning $true • 0x2a2a0:$s3: Set-MpPreference -DisableIntrusionPreventionSystem $true • 0x2a2f8:$s4: Set-MpPreference -DisableScriptScanning $true • 0x2a344:$s5: Set-MpPreference -SubmitSamplesConsent 2 • 0x2a384:$s6: Set-MpPreference -MAPSReporting 0 • 0x2a3d0:$s7: Set-MpPreference -HighThreatDefaultAction 6 • 0x2a428:$s8: Set-MpPreference -ModerateThreatDefaultAction 6 • 0x2a478:$s9: Set-MpPreference -LowThreatDefaultAction 6 • 0x2a4c8:$s10: Set-MpPreference -SevereThreatDefaultAction 6
Click to see the 13 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.6 - Destination IP: 111.118.212.38 −

Timestamp:	192.168.2.6111.118.212.38497175872030171 11/29/22-16:51:24.449797
SID:	2030171
Source Port:	49717
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.6 - Destination IP: 111.118.212.38 −

Timestamp:	192.168.2.6111.118.212.38497225872030171 11/29/22-16:52:18.188399
SID:	2030171
Source Port:	49722
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

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

Copyright Joe Security LLC 2022

Boot Survival

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

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

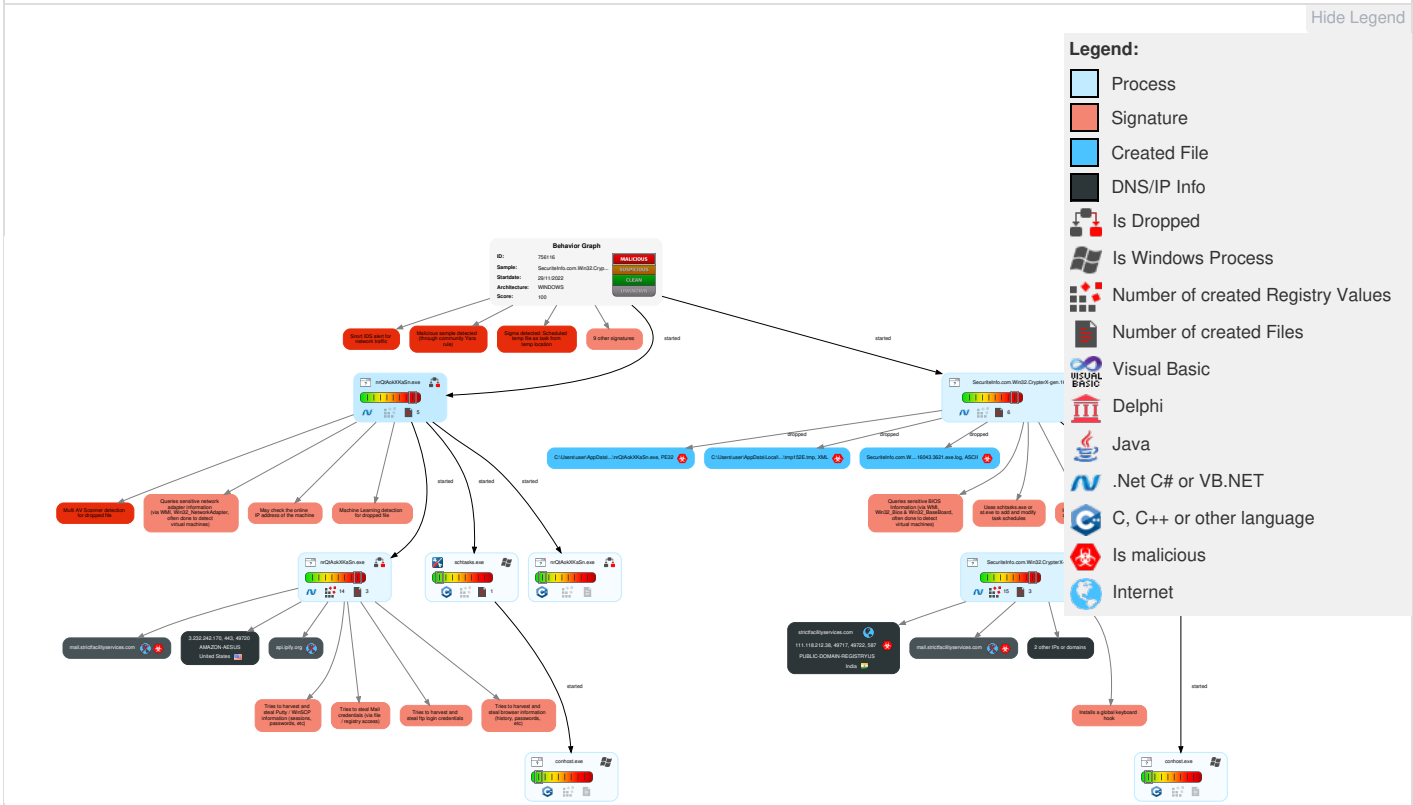
Yara detected AgentTesla

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	1 Scheduled Task/Job	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

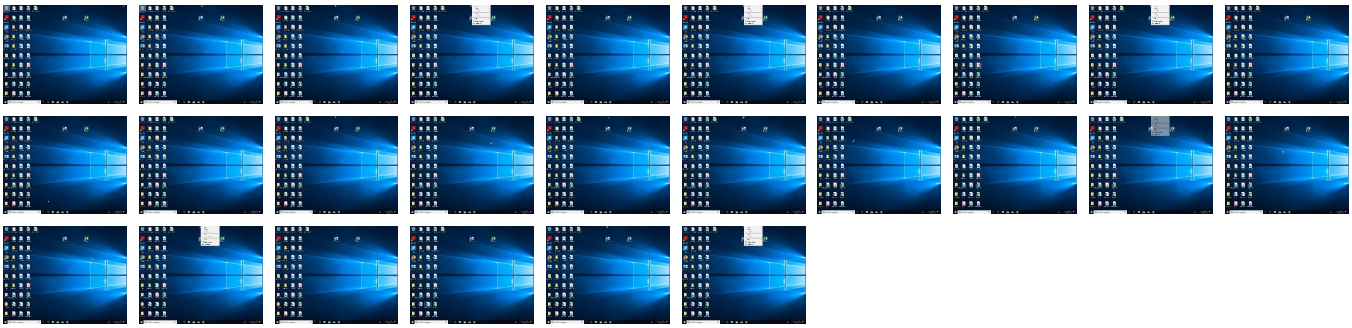
Behavior Graph



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.Win32.CrypterX-gen.16043.3621.exe	32%	ReversingLabs	Win32.Trojan.AgentTesla	
SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe	32%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdH-u	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s-P	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/&-c	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://strictfacilityservices.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y001	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm/	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgmail.strictfacilityservices.comaccounts	0%	Avira URL Cloud	safe	
http://UrUbMY.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/--	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comd--	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.coms-P	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/d	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv_-l	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comml-Y	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasF;-	0%	Avira URL Cloud	safe	
http://www.carterandcone.com%(	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.urwpp.deeg	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.comE.TTF	0%	URL Reputation	safe	
http://mail.strictfacilityservices.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/H-u	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd&-c	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomt	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/;-	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdf	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/&-c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/_-l	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/--	0%	Avira URL Cloud	safe	
http://https://OPBeIPZ8XbJqLOvY6X.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	52.20.78.240	true	false		unknown
strictfacilityservices.com	111.118.212.38	true	true		unknown
api.ipify.org	unknown	unknown	false		high
mail.strictfacilityservices.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.531415625.0000000002CA1000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://UrUbMY.com	nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/s-P	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdH-u	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272466078.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/&-c	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://strictfacilityservices.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.538758099.0000000002F8D000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.539377168.0000000002B6E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y001	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgmail.strictfacilityservices.comaccounts	nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272447141.0000000005A47000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271875759.0000000005A4A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm/	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.274751062.0000000005A43000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.266402265.0000000005A4C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269749174.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268520007.0000000005A57000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268864547.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269636094.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269244387.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269116939.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268302757.0000000005A57000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269536974.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269576221.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269468103.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269037859.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267000618.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269366094.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269305227.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm2	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.274751062.0000000005A43000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/--	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.531415625.0000000002CA1000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271614897.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271209683.0000000005A51000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271153816.0000000005A51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coms-P	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.316302127.0000000005A40000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html/	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268958128.0000000005A4A000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268838022.0000000005A4A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd--	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comB.TTF	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/d	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.265019576.0000000005A59000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.264911934.0000000005A57000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.264791589.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comrsiv_-l	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272466078.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comasF;-	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271614897.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comml-Y	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.316302127.0000000005A40000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com%(	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.266402265.0000000005A4C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269749174.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270130809.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268520007.0000000005A57000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268864547.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270302429.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269636094.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269244387.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269116939.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268302757.0000000005A57000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270410317.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270179920.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269843779.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269945334.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269536974.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270233958.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269576221.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269468103.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269037859.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273210069.0000000005A48000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270890643.0000000005A4A000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273089223.0000000005A48000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273295422.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.318278212.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.531415625.0000000002CA1000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 0000000C.00000002.433160611.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsd	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/H-u	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269749174.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268864547.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269636094.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269244387.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269116939.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269536974.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269576221.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269468103.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269037859.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269366094.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269305227.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.274806173.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272335142.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.strictfacilityservices.com	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.538758099.0000000002F8D000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.539377168.0000000002B6E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/P	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 0000000B.00000002.531415625.0000000002CA1000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/;-	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267000618.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdf	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271614897.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

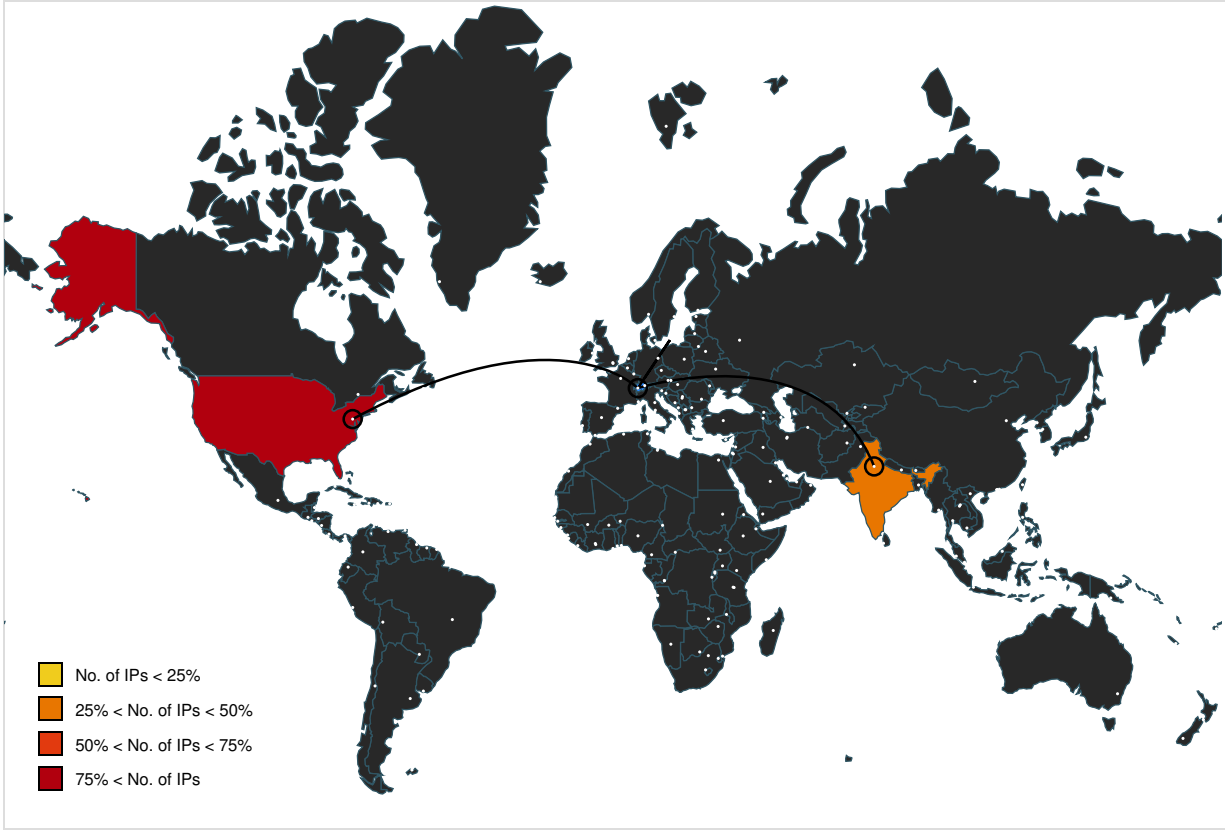
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcomt	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272335142.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271614897.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269749174.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.270013809.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268864547.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269636094.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269244387.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269116939.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269843779.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269945334.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269536974.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269576221.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269468103.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269037859.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269366094.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269800007.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269305227.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271886008.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271614897.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271964358.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273916785.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deeg	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273089223.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comd&-c	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272335142.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272466078.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.264791589.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comoitu	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272335142.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272466078.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272565753.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/t	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267000618.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.272325014.0000000005A46000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269800007.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.269305227.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.265582317.0000000005A57000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000002.341560116.0000000006C52000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.271875759.0000000005A4A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/&-c	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267565316.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267000618.0000000005A43000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/--	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/_-l	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268506637.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268654675.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.268296688.0000000005A55000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.267904029.0000000005A55000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comE.TTF	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273496235.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273102970.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273306720.0000000005A50000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273005972.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe, 00000000.00000003.273220976.0000000005A4F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://OPBeIPZ8XbJqLOvY6X.net	nrQtAokXKaSn.exe, 00000010.00000002.538774344.0000000002B2F000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.539333299.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp, nrQtAokXKaSn.exe, 00000010.00000002.539499206.0000000002B7C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.232.242.170	unknown	United States		14618	AMAZON-AESUS	false
111.118.212.38	strictfacilityservices.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true
52.20.78.240	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756116
Start date and time:	2022-11-29 16:49:16 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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@16/5@8/3
EGA Information:	• Successful, ratio: 100%

Copyright Joe Security LLC 2022

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe

Simulations

Behavior and APIs

Time	Type	Description
16:50:37	API Interceptor	432x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe modified
16:50:45	Task Scheduler	Run new task: nrQtAokXKaSn path: C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
16:51:22	API Interceptor	69x Sleep call for process: nrQtAokXKaSn.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.Win32.CrypterX-gen.16043.3621.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nrQtAokXKaSn.exe.log

Process:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp152E.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.1584897189168
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3PItn:cbha7JlNQV/rydbz9I3YODOLNdq3Ju
MD5:	03051B1F18A035DE03D059366AC0473E
SHA1:	155345324D235531556DDFE9F16B9C056D4C9505
SHA-256:	92BF6136677687B06E7E22A50F24B0DD8B0B5FA6C3A89DA9516AAC6259ACA56D
SHA-512:	1EB4CCBBD475035EAEF04AFCEB318583B8BB26F350AF5B68D7F19D080AEEADA96B67E00DC89DE4CA4608561B3F6AB64D135A505B322D24BBDE60437B8FA49 1CC
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp

Process:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657

Entropy (8bit):	5.1584897189168
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3PItn:cbha7JlNQV/rydbz9I3YODOLNdq3Ju
MD5:	03051B1F18A035DE03D059366AC0473E
SHA1:	155345324D235531556DDFE9F16B9C056D4C9505
SHA-256:	92BF6136677687B06E7E22A50F24B0DD8B0B5FA6C3A89DA9516AAC6259ACA56D
SHA-512:	1EB4CCBBD475035EAEF04AFCEB318583B8BB26F350AF5B68D7F19D080AEEADA96B67E00DC89DE4CA4608561B3F6AB64D135A505B322D24BBDE60437B8FA491CC
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	847360
Entropy (8bit):	7.451826150772928
Encrypted:	false
SSDEEP:	12288:/mMlc1PL/pFr5cE8LHWU/SEdRMA/LyVu6gtXSRxS36qGn3eV6H5ADAUaoZqxIB/N:eqvLj9/L1tsAK/n3eVk55Ul4x+/yIn
MD5:	FE1AA7FA995970EBB34465D5DC0D8CE1
SHA1:	7505B261CC9DF8C6AB8F10E035CF8D8319043CDB
SHA-256:	655B12A219D0F0E39A84FE44483E25411BE852CE2BB0D451A1CB1A9A670F70B8
SHA-512:	245277E1F0F637BDA7E2B5D1F76AE06656AEB0A7DF47EB428EDF8C6472F9AF03580234B9CD4A95321A96E6511D9E75279C452C5B58AE182B060A6CA35949A77C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....P..... ... .@.. .....`..... .@.....K.... .....@.....[..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.relo c.....@.....@..B.....H.....:.....Z(....8.....(....8....*.&~.....*...~....*.b(....8.....(....8.....*...&~.....*...~....*..0..~.....8O... ....E....$...8....s.....8....s.....8)...*s.....8....s.....8....(....8....s..... .....:....& ....8.....0.....~....o.....8.....*8....8.....0..$.....8....8....8.....*.~....o.....8.....0.....~. ...o.....8....8....8.....*..0.....~....o.....8....8....8....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.451826150772928
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
File size:	847360
MD5:	fe1aa7fa995970ebb34465d5dc0d8ce1
SHA1:	7505b261cc9df8c6ab8f10e035cf8d8319043cdb
SHA256:	655b12a219d0f0e39a84fe44483e25411be852ce2bb0d451a1cb1a9a670f70b8
SHA512:	245277e1f0f637bda7e2b5d1f76ae06656aeb0a7df47eb428edf8c6472f9af03580234b9cd4a95321a96e6511d9e75279c452c5b58ae182b060a6ca35949a77c
SSDEEP:	12288:/mMlc1PL/pFr5cE8LHWU/SEdRMA/LyVu6gtXSRxS36qGn3eV6H5ADAUaoZqxIB/N:eqvLj9/L1tsAK/n3eVk55Ul4x+/yIn
TLSH:	B0057C9573728973F1CF01359095718C6EBCE543A2A6E2076FB63A8146027BFFA9CE41
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....P..... ... .@.. .....`.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d02ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385E21F [Tue Nov 29 10:42:39 2022 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:	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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd02a0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd025b	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	0xce2f4	0xce400	False	0.764352509469697	data	7.457613017086461	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5c8	0x600	False	0.427734375	data	4.1465073095381015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd20a0	0x33c	data		
RT_MANIFEST	0xd23dc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6111.118.212.38497175872030171 11/29/22-16:51:24.449797	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49717	587	192.168.2.6	111.118.212.38

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6111.118.212.38497225872030171 11/29/22-16:52:18.188399	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49722	587	192.168.2.6	111.118.212.38

Network Port Distribution

Total Packets: 53

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:57.881586075 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:57.881650925 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:57.881889105 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:58.005610943 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:58.005644083 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:58.314330101 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:58.314445019 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:58.332873106 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:58.332928896 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:58.333657026 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:58.413805962 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:59.610924959 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:59.610958099 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:59.757527113 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:59.757646084 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:50:59.757844925 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:50:59.763855934 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:51:19.879105091 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:20.153131008 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:20.155756950 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:21.977685928 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:21.978070021 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:22.252252102 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:22.253521919 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:22.526686907 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:22.527221918 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:22.840261936 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:23.584398985 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:23.585345030 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:23.860565901 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:23.860614061 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:23.860863924 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:24.168071032 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:24.169872999 CET	49717	587	192.168.2.6	111.118.212.38

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:51:24.442694902 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:24.443375111 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:24.449796915 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:24.449903011 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:24.449991941 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:24.450061083 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:24.722711086 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:24.724167109 CET	587	49717	111.118.212.38	192.168.2.6
Nov 29, 2022 16:51:24.771972895 CET	49717	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:51:46.825879097 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:46.825941086 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:46.826066017 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:46.846575975 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:46.846611977 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:47.147500992 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:47.147674084 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:47.156049967 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:47.156074047 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:47.156639099 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:47.261645079 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:48.546381950 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:48.546422958 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:48.813997984 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:48.814122915 CET	443	49720	3.232.242.170	192.168.2.6
Nov 29, 2022 16:51:48.814193010 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:51:48.816801071 CET	49720	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:52:11.437999010 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:11.715953112 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:11.716146946 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:14.190653086 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:14.194787025 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:14.473042011 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:14.499712944 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:14.778090954 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:14.842102051 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:16.164179087 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:16.482769012 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.294580936 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.297631979 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:17.575767994 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.575813055 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.576160908 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:17.894834995 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.900510073 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:17.901293039 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:18.179555893 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:18.179738045 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:18.188399076 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:18.188513041 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:18.188616991 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:18.188690901 CET	49722	587	192.168.2.6	111.118.212.38
Nov 29, 2022 16:52:18.466383934 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:18.467991114 CET	587	49722	111.118.212.38	192.168.2.6
Nov 29, 2022 16:52:18.514267921 CET	49722	587	192.168.2.6	111.118.212.38

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:57.772516966 CET	59082	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:57.789524078 CET	53	59082	8.8.8.8	192.168.2.6
Nov 29, 2022 16:50:57.822091103 CET	59504	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:50:57.841023922 CET	53	59504	8.8.8.8	192.168.2.6
Nov 29, 2022 16:51:19.333461046 CET	63229	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:51:19.724127054 CET	53	63229	8.8.8.8	192.168.2.6
Nov 29, 2022 16:51:19.859044075 CET	62538	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:51:19.876422882 CET	53	62538	8.8.8.8	192.168.2.6
Nov 29, 2022 16:51:46.733128071 CET	56122	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:51:46.752038956 CET	53	56122	8.8.8.8	192.168.2.6
Nov 29, 2022 16:51:46.779407978 CET	52556	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:51:46.796346903 CET	53	52556	8.8.8.8	192.168.2.6
Nov 29, 2022 16:52:10.584884882 CET	52481	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:52:10.964626074 CET	53	52481	8.8.8.8	192.168.2.6
Nov 29, 2022 16:52:11.035455942 CET	53943	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:52:11.434695959 CET	53	53943	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:57.772516966 CET	192.168.2.6	8.8.8.8	0x2ea1	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.822091103 CET	192.168.2.6	8.8.8.8	0xa8aa	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:19.333461046 CET	192.168.2.6	8.8.8.8	0xe3da	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:19.859044075 CET	192.168.2.6	8.8.8.8	0xf4ba	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.733128071 CET	192.168.2.6	8.8.8.8	0x1df9	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.779407978 CET	192.168.2.6	8.8.8.8	0x6660	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:10.584884882 CET	192.168.2.6	8.8.8.8	0x1930	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:11.035455942 CET	192.168.2.6	8.8.8.8	0xd825	Standard query (0)	mail.strictfacilityservices.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:57.789524078 CET	8.8.8.8	192.168.2.6	0x2ea1	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:50:57.789524078 CET	8.8.8.8	192.168.2.6	0x2ea1	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.789524078 CET	8.8.8.8	192.168.2.6	0x2ea1	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.789524078 CET	8.8.8.8	192.168.2.6	0x2ea1	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.789524078 CET	8.8.8.8	192.168.2.6	0x2ea1	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.841023922 CET	8.8.8.8	192.168.2.6	0xa8aa	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:50:57.841023922 CET	8.8.8.8	192.168.2.6	0xa8aa	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.841023922 CET	8.8.8.8	192.168.2.6	0xa8aa	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:57.841023922 CET	8.8.8.8	192.168.2.6	0xa8aa	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:57.841023922 CET	8.8.8.8	192.168.2.6	0xa8aa	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:19.724127054 CET	8.8.8.8	192.168.2.6	0xe3da	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:19.724127054 CET	8.8.8.8	192.168.2.6	0xe3da	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:19.876422882 CET	8.8.8.8	192.168.2.6	0xf4ba	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:19.876422882 CET	8.8.8.8	192.168.2.6	0xf4ba	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.752038956 CET	8.8.8.8	192.168.2.6	0x1df9	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:46.752038956 CET	8.8.8.8	192.168.2.6	0x1df9	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.752038956 CET	8.8.8.8	192.168.2.6	0x1df9	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.752038956 CET	8.8.8.8	192.168.2.6	0x1df9	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.752038956 CET	8.8.8.8	192.168.2.6	0x1df9	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.796346903 CET	8.8.8.8	192.168.2.6	0x6660	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:46.796346903 CET	8.8.8.8	192.168.2.6	0x6660	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.796346903 CET	8.8.8.8	192.168.2.6	0x6660	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.796346903 CET	8.8.8.8	192.168.2.6	0x6660	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:46.796346903 CET	8.8.8.8	192.168.2.6	0x6660	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:10.964626074 CET	8.8.8.8	192.168.2.6	0x1930	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:52:10.964626074 CET	8.8.8.8	192.168.2.6	0x1930	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:11.434695959 CET	8.8.8.8	192.168.2.6	0xd825	No error (0)	mail.strictfacilityservices.com	strictfacilityservices.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:52:11.434695959 CET	8.8.8.8	192.168.2.6	0xd825	No error (0)	strictfacilityservices.com		111.118.212.38	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org

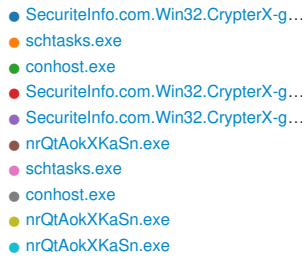
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 16:51:21.977685928 CET	587	49717	111.118.212.38	192.168.2.6	220-bh-in-36.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 15:51:21 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 16:51:21.978070021 CET	49717	587	192.168.2.6	111.118.212.38	EHLO 302494

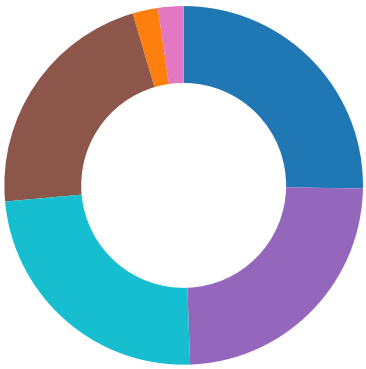
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 16:51:22.252252102 CET	587	49717	111.118.212.38	192.168.2.6	250-bh-in-36.webhostbox.net Hello 302494 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 16:51:22.253521919 CET	49717	587	192.168.2.6	111.118.212.38	AUTH login YWNjb3VudHNAc3RyaWN0ZmFjaWxpdHlzZXJ2aWNlcy5jb20=
Nov 29, 2022 16:51:22.526686907 CET	587	49717	111.118.212.38	192.168.2.6	334 UGFzc3dvcmQ6
Nov 29, 2022 16:51:23.584398985 CET	587	49717	111.118.212.38	192.168.2.6	235 Authentication succeeded
Nov 29, 2022 16:51:23.585345030 CET	49717	587	192.168.2.6	111.118.212.38	MAIL FROM:<accounts@strictfacilityservices.com>
Nov 29, 2022 16:51:23.860614061 CET	587	49717	111.118.212.38	192.168.2.6	250 OK
Nov 29, 2022 16:51:23.860863924 CET	49717	587	192.168.2.6	111.118.212.38	RCPT TO:<guc850155@gmail.com>
Nov 29, 2022 16:51:24.168071032 CET	587	49717	111.118.212.38	192.168.2.6	250 Accepted
Nov 29, 2022 16:51:24.169872999 CET	49717	587	192.168.2.6	111.118.212.38	DATA
Nov 29, 2022 16:51:24.443375111 CET	587	49717	111.118.212.38	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 16:51:24.450061083 CET	49717	587	192.168.2.6	111.118.212.38	.
Nov 29, 2022 16:51:24.724167109 CET	587	49717	111.118.212.38	192.168.2.6	250 OK id=1p02tl-0007mJ-Bj
Nov 29, 2022 16:52:14.190653086 CET	587	49722	111.118.212.38	192.168.2.6	220-bh-in-36.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 15:52:14 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 16:52:14.194787025 CET	49722	587	192.168.2.6	111.118.212.38	EHLO 302494
Nov 29, 2022 16:52:14.473042011 CET	587	49722	111.118.212.38	192.168.2.6	250-bh-in-36.webhostbox.net Hello 302494 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 16:52:14.499712944 CET	49722	587	192.168.2.6	111.118.212.38	AUTH login YWNjb3VudHNAc3RyaWN0ZmFjaWxpdHlzZXJ2aWNlcy5jb20=
Nov 29, 2022 16:52:14.778090954 CET	587	49722	111.118.212.38	192.168.2.6	334 UGFzc3dvcmQ6
Nov 29, 2022 16:52:17.294580936 CET	587	49722	111.118.212.38	192.168.2.6	235 Authentication succeeded
Nov 29, 2022 16:52:17.297631979 CET	49722	587	192.168.2.6	111.118.212.38	MAIL FROM:<accounts@strictfacilityservices.com>
Nov 29, 2022 16:52:17.575813055 CET	587	49722	111.118.212.38	192.168.2.6	250 OK
Nov 29, 2022 16:52:17.576160908 CET	49722	587	192.168.2.6	111.118.212.38	RCPT TO:<guc850155@gmail.com>
Nov 29, 2022 16:52:17.900510073 CET	587	49722	111.118.212.38	192.168.2.6	250 Accepted
Nov 29, 2022 16:52:17.901293039 CET	49722	587	192.168.2.6	111.118.212.38	DATA
Nov 29, 2022 16:52:18.179738045 CET	587	49722	111.118.212.38	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 16:52:18.188690901 CET	49722	587	192.168.2.6	111.118.212.38	.
Nov 29, 2022 16:52:18.467991114 CET	587	49722	111.118.212.38	192.168.2.6	250 OK id=1p02uA-00087S-33

Statistics

Behavior



Copyright Joe Security LLC 2022



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe PID: 4580, Parent PID: 3452

General

Target ID:	0
Start time:	16:50:18
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Imagebase:	0x690000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
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: 00000000.00000002.325021706.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.325021706.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.325021706.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C461E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp152E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp152E.tmp	success or wait	1	6C466A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe	0	847360	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1f fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 50 00 00 fd 0c 00 00 08 00 00 00 00 00 fd 02 0d 00 00 20 00 00 00 20 0d 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 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELcP @ `@	success or wait	1	6C461B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp152E.tmp	0	1657	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </Registratio	success or wait	1	6C461B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe.log	0	1216	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	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe	unknown	847360	success or wait	1	6C461B4F	ReadFile

Analysis Process: schtasks.exe PID: **5756**, Parent PID: **4580**

General

Target ID:	8
Start time:	16:50:43
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nrQtAokXKaSn" /XML "C:\Users\user\AppData\Local\Temp\tmp152E.tmp
Imagebase:	0x210000
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp152E.tmp	unknown	2	success or wait	1	21AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp152E.tmp	unknown	1658	success or wait	1	21ABD9	ReadFile

Analysis Process: conhost.exe PID: **5452**, Parent PID: **5756**

General

Target ID:	9
Start time:	16:50:44
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe PID: **5688**, Parent PID: **4580**

General

Target ID:	10
Start time:	16:50:44
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x370000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe PID: **5900**, Parent PID: **4580**

General

Target ID:	11
Start time:	16:50:44
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.16043.3621.exe
Wow64 process (32bit):	true
Commandline:	{path}

Copyright Joe Security LLC 2022

Imagebase:	0x870000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
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: 0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000B.00000000.315331976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.532293061.0000000002CF4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.531415625.0000000002CA1000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpEBF5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ac5dbcd4-51c1-4ab3-b1a6-0f60d34ce758	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C461B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: nrQtAokXKaSn.exe PID: **5976**, Parent PID: **1064**

General

Target ID:	12
Start time:	16:50:45
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
Imagebase:	0x5c0000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, 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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nrQtAokXKaSn.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp	success or wait	1	6C466A95	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\Local\Temp\tmpCC0B.tmp	0	1657	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </Registratio	success or wait	1	6C461B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nrQtAokXKaSn.exe.log	0	1216	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	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile

Analysis Process: schtasks.exe PID: **1372**, Parent PID: **5976**

General

Target ID:	13
Start time:	16:51:31
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nrQtAokXKaSn" /XML "C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp
Imagebase:	0x210000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp	unknown	2	success or wait	1	21AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCC0B.tmp	unknown	1658	success or wait	1	21ABD9	ReadFile

Analysis Process: conhost.exe PID: **3408**, Parent PID: **1372**

General

Target ID:	14
Start time:	16:51:31
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nrQtAokXKaSn.exe PID: **2744**, Parent PID: **5976**

General

Target ID:	15
Start time:	16:51:32
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
Wow64 process (32bit):	false

Commandline:	{path}
Imagebase:	0x2e0000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: nrQtAokXKaSn.exe PID: **1008**, Parent PID: **5976**

General

Target ID:	16
Start time:	16:51:33
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\nrQtAokXKaSn.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x460000
File size:	847360 bytes
MD5 hash:	FE1AA7FA995970EBB34465D5DC0D8CE1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.533369231.00000000028E4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.532462363.0000000002891000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpC4F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile

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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ac5dbcd4-51c1-4ab3-b1a6-0f60d34ce758	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C461B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly