

JoeSandbox Cloud BASIC



ID: 756003

Sample Name:

SecuriteInfo.com.Win32.CrypterX-
gen.12778.11165.exe

Cookbook: default.jbs

Time: 13:49:14

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.12778.11165.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Telegram RAT	4
Threatname: Agenttesla	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Persistence and Installation Behavior	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
Key, Mouse, Clipboard, Microphone and Screen Capturing	6
System Summary	6
Boot Survival	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
Public IPs	12
Private	12
General Information	13
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
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.12778.11165.exe.log	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UmpBcHBDbXhaX.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_2sdibjn1.iex.ps1	15
C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_j1bp3fok.q3g.psm1	15
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	15
C:\Users\user\AppData\Local\Temp\tmp8847.tmp	16
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe	16
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe.Zone.Identifier	16
Static File Info	17
General	17
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	18
Data Directories	19
Sections	20

Resources	20
Imports	20
Network Behavior	20
Statistics	20
Behavior	20
System Behavior	20
Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exePID: 5644, Parent PID: 3528	21
General	21
File Activities	21
File Created	21
File Deleted	21
File Written	21
File Read	23
Analysis Process: powershell.exePID: 3216, Parent PID: 5644	23
General	23
File Activities	24
File Created	24
File Deleted	24
File Written	24
File Read	25
Analysis Process: conhost.exePID: 5284, Parent PID: 3216	29
General	29
Analysis Process: schtasks.exePID: 3644, Parent PID: 5644	29
General	29
File Activities	29
File Read	29
Analysis Process: conhost.exePID: 5484, Parent PID: 3644	29
General	29
Analysis Process: UmpBcHBDbXhaX.exePID: 624, Parent PID: 1088	30
General	30
File Activities	30
File Created	30
File Deleted	30
File Written	30
File Read	31
Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exePID: 5340, Parent PID: 5644	32
General	32
File Activities	32
File Created	32
File Read	32
Analysis Process: schtasks.exePID: 3540, Parent PID: 624	33
General	33
File Activities	33
File Read	33
Analysis Process: conhost.exePID: 1348, Parent PID: 3540	33
General	33
Analysis Process: UmpBcHBDbXhaX.exePID: 5468, Parent PID: 624	33
General	33
File Activities	34
File Created	34
File Read	34
Disassembly	34

Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe

Overview

General Information

Sample Name:

SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe

Analysis ID:

756003

MD5:

f64f729e0ba974c...

SHA1:

d1225322fd5f16e...

SHA256:

680f16527c5dc7...

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...

Icon mismatch, binary includes an i...

Malicious sample detected (through...

Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected AntiVM3

Sigma detected: Scheduled temp fil...

Multi AV Scanner detection for drop...

Installs a global keyboard hook

Tries to steal Mail credentials (via fi...

Tries to detect sandboxes and other...

Machine Learning detection for sam...

Classification

Process Tree

System is w10x64

SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe (PID: 5644 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe MD5: F64F729E0BA974C578AFAAC25665E067)

powershell.exe (PID: 3216 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10")

conhost.exe (PID: 5284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

schtasks.exe (PID: 3644 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UmpBcHBDbXhaX" /XML "C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe (PID: 5484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe (PID: 5340 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe MD5: F64F729E0BA974C578AFAAC25665E067)

UmpBcHBDbXhaX.exe (PID: 624 cmdline: C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe MD5: F64F729E0BA974C578AFAAC25665E067)

schtasks.exe (PID: 3540 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UmpBcHBDbXhaX" /XML "C:\Users\user\AppData\Local\Temp\tmp8847.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe (PID: 1348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

UmpBcHBDbXhaX.exe (PID: 5468 cmdline: C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe MD5: F64F729E0BA974C578AFAAC25665E067)

cleanup

Malware Configuration

Threatname: Telegram RAT

{

"C2_url": "https://api.telegram.org/bot5796842243:AAESM2w0ubqts6zEsE_xN4PZ56pLfxQ9e7M/sendMessage"

}

Threatname: Agenttesla

{

"Exfil Mode": "Telegram",

"Telegram Url": "https://api.telegram.org/bot5796842243:AAESM2w0ubqts6zEsE_xN4PZ56pLfxQ9e7M/sendMessage?chat_id=5733364805"

}

Copyright Joe Security LLC 2022

Page 4 of 34

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.363415114.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.363415114.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.363415114.0000000000402000.0000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x31883:\$a13: get_DnsResolver 0x2ff53:\$a20: get_LastAccessed 0x322b1:\$a27: set_InternalServerPort 0x325e6:\$a30: set_GuidMasterKey 0x30065:\$a33: get_Clipboard 0x30073:\$a34: get_Keyboard 0x3147d:\$a35: get_ShiftKeyDown 0x3148e:\$a36: get_AltKeyDown 0x30080:\$a37: get_Password 0x30bd8:\$a38: get_PasswordHash 0x31ce5:\$a39: get_DefaultCredentials
0000000A.00000002.592547674.0000000002AF8000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.592981435.0000000002BF8000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.3f41100.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.3f41100.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.3f41100.7.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x327c4:\$s10: logins 0x3223e:\$s11: credential 0x2e465:\$g1: get_Clipboard 0x2e473:\$g2: get_Keyboard 0x2e480:\$g3: get_Password 0x2f86d:\$g4: get_CtrlKeyDown 0x2f87d:\$g5: get_ShiftKeyDown 0x2f88e:\$g6: get_AltKeyDown
0.2.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.3f41100.7.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x2fc83:\$a13: get_DnsResolver 0x2e353:\$a20: get_LastAccessed 0x306b1:\$a27: set_InternalServerPort 0x309e6:\$a30: set_GuidMasterKey 0x2e465:\$a33: get_Clipboard 0x2e473:\$a34: get_Keyboard 0x2f87d:\$a35: get_ShiftKeyDown 0x2f88e:\$a36: get_AltKeyDown 0x2e480:\$a37: get_Password 0x2efd8:\$a38: get_PasswordHash 0x300e5:\$a39: get_DefaultCredentials
6.0.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 24 entries

Sigma Signatures

Persistence and Installation Behavior



Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

 No Snort rule has matched

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

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



Icon mismatch, binary includes an icon from a different legit application in order to fool users

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



Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information



Yara detected Telegram RAT

Yara detected AgentTesla

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

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

Remote Access Functionality



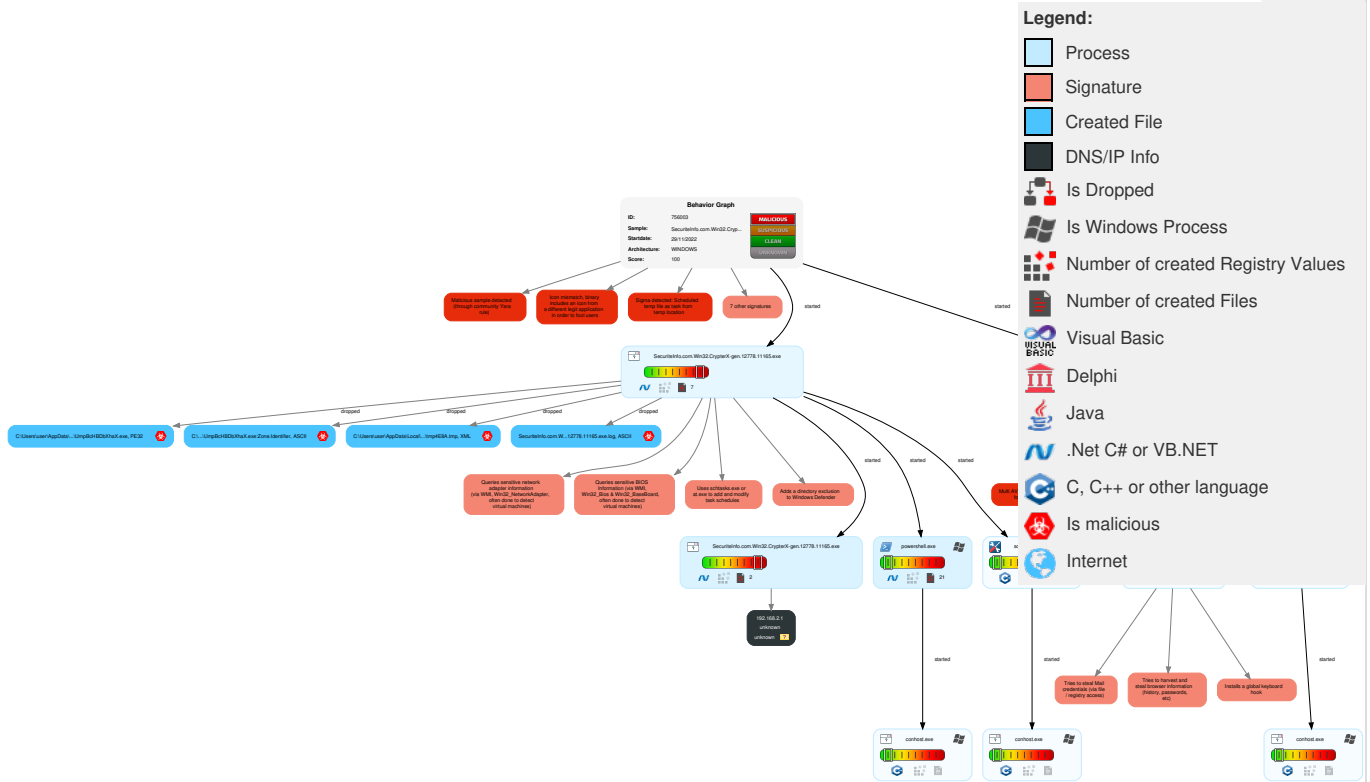
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 Process Injection	1 1 Masquerading	1 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 Scheduled Task/Job	1 1 Disable or Modify Tools	1 1 1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 1 1 Input Capture	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscate Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

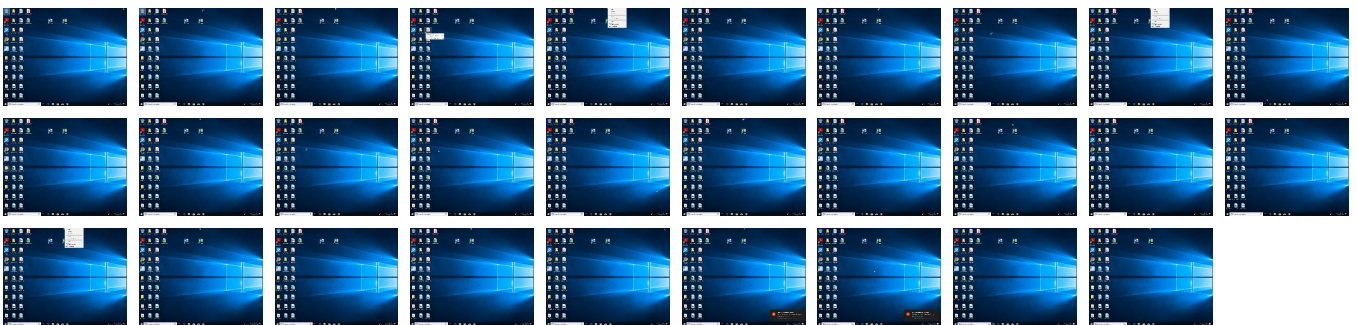
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe	32%	ReversingLabs	Win32.Trojan.Woreflint	
SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

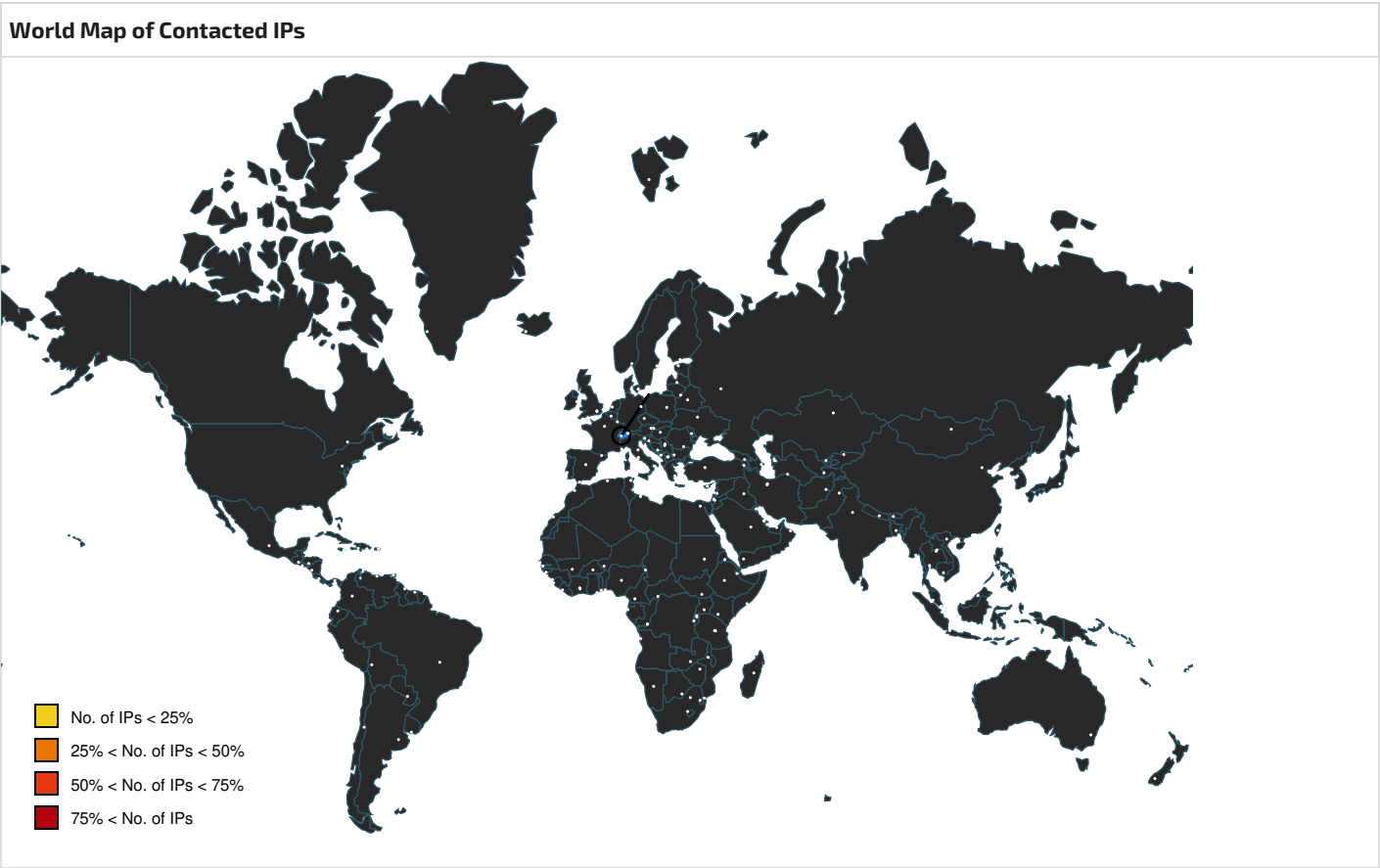
URLs				
Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	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://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://SDRcFr.com	0%	Avira URL Cloud	safe	

Domains and IPs
Contacted Domains
 No contacted domains info

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000006.00000002.592124173.0000000002B51000.00000004.00000800.00020000.00000000.sdm, UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdm	false	Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.fontbureau.comF	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.366428290.0000000001207000.00000004.00000020.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://https://api.telegram.org/bot5796842243:AAESM2w0ubqts6zEsE_xN4PZ56pLfxQ9e7M/	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000006.00000002.592124173.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.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.12778.11165.exe, 00000006.00000002.592124173.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org/bot5796842243:AAESM2w0ubqts6zEsE_xN4PZ56pLfxQ9e7M/5733364805%discordapi%yyy	UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.0000000006BF2000.00000004.00000800.00020000.000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPLease	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.367157703.00000000002B71000.00000004.00000800.00020000.0000000.sdmp, UmpBcHBDbXhaX.exe, 00000005.0000002.405119003.00000000029E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe, 00000000.00000002.373712902.00000000006BF2000.00000004.00000800.00020000.0000000.sdmp	false	URL Reputation: safe	unknown
http://SDRcFr.com	UmpBcHBDbXhaX.exe, 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
Private						
IP						
192.168.2.1						

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756003
Start date and time:	2022-11-29 13:49:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.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@15/9@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe • Not all processes where analyzed, report is missing behavior information • Report creation exceeded maximum time and may have missing d isassembly code information. • Report size exceeded maximum capacity and may have missing b ehavior information. • Report size getting too big, t oo many NtAllocateVirtualMemory calls found. • Report size getting too big, t oo many NtOpenKeyEx calls found. • Report size getting too big, t oo many NtProtectVirtualMemory calls found. • Report size getting too big, t oo many NtQueryValueKey calls found.

Simulations		
Behavior and APIs		
Time	Type	Description
13:50:24	API Interceptor	591x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe modified
13:50:30	API Interceptor	19x Sleep call for process: powershell.exe modified
13:50:32	Task Scheduler	Run new task: UmpBcHBDbXhaX path: C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
13:50:39	API Interceptor	467x Sleep call for process: UmpBcHBDbXhaX.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.12778.11165.exe.log 	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UmpBcHBDbXhaX.exe.log	
Process:	C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.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:	false

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebdbbc72e6\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\1f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21876
Entropy (8bit):	5.601829389408276
Encrypted:	false
SSDEEP:	384:3tCRdN02OVJ/cVCyYnP0SBxnju57iJ9gvRSJ3uyO1+m0S1AVrdtGuA+inYQ:r/cG84xiS57JcuG7lQ
MD5:	2E9B889A60208A20362A3E53763B6013
SHA1:	7F1F939BC9A458DEE7D453964AEBF1D7FAFAA80C
SHA-256:	BFDABCA0F512BD8D3E9CB576755745431D206F0A62227CB17F878E7941D02AB2
SHA-512:	A17F20FF83AF7CBF72DD1796377E0A251E61A06BF4A3AD258694BDBCCD231BCC5A2C5B61D4DCE7F8444D967F26F739D19E8C8701F31021B692EB9AEA753F0379
Malicious:	false
Preview:	@...e.....:B.....@.....H.....<@.^L."My..... Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C.%6..h.....System.Core.0.....G-.o...A...4B.....System.4.....Zg5...O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'.....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....#.....System.Data.H.....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....)gK...G...\$.1.q.....System.ConfigurationP...../C..J..%...].%.....Microsoft.PowerShell.Commands.Utility...D.....-D.F.<.;nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_2sdbjn1.iex.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_j1bp3fok.q3g.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp 	
---	--

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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
Preview:	[ZoneTransfer].....Zoneld=0

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6550716384576925
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.12778.11165.exe
File size:	951296
MD5:	f64f729e0ba974c578afaac25665e067
SHA1:	d1225322fd5f16eb18a90ec4a4b007a010e2d51a
SHA256:	680f16527c5dc7e7e32bb27b99dc8c85c75282d853cb9a27c186963dae883d2e
SHA512:	6bf0f4a2567736cdfa5e422e23f1f43a593699a1276654264a619e2f1b4690af911e04508d0928c3a84ea658c022dc4b44f4f0467254c72bb92191e212e029c8
SSDEEP:	12288:kBuqU+PCH5W8lgKprPRibKTh6SoqZpK3tUjjAK7nYbSuSmFbWNHrDdzoa1cfN:ldrf6SoqbK3lnYUJDdEPf
TLSH:	FC15D08023A6AF70F5386BF37521904827763C6E94F1D2296DDDB0DE2A76B5049F0B27
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L...j..c.....0..j.....@..

File Icon	
	
Icon Hash:	63e6a3a1a6bdbdbb

Static PE Info	
General	
Entrypoint:	0x4e89fa
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:	0x6385A66A [Tue Nov 29 06:27:54 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

[illegible]

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe89a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xea000	0x14d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xec000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0xe6a00	0xe6a00	False	0.8274824271680217	data	7.663847187465398	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x14d0	0x1600	False	0.5793678977272727	data	5.573635871144453	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xec000	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_ICON	0xea0e8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_GROUP_ICON	0xeb190	0x14	data		
RT_VERSION	0xeb1a4	0x32c	data		

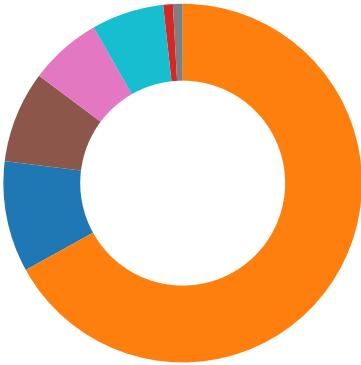
Imports	
DLL	Import
mscorlib.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior



- SecuriteInfo.com.Win32.CrypterX-g...
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- UmpBcHBDbXhaX.exe
- SecuriteInfo.com.Win32.CrypterX-g...
- schtasks.exe
- conhost.exe
- UmpBcHBDbXhaX.exe

Click to jump to process

System Behavior

General

Target ID:	0
Start time:	13:50:16
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe
Imagebase:	0x6f0000
File size:	951296 bytes
MD5 hash:	F64F729E0BA974C578AFAAC25665E067
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: 00000000.00000002.368700625.0000000002D78000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.370626906.0000000003E1E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.370626906.0000000003E1E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.370626906.0000000003E1E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.367157703.0000000002B71000.00000004.00000800.00020000.00000000.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	6D85CF06	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	6D85CF06	unknown
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.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	6C6ADD66	CopyFileW
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6C6ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6A7038	GetTempFile NameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB6C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	success or wait	1	6C6A6A95	DeleteFileW

File Written

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6a fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 6a 0e 00 00 18 00 00 00 00 00 00 fd fd 0e 00 00 20 00 00 00 fd 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PELjc0j @ @	success or wait	4	6C6ADD66	CopyFileW
C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C6ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	0	1600	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6C6A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsof\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.CrypterX-gen.12778.11165.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	6DB6C907	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	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile	

Analysis Process: powershell.exe PID: 3216, Parent PID: 5644	
General	
Target ID:	1
Start time:	13:50:27
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
Imagebase:	0xd00000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high
-------------	------

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C605B28	unknown	
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C605B28	unknown	
C:\Users\user\AppData\Local\Temp__PSscrip iptPolicyTest_2sdbjn1.iex.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C6A1E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscrip iptPolicyTest_j1bp3fok.q3g.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C6A1E60	CreateFileW	
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	6D85CF06	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	6D85CF06	unknown	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_2sdbjn1.iex.ps1	success or wait	1	6C6A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_j1bp3fok.q3g.psm1	success or wait	1	6C6A6A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C605B28	unknown
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_2sdbjn1.iex.ps1	0	1	31	1	success or wait	1	6C6A1B4F	WriteFile
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_j1bp3fok.q3g.psm1	0	1	31	1	success or wait	1	6C6A1B4F	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 14 14 00 00 1a 00 00 00 fd 0e fd 05 fd 08 fd 08 fd 08 00 00 3a 01 42 00 06 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e:B@	success or wait	1	6DB276FC	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	6DB276FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 05 0e fd 00 06 0e fd 00 04 0e fd 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 07 0e fd 00 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 08 0e fd 00 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 12 6f 40 01 2a 29 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 fd 29 40 01 fd 29 40 01 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 21 4d 40 01 3b 4d 40 01 09 06 fd 00 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40	T@>@V@H@X@[@N T@HT@S@S@hT@S@ S@S@.@T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@o@*)@DM@:M @"M@ M@)@Md@d@ Nd@)@)@#)@d@Zd@ d@!M@:M@D@D@@ M@<M@\$M@8M@	success or wait	11	6DB276FC	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D83CA54	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D83CA54	ReadFile		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D841F73	ReadFile		
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	6D84203F	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile		

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mif49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C6A1B4F	ReadFile

Analysis Process: conhost.exe PID: 5284, Parent PID: 3216

General

Target ID:	2
Start time:	13:50:27
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 3644, Parent PID: 5644

General

Target ID:	3
Start time:	13:50:28
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe /Create /TN "Updates\UmpBcHBDbXhaX" /XML "C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp
Imagebase:	0xcb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Read							
File Path	Offset		Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	unknown		2	success or wait	1	CBAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4E8A.tmp	unknown		1601	success or wait	1	CBABD9	ReadFile

Analysis Process: conhost.exe PID: 5484, Parent PID: 3644

General

Target ID:	4
------------	---

Start time:	13:50:28
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: UmpBcHBDbXhaX.exe PID: 624, Parent PID: 1088

General

Target ID:	5
Start time:	13:50:34
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
Imagebase:	0x690000
File size:	951296 bytes
MD5 hash:	F64F729E0BA974C578AFAAC25665E067
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: 00000005.00000002.406721462.0000000002BE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.405119003.00000000029E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 32%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D85CF06	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	6D85CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp8847.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6A7038	GetTempFile NameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UmpBcHBDbXhaX.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB6C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8847.tmp	success or wait	1	6C6A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8847.tmp	0	1600	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6C6A1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\UmpBcHBDbXhaX.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,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089", C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	6DB6C907	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	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebdbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile

Analysis Process: SecuritInfo.com.Win32.CrypterX-gen.12778.11165.exe PID: 5340, Parent PID: 5644

General

Target ID:	6
Start time:	13:50:35
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuritInfo.com.Win32.CrypterX-gen.12778.11165.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuritInfo.com.Win32.CrypterX-gen.12778.11165.exe
Imagebase:	0x7b0000
File size:	951296 bytes
MD5 hash:	F64F729E0BA974C578AFAAC25665E067
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: 00000006.00000000.363415114.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.363415114.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.363415114.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.592981435.0000000002BF8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000002.592124173.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.592124173.0000000002B51000.00000004.00000800.00020000.00000000.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	6D85CF06	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	6D85CF06	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	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C6A1B4F	ReadFile

Analysis Process: schtasks.exe PID: 3540, Parent PID: 624

General

Target ID:	8
Start time:	13:50:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe /Create /TN "Updates\UmpBcHBDbXhaX" /XML "C:\Users\user\AppData\Local\Temp\tmp8847.tmp
Imagebase:	0xcb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Read							
File Path		Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8847.tmp		unknown	2	success or wait	1	CBAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8847.tmp		unknown	1601	success or wait	1	CBABD9	ReadFile

Analysis Process: conhost.exe PID: 1348, Parent PID: 3540

General

Target ID:	9
Start time:	13:50:46
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: UmpBcHBDbXhaX.exe PID: 5468, Parent PID: 624

General

Target ID:	10
Start time:	13:50:48

Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\UmpBcHBDbXhaX.exe
Imagebase:	0x740000
File size:	951296 bytes
MD5 hash:	F64F729E0BA974C578AFAAC25665E067
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: 0000000A.00000002.592547674.0000000002AF8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.592099137.0000000002AA1000.00000004.00000800.00020000.00000000.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	6D85CF06	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	6D85CF06	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	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D835705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4e36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D83CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7903DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7903DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D835705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6A1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6A1B4F	ReadFile	
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C6A1B4F	ReadFile	

Disassembly

 No disassembly