ID: 756187
Sample Name: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Cookbook: default.jbs
Time: 19:32:18
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

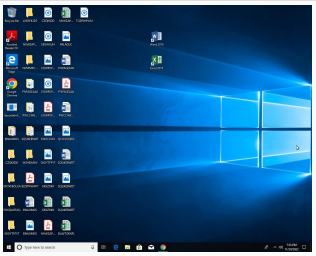
Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe

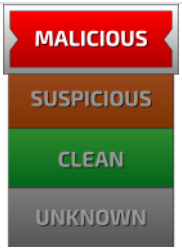
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Analysis ID:	756187
MD5:	2364501a86685f..
SHA1:	ebacf33c1e9f530..
SHA256:	74a3379894a1b9.
Tags:	exe
Infos:	



Detection



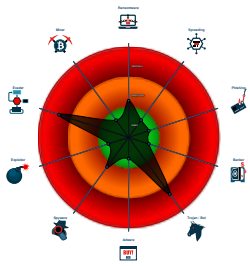
FormBook

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe (PID: 2804 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe MD5: 2364501A86685F9A53D37D339549CEE5)
  - SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe (PID: 5964 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe MD5: 2364501A86685F9A53D37D339549CEE5)
  - SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe (PID: 5948 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe MD5: 2364501A86685F9A53D37D339549CEE5)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.imperiumtowns.xyz/b3es/"
  ],
  "decoy": [
    "sweets.wtf",
    "apextama.com",
    "tygbs.com",
    "kumaoedu.com",
    "bestbathroomremodeling.club",
    "lnshykj.com",
    "nelsonanddima.com",
    "falunap.info",
    "codyhinrichs.com",
    "2797vip.com",
    "danutka.com",
    "3o2t307a.com",
    "kellymariewest.com",
    "profilelonn.online",
    "procan.website",
    "sopjimmy.com",
    "xn--skdarkae-55ac80i.net",
    "entitymanaged.com",
    "melitadahl.art",
    "joineguru.net",
    "good-meme.com",
    "creditconepts.com",
    "narafconstruction.com",
    "paspsichologa.com",
    "rancho365.com",
    "rimplefeel.com",
    "kingsub.online",
    "cnsrdns.com",
    "billythepainter.com",
    "clientevirtualpdf.net",
    "marycruzruiz.com",
    "renaultcikmaparca.xyz",
    "1600156.com",
    "paymallmart.info",
    "garafe.com",
    "fredrikk.net",
    "gogo-tunisia.space",
    "center-me.com",
    "xiaohuayhq.com",
    "xn--h49a60xt7azzcm91a.com",
    "unidiliobobo.info",
    "libertypolestore.com",
    "20111210.net",
    "atraofix.online",
    "furniron.com",
    "mingyun58.com",
    "shfesmua.com",
    "rdougdigital.life",
    "safsip.com",
    "melon.town",
    "sagihigaibengo.net",
    "ethnicsbyak.com",
    "designoffaitheventsllc.com",
    "dpmforensics.com",
    "ripple-us.net",
    "fuyouhin-happiness.com",
    "conceptweb.online",
    "l453.net",
    "zenars.com",
    "mepcoonlinebill.com",
    "oonn99.xyz",
    "dackus.energy",
    "articvas.com",
    "yayuanlin.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.258835814.00000000024C6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.256915328.00000000023B1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bb90:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x99cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x959a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bd90:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.0.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1aaf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bafa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a19:$sqlite3step: 68 34 1C 7B E1 • 0x17b2c:$sqlite3step: 68 34 1C 7B E1 • 0x17a48:$sqlite3text: 68 38 2A 90 C5 • 0x17b6d:$sqlite3text: 68 38 2A 90 C5 • 0x17a5b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b83:$sqlite3blob: 68 53 D8 7F 8C
0.2.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.3706fe0.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 11 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

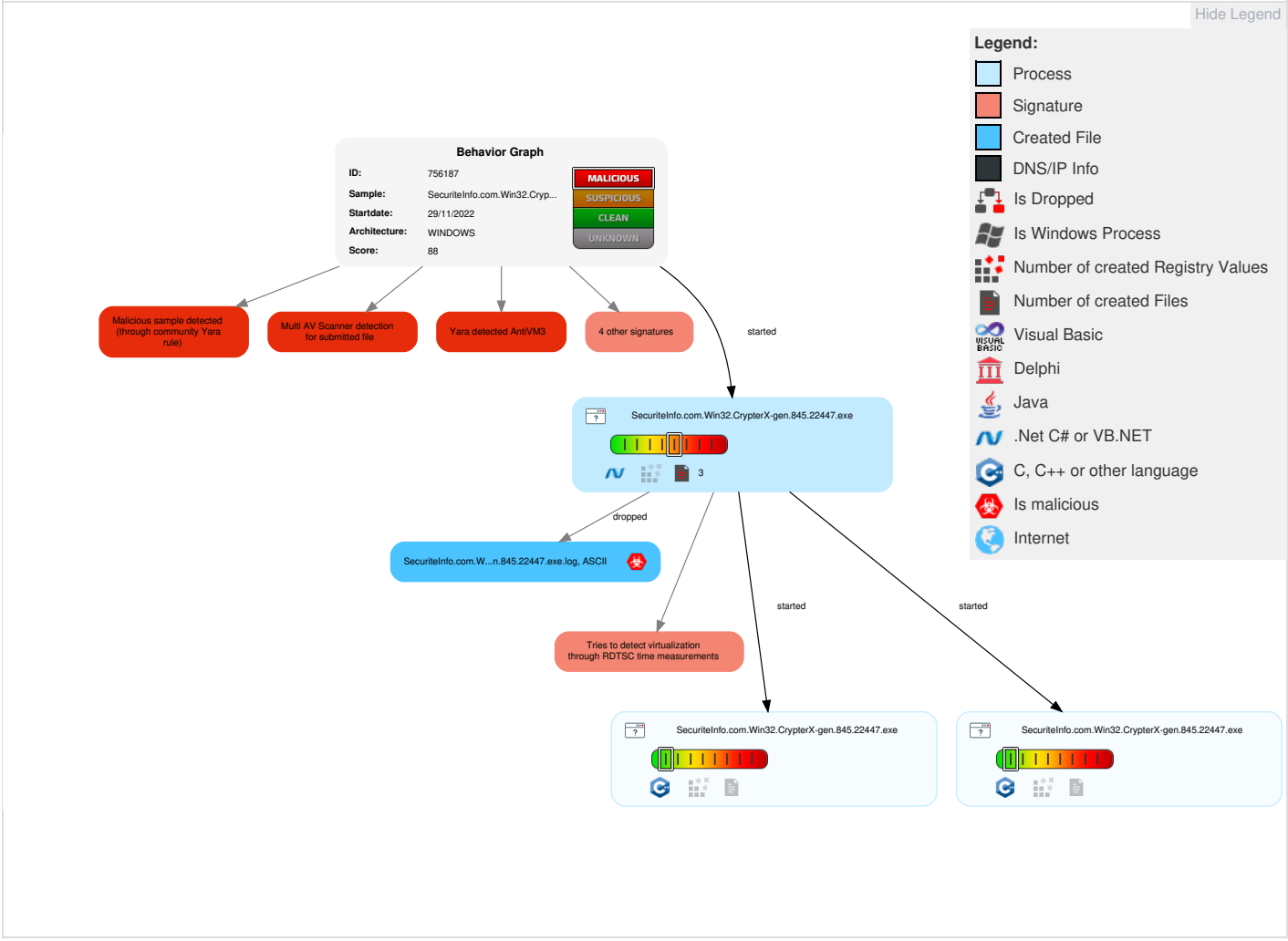
Yara detected FormBook

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 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

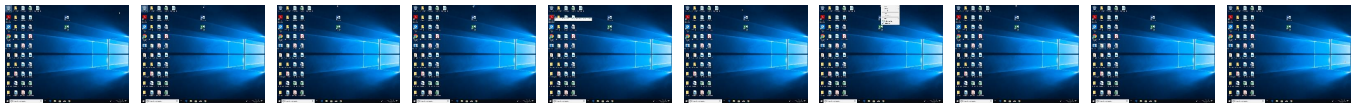
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

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://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcoma	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.fontbureau.comlvfetPx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comyux	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comessedBx	0%	Avira URL Cloud	safe	
http://en.wikip	0%	URL Reputation	safe	
http://www.fontbureau.comFPx	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comOx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/Kx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/nt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(x	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/6x	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdKx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Ox	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/gx	0%	Avira URL Cloud	safe	
www.imperiumtowns.xyz/b3es/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ux	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/T	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFgx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Px	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/os	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.imperiumtowns.xyz/b3es/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/Kx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comlvfetPx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240670623.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240603222.00000000053B4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Ox	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comyux	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241550871.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240742786.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241336054.00000000053BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.238183730.00000000053DE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ux	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.235284225.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242734447.00000000053B8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242880246.00000000053B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.254193387.00000000053B6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/gx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessedBx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240742786.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdKx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241550871.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFPx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241314930.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241336054.00000000053BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/6x	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241550871.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925765.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242944051.00000000053B8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242734447.00000000053B8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242880246.00000000053B8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.243359577.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.243191419.00000000053B7000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.243076980.00000000053B7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240670623.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcoma	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241550871.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241314930.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241336054.00000000053BA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(x	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239615103.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239638756.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239744541.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239686574.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239850577.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239808719.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239830507.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239706031.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.c	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.237766559.00000000053A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/nt	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.236833345.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comOx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240742786.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240670623.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240603222.00000000053B4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241146831.00000000053B6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/T	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.237783564.00000000053AE000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.237951551.00000000053AE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wikip	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.237103546.00000000053AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/os	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239615103.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239638756.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239686574.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Px	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.237766559.00000000053A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comFgx	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242284956.00000000053B6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comoitu	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240742786.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240670623.00000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.242595921.00000000053A5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.254193387.00000000053B6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239615103.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239980903.00000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239638756.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240051220.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239744541.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240088210.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239686574.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239850577.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239918940.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240133807.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239447034.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239808719.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239830507.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239944814.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239899581.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.239706031.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240110528.00000000053BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.240166526.00000000053BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000002.275925764.00000000065B2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comals	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241550871.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241616644.00000000053BA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe, 00000000.00000003.241336054.00000000053BA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756187
Start date and time:	2022-11-29 19:32:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.845.22447.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:	8
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:	mal88.troj.evad.winEXE@5/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 90%) • Quality average: 74.6% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- VT rate limit hit for: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe

Simulations

Behavior and APIs

Time	Type	Description
19:33:18	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.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.845.22447.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.643627342935855

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.845.22447.exe
File size:	926208
MD5:	2364501a86685f9a53d37d339549cee5
SHA1:	ebacf33c1e9f53048a8e808429671ed489dc285d
SHA256:	74a3379894a1b92cb381a128c7fe7c5f97e1a12df02588ec816d1a4fc5dc0a25
SHA512:	1210b67603986cfa62d6ac7df1ac3da1aeb03d80716f605465967e8895ec9fd39106918b5de5f865b7ce937cc2f111849b88450b517201cc6ea4b2af269e819d
SSDEEP:	12288:8SYqU+RPN8z0WC9ZG5MyVh+rpDhl6loeY7XccEKjxN4qwkqpUKPPDdzoa1cfN:/JKzOZl56lE7McE6xN44ZKPPDdEPf
TLSH:	FA15D0803366AF75F5686BF37521814827B63C6E95F1C2285ECDB0DE2A72B5049F0B27
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f..c.....0.....9... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e39c2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385D466 [Tue Nov 29 09:44:06 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe3970	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
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	0xe19c8	0xe1a00	False	0.8235933171745152	data	7.650390698554388	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x388	0x400	False	0.3701171875	data	2.8531167057982127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe6000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe4058	0x32c	data		

Imports

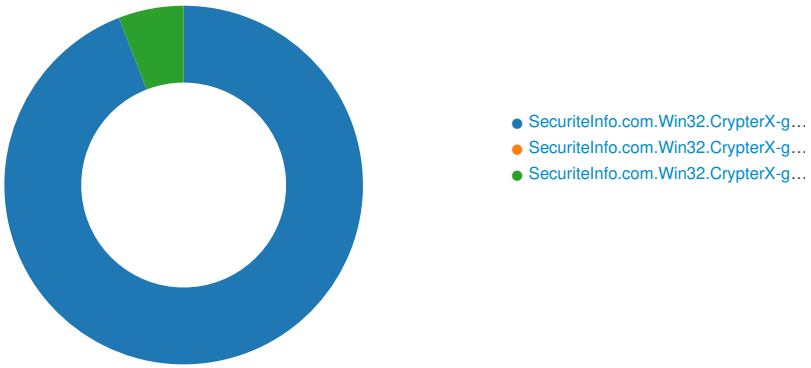
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe PID: 2804, Parent PID: 3320

General	
Target ID:	0
Start time:	19:33:11
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Imagebase:	0x80000
File size:	926208 bytes
MD5 hash:	2364501A86685F9A53D37D339549CEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.258835814.00000000024C6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.256915328.00000000023B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.266786451.000000000364F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.266786451.000000000364F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.266786451.000000000364F000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.266786451.000000000364F000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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	6D5DCF06	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	6D5DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.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	6D8EC907	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	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C421B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C421B4F	ReadFile

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe PID: **5964**, Parent PID: **2804**

General

Target ID:	1
Start time:	19:33:20
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Imagebase:	0x2b0000
File size:	926208 bytes
MD5 hash:	2364501A86685F9A53D37D339549CEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe PID: **5948**, Parent PID: **2804**

General

Target ID:	2
Start time:	19:33:20
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.845.22447.exe
Imagebase:	0x490000
File size:	926208 bytes
MD5 hash:	2364501A86685F9A53D37D339549CEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.252621166.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A427	NtReadFile

Disassembly

No disassembly