ID: 756011
Sample Name: SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Cookbook: default.jbs
Time: 13:52:42
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

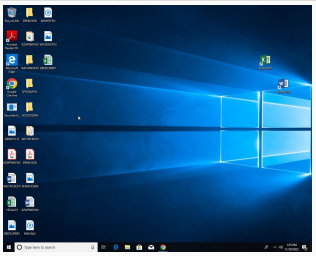
Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe

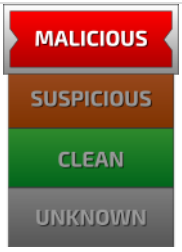
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Analysis ID:	756011
MD5:	277a9cd8ef3618..
SHA1:	9b703e61330779.
SHA256:	8cdfbe67b60922..
Tags:	exe
Infos:	



Detection



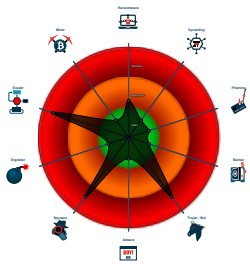
AgentTesla

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
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe (PID: 4356 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe MD5: 277A9CD8EF361888EB41A6B7D0D94E26)
  - SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe (PID: 4596 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe MD5: 277A9CD8EF361888EB41A6B7D0D94E26)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail2.bpk-spb.ru",
  "Username": "grafkina.gg@sasta.ru",
  "Password": "SGZ3574344"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.342203286.0000000002B7B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.340639694.0000000002871000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31cfe:$a13: get_DnsResolver • 0x303f3:$a20: get_LastAccessed • 0x3272c:$a27: set_InternalServerPort • 0x32a61:$a30: set_GuidMasterKey • 0x30505:$a33: get_Clipboard • 0x30513:$a34: get_Keyboard • 0x318f8:$a35: get_ShiftKeyDown • 0x31909:$a36: get_AltKeyDown • 0x30520:$a37: get_Password • 0x31053:$a38: get_PasswordHash • 0x32160:$a39: get_DefaultCredentials
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.28b0724.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.28b0724.2.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0xd16e:$v1: SbieDll.dll • 0xd188:$v2: USER • 0xd194:$v3: SANDBOX • 0xd1a6:$v4: VIRUS • 0xd1f6:$v4: VIRUS • 0xd1b4:$v5: MALWARE • 0xd1c6:$v6: SCHMIDTI • 0xd1da:$v7: CURRENTUSER
1.0.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.0.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x34a40:$s10: logins • 0x344ba:$s11: credential • 0x30705:$g1: get_Clipboard • 0x30713:$g2: get_Keyboard • 0x30720:$g3: get_Password • 0x31ae8:$g4: get_CtrlKeyDown • 0x31af8:$g5: get_ShiftKeyDown • 0x31b09:$g6: get_AltKeyDown
Click to see the 21 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

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

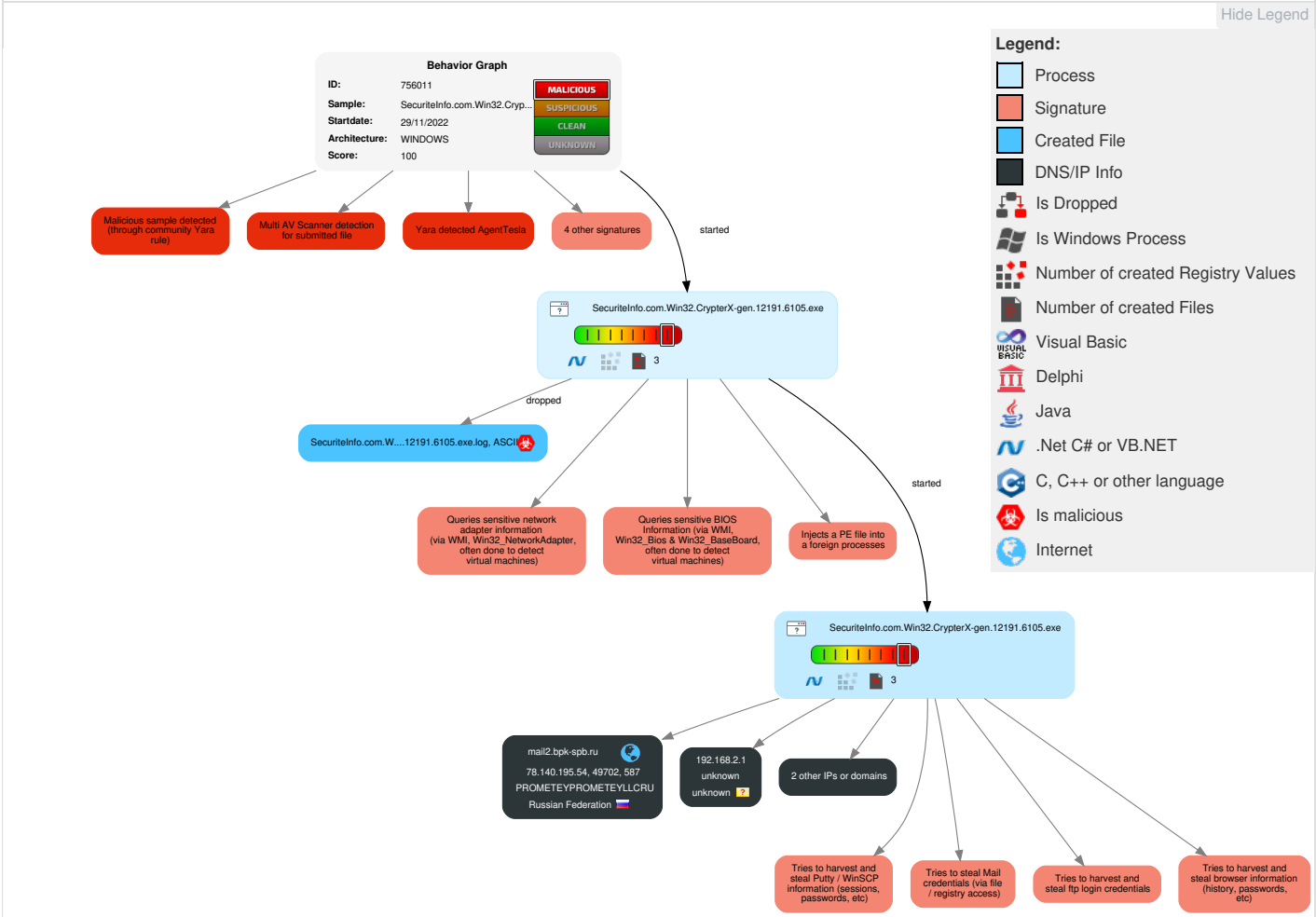
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window 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	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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	1 1 4 System Information Discovery	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.12191.6105.exe	34%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe	28%	Virustotal		Browse
SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
c-0001.c-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/ocsp0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://microsoft.coC?	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://fhESbX.com	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/DPCyPoliticas0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://ocsp.ncdc.gov.sa0	0%	URL Reputation	safe	
http://mail2.bpk-spb.ru	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://www.tiro.coma-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false	• 0%, Virustotal, Browse	unknown
mail2.bpk-spb.ru	78.140.195.54	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.573661423.0000000003061000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383888553.0000000006BFC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.000000006E12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-me.lv/repository0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384119215.0000000006BE4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.swisssign.com/0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384119215.0000000006BE4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579642195.0000000006BBD000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384190628.0000000006BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.suscerte.gob.ve/dpc0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384119215.0000000006BE4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fhESbX.com	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.573661423.0000000003061000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579642195.0000000006BBD000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384190628.0000000006BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sk.ee/cps/0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0=	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579679447.0000000006BDF000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://microsoft.coC?	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.580423251.0000000006E91000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.registradores.org/normativa/index.htm0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.root-x1.letsencrypt.org0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.572908994.000000001 4BE000.00000004.00000020.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000002.576650294.0 0000000033DE000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://policy.camerfirma.com0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006 BC6000.00000004.00000800.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000003.384130770.0 000000006BA7000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ssc.lt/cps03	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006 E85000.00000004.00000800.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000003.384041947.0 000000006BC6000.00000004.00000800.000200 00.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.38 3812134.0000000006BDB000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006 B8E000.00000004.00000800.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000003.384238128.0 000000006B7B000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006 BC6000.00000004.00000800.00020000.000000 00.sdmp	false		high
http://https://www.anf.es/address/)1(0&	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384553962.0000000006 E20000.00000004.00000800.00020000.000000 00.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006 B8E000.00000004.00000800.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000003.384238128.0 000000006B7B000.00000004.00000800.000200 00.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.38 4130770.0000000006BA7000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.coma-e	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000003.309946235.0000000000 ECC000.00000004.00000020.00020000.000000 00.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006 BC6000.00000004.00000800.00020000.000000 00.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.385128719.0000000001 504000.00000004.00000020.00020000.000000 00.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191 .6105.exe, 00000001.00000002.573185738.0 00000000150C000.00000004.00000020.000200 00.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.57 2908994.00000000014BE000.00000004.000000 20.00020000.00000000.sdmp, SecuriteInfo. com.Win32.CrypterX-gen.12191.6105.exe, 0 0000001.00000002.576650294.00000000033DE 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006 BDB000.00000004.00000800.00020000.000000 00.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006 BA7000.00000004.00000800.00020000.000000 00.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384553962.0000000006 E20000.00000004.00000800.00020000.000000 00.sdmp	false		high

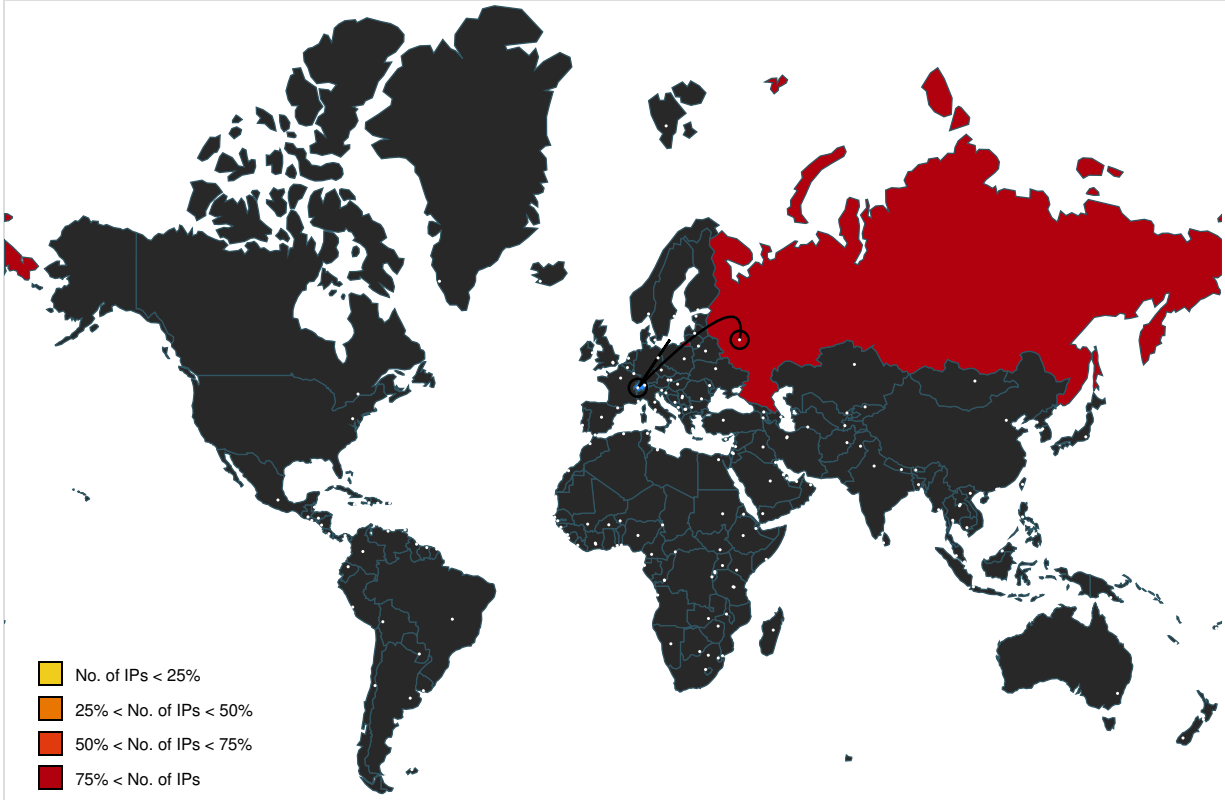
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • 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.12191.6105.exe, 00000001.00000002.573661423.0000000003061000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail2.bpk-spb.ru	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.576650294.0000000033DE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384553962.0000000006E20000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579679447.0000000006BDF000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384553962.0000000006E20000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.catcert.net/verarrel	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca0f	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579642195.0000000006BBD000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384190628.0000000006BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadis.bm0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383812134.0000000006BDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es00	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pkioverheid.nl/policies/root-policy-G20	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.net/docs	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384504580.0000000006BC5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384190628.0000000006BC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384847493.0000000006E12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384610055.0000000006E04000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384130770.0000000006BA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384432501.0000000006BA5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384041947.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000002.579625475.0000000006BA5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384366166.0000000006B8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.384238128.0000000006B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000000.00000002.345955674.0000000006852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://repository.luxtrust.lu0	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe, 00000001.00000003.383679132.0000000006E85000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.140.195.54	mail2.bpk-spb.ru	Russian Federation		35000	PROMETEYPROMETEYLLCRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756011
Start date and time:	2022-11-29 13:52:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@1/2
EGA Information:	• Successful, ratio: 100%
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, WMIADAP.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 13.107.4.50, 209.197.3.8
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:53:54	API Interceptor	652x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62919
Entropy (8bit):	**7.995280921994772**
Encrypted:	**true**
SSDEEP:	1536:d+OfVxHl7Wyf11lYom3xQcRVOtPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q
MD5:	3DCF580A93972319E82CAFBC047D34D5
SHA1:	8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B
SHA-256:	40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1
SHA-512:	98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....Q.....GU.\ .authroot.stl..O..5..CK..<Tk...c_.d....A.K...+.d.-;%.BJI!.QIR..$t)Kd.-QQ*...g.....^..~|N=...y....{. .4{...W....b.i...j.l.....1:..b\.0.... .Ait.2t.....w.%.&.",tL_...4.8L[G..;.57....AT.k.....V..K.....(....mzS...G....r.".=H.?>.....x&...S%....X.M^..j...A..x.9`.9...A../.s..#.4#.....ld.w..B....s.8..(...dj....=L.)..s.d.]NxQX8 ....stV#.K.'7.tH..9u~.2..!..2./.....!..9C../...mP $..../y.....@p.6.}.`...5. 0r.w...@(.. .Q....)g.....m..z*.8rR..).].T9r<.L....0..`.....c.....;-.g..;.wk.).....i..c5.....{v.u...AS..=.....&.:... .....+..P.N..9..EAQ.V.$s.....B.`.Mfe..8.....$...y-.q9J.....W...2.Q8...O.....i..@\^.=X..dG$.M..#=....m.h..{9.'...-.v..Z...!....z.....N....i..^.,.....d...%Xa~q.@D|0...Y.m..... ...&d.4..A..{t=...../.t.3._.....?-.....uroP?.d.Z..S..{...$.i....X..$.O..4..N.)....U.Z..P....X,.... ...Lg..35..W..s.!c...Ap.].P..8..M..W.....U..,...m.u..|=.m1..~..!..b...._.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1085359935940406
Encrypted:	false
SSDEEP:	6:kKLTEN1HlNiN+SkQlPlEGYRMY9z+4KlDA3RUeKlTAlWRyf1:DTk/kPlE99SNxAhUexYo1
MD5:	B81EE1A8A335587B8E02783E3D400D2D
SHA1:	68C4FAB0E6B9330789ADE1048D8BA46D5DE2C544
SHA-256:	ADCF90B3C43AF8DC7E11AFC46523C7D3EEF91AAB890B27D8C91505C1DBE62B3C
SHA-512:	EFA34C213A89887618E2998A1020AE87DECF11BC4F9AA7A8E3436DCED18E6313AD8D921465AF033CEFFB8383A2B11CFD453C588FAF7D4EB2DDEC460621D1BEA
Malicious:	false
Reputation:	low
Preview:	p..... ....."S.!B...(..... .....&.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.d.e.4.d.3.9.b.e.8.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.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):	7.664770270231839
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.12191.6105.exe
File size:	960000
MD5:	277a9cd8ef361888eb41a6b7d0d94e26
SHA1:	9b703e613307793cd9f0309eb458d5f12f8400dd
SHA256:	8cdfbe67b609226da852adf3db3098941cffda7cea7443b935e1eed5fdae0bf3
SHA512:	fb35b96d3153b13ec2cea3c243114b9e1c8a58ee391c94f44555a2d7c07137702a4230446f616373c0cf139695d3dcf8fcc9a55de778ad2112f6874011dad44d
SSDEEP:	12288:o/x3qU+ai4t0ZiB3s8K4fMP7zs5y8m6Zwjz2boW9zq1krmvkhog/6Fb7wqzwBSDE:mxR0i3s8qDww8m6ZcQq21ht6woDdEPf
TLSH:	FC15DF8023A6AF75F1296BF37421900827B63C5EA5F1D2296DCDF0DE2A71B415AF0B17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ebd9a
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:	0x6385B5DD [Tue Nov 29 07:33:49 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

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
add 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	0xebd48	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xec000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xee000	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	0xe9da0	0xe9e00	False	0.8298025370791021	data	7.671253644478303	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xec000	0x388	0x400	False	0.37109375	data	2.860979956316595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

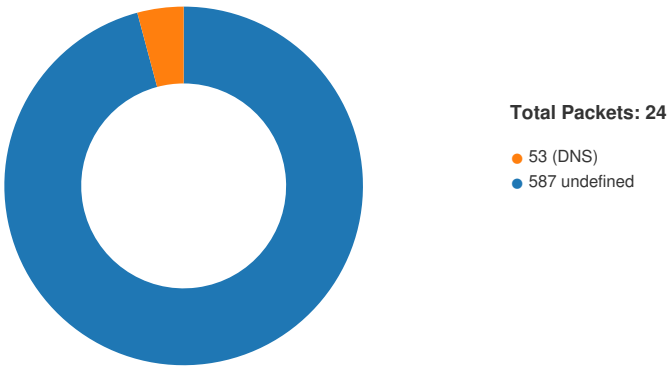
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xec058	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:54:15.805341959 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:15.861587048 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:15.861691952 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:15.996521950 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:15.996942043 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.049736023 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.053610086 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.094831944 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.097780943 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.157645941 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.161354065 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.204152107 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.760996103 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.815157890 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.815237999 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.815262079 CET	587	49702	78.140.195.54	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:54:16.815372944 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.815437078 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.815469027 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.815517902 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.867993116 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:16.928946018 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.933392048 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:16.994105101 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:17.048006058 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.626239061 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.682285070 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.684568882 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.747383118 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.748119116 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.817748070 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.818945885 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.877036095 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.877501965 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.938349009 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.938827991 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.992013931 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:21.995357990 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.995471001 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.995975018 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:21.996053934 CET	49702	587	192.168.2.5	78.140.195.54
Nov 29, 2022 13:54:22.061959982 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:22.061983109 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:22.679898024 CET	587	49702	78.140.195.54	192.168.2.5
Nov 29, 2022 13:54:22.720345974 CET	49702	587	192.168.2.5	78.140.195.54

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:54:15.704055071 CET	51441	53	192.168.2.5	8.8.8.8
Nov 29, 2022 13:54:15.779623985 CET	53	51441	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 13:54:15.704055071 CET	192.168.2.5	8.8.8.8	0x57e7	Standard query (0)	mail2.bpk-spb.ru	A (IP address)	IN (0x0001)	false

DNS Answers

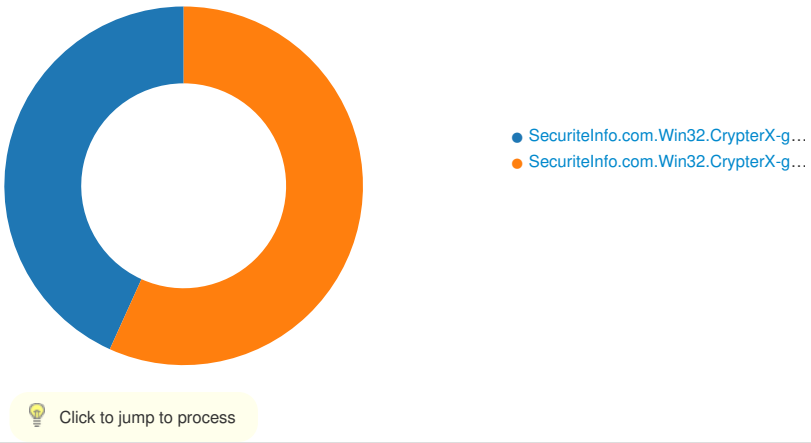
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 13:54:15.779623985 CET	8.8.8.8	192.168.2.5	0x57e7	No error (0)	mail2.bpk-spb.ru		78.140.195.54	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:54:15.779623985 CET	8.8.8.8	192.168.2.5	0x57e7	No error (0)	mail2.bpk-spb.ru		217.119.27.174	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:54:19.506061077 CET	8.8.8.8	192.168.2.5	0x7664	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 13:54:19.506061077 CET	8.8.8.8	192.168.2.5	0x7664	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:54:34.261774063 CET	8.8.8.8	192.168.2.5	0x2e9b	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 13:54:34.261774063 CET	8.8.8.8	192.168.2.5	0x2e9b	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 13:54:15.996521950 CET	587	49702	78.140.195.54	192.168.2.5	220 mail2.bpk-spb.ru ESMTP Postfix
Nov 29, 2022 13:54:15.996942043 CET	49702	587	192.168.2.5	78.140.195.54	EHLO 019635
Nov 29, 2022 13:54:16.053610086 CET	587	49702	78.140.195.54	192.168.2.5	250-mail2.bpk-spb.ru 250-PIPELINING 250-SIZE 36214400 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING
Nov 29, 2022 13:54:16.097780943 CET	49702	587	192.168.2.5	78.140.195.54	STARTTLS
Nov 29, 2022 13:54:16.161354065 CET	587	49702	78.140.195.54	192.168.2.5	220 2.0.0 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe PID: **4356**, Parent PID: **3324**

General

Target ID:	0
Start time:	13:53:42
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Imagebase:	0x370000
File size:	960000 bytes
MD5 hash:	277A9CD8EF361888EB41A6B7D0D94E26
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: 00000000.00000002.342203286.0000000002B7B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.340639694.0000000002871000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.343455182.0000000003AD8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.343455182.0000000003AD8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.343455182.0000000003AD8000.00000004.00000800.00020000.00000000.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	6C9BCF06	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	6C9BCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCCC78D	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.12191.6105.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 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	6CCCC907	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	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C995705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C8F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C99CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C8F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C8F03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C8F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C8F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B801B4F	ReadFile

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe PID: **4596**, Parent PID: **4356**

General

Target ID:	1
Start time:	13:53:56
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12191.6105.exe
Imagebase:	0xc70000
File size:	960000 bytes
MD5 hash:	277A9CD8EF361888EB41A6B7D0D94E26
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: 00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.332476278.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.573661423.0000000003061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.573661423.0000000003061000.00000004.00000800.00020000.00000000.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	6C9BCF06	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	6C9BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2CA3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B807038	GetTempFileNameW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C995705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C8F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C99CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C8F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C8F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C8F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C8F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C995705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B801B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6B801B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6B801B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	6B801B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6B801B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6B801B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6B801B4F	ReadFile

Disassembly

No disassembly