ID: 756016
Sample Name: SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Cookbook: default.jbs
Time: 14:00:02
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

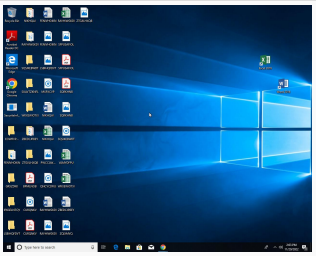
Windows Analysis Report

SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe

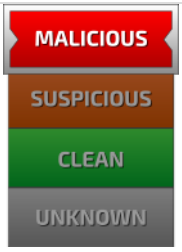
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Analysis ID:	756016
MD5:	630ffd21c1de8a5..
SHA1:	7cdb7d33a07326..
SHA256:	02b628dcbfaa0c...
Tags:	exe Formbook
Infos:	



Detection



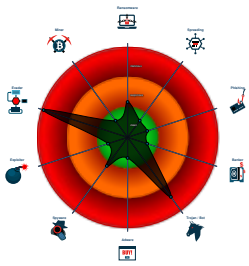
FormBook

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

Signatures

- Yara detected FormBook
- Malicious sample detected (through...
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil...
- Multi AV Scanner detection for drop...
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- Modifies the prolog of user mode fun...
- Queues an APC in another process ...
- Tries to detect virtualization through...

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe (PID: 5808 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe MD5: 630FFD21C1DE8A583A4E1627B8AC6534)
  - powershell.exe (PID: 1436 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\owFIYUUG.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1092 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\owFIYUUG" /XML "C:\Users\user\AppData\Local\Temp\tmpE80B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe (PID: 1044 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe MD5: 630FFD21C1DE8A583A4E1627B8AC6534)
- owFIYUUG.exe (PID: 5580 cmdline: C:\Users\user\AppData\Roaming\owFIYUUG.exe MD5: 630FFD21C1DE8A583A4E1627B8AC6534)
  - schtasks.exe (PID: 2204 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\owFIYUUG" /XML "C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - owFIYUUG.exe (PID: 4764 cmdline: C:\Users\user\AppData\Roaming\owFIYUUG.exe MD5: 630FFD21C1DE8A583A4E1627B8AC6534)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 5544 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 1380 cmdline: /c del "C:\Users\user\AppData\Roaming\owFIYUUG.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.shinecleaningasheville.com/f9r5/"
  ],
  "decoy": [
    "teknotimur.com",
    "zuliboo.com",
    "remmingtoncampbell.com",
    "vehicletitleloansphoenix.com",
    "sen-computer.com",
    "98731.biz",
    "shelikesblu.com",
    "canis-totem.com",
    "metaversemedianetwork.com",
    "adsdu.com",
    "vanishmediasystems.com",
    "astewaykebede.com",
    "wszhongxue.com",
    "gacha-animator-free.com",
    "papatyadekorasyon.com",
    "mqc168.top",
    "simplebrilliantsolutions.com",
    "jubileehawkesprairie.com",
    "ridflab.com",
    "conboysfilm.com",
    "iseemerit.world",
    "airhbb.com",
    "haveyourshare.com",
    "qcstcsz.com",
    "attorneykarinaramirez.com",
    "patriziabartelle.com",
    "dcc.coop",
    "hdzz.top",
    "treesandstarsoracle.com",
    "rebarunikont.com",
    "achivego.site",
    "baipiao100.com",
    "menslibwrty.com",
    "insulationtraining.online",
    "horseflix.club",
    "suxyqyu.xyz",
    "sqoki.com",
    "ffbsjhvbsjhbvsajv.xyz",
    "beapest.cfd",
    "4892166.com",
    "dvdmediastar.com",
    "hotwomensearching4u.site",
    "cupompetlover.com",
    "terrapretasales.com",
    "joinsequene.com",
    "powerkitap.com",
    "jonjene.com",
    "wqcwgl.com",
    "utahexotics.com",
    "ballerboutique.com",
    "cftronline.com",
    "gettidaladvance.site",
    "anagladstonedesign.com",
    "bunsi-figura.store",
    "ttvip-13.net",
    "cmjysx-uqps.website",
    "ifealafia.com",
    "carlospainter.com",
    "elitetrio.xyz",
    "inggridangelia.com",
    "leporebaq.com",
    "youpinhang.com",
    "palm3d.net",
    "wo567567.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x9b90:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x28b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x88f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x98fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x5819:$sqlite3step: 68 34 1C 7B E1 • 0x592c:$sqlite3step: 68 34 1C 7B E1 • 0x5848:$sqlite3text: 68 38 2A 90 C5 • 0x596d:$sqlite3text: 68 38 2A 90 C5 • 0x585b:$sqlite3blob: 68 53 D8 7F 8C • 0x5983:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.358868037.0000000002ACB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.owFIYUUG.exe.3012e30.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
5.2.owFIYUUG.exe.3012e30.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x2a98a:$v1: SbieDll.dll • 0x2a9a4:$v2: USER • 0x2a9b0:$v3: SANDBOX • 0x2a9c2:$v4: VIRUS • 0x2aa12:$v4: VIRUS • 0x2a9d0:$v5: MALWARE • 0x2a9e2:$v6: SCHMIDTI • 0x2a9f6:$v7: CURRENTUSER
5.2.owFIYUUG.exe.3030600.0.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
5.2.owFIYUUG.exe.3030600.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0xd1ba:$v1: SbieDll.dll • 0xd1d4:$v2: USER • 0xd1e0:$v3: SANDBOX • 0xd1f2:$v4: VIRUS • 0xd242:$v4: VIRUS • 0xd200:$v5: MALWARE • 0xd212:$v6: SCHMIDTI • 0xd226:$v7: CURRENTUSER
0.2.SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe.283072c.0.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 15 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

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected FormBook

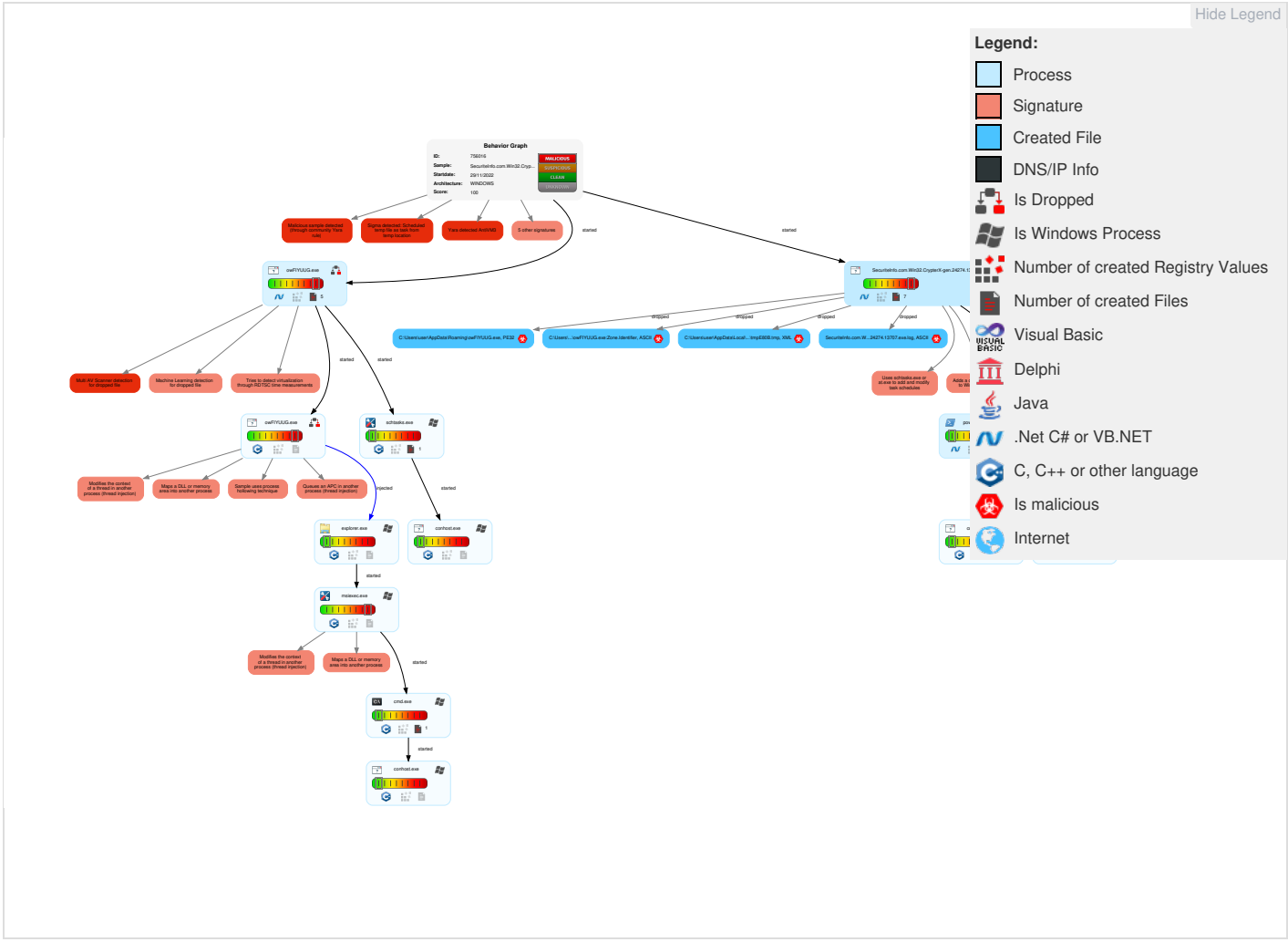
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	4 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	3 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 DLL Side-Loading	1 Scheduled Task/Job	1 Masquerading	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	1 DLL Side-Loading	1 1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	4 1 2 Process Injection	LSA Secrets	1 File and Directory 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	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 1 2 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 Obfuscated Files or Information	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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.24274.13707.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\owFIYUUG.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\owFIYUUG.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Worefiint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-&	0%	Avira URL Cloud	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comldF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comedta	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasik	0%	Avira URL Cloud	safe	
http://www.sakkal.comn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd-&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Q&	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFF&	0%	Avira URL Cloud	safe	
http://www.fontbureau.comc&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/X&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/u&	0%	Avira URL Cloud	safe	
www.shinecleaningasheville.com/f9r5/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsu&	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.shinecleaningasheville.com/f9r5/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000006 9C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comI.TTF	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.000000005 7D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322643766.000000005 7D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322074460.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322109625.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322153903.000000005 7D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321820881.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321913738.000000005 7D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321855758.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321967040.000000005 7D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322703072.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323229165.000000005 7D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322047224.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323259594.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.000000005 7D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.00000000057D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000006 9C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000006 9C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comedta	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322643766.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322703072.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/-&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320263598.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320494921.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319310856.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319212503.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319392230.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320525670.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320440189.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319279685.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320571444.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320191564.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320099257.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319941075.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320055869.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319986515.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320394274.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320301449.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comldF	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322643766.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322807447.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322861249.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322703072.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323229165.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322929853.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323259594.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.00000000057D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.313670458.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comn	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319806390.00000000057C4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324285201.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.324559034 .00000000057D4000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.324418155.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324662108.000000000 57D4000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.324459395 .00000000057D4000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000002.362716051.00000000069C2000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.325354347.000000000 57D2000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.325199869 .00000000057CA000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000002.362488084.00000000057D4000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.351725281.000000000 57C7000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.324736578 .00000000057D4000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000000 69C2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrita	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362488084.000000000 57D4000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.351725281 .00000000057C7000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comasik	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323589071.000000000 57D1000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.000000000 57D1000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd-&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.323023842 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.323229165.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322929853.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.323259594 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.323078179.00000000057D2000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.000000000 57D1000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnt	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.317261346.000000000 57B2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319310856.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319212503.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319392230.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319015579.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319279685.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318849645.00000000057D1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318972157.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Q&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319941075.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320055869.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319986515.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFF&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.358868037.00000000002ACB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.356409073.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, owFIYUUG.exe, 00000005.00000002.376634128.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp, owFIYUUG.exe, 00000005.00000002.379609104.00000000032CA000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320237486.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320477184.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319735455.00000000057C3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319806390.00000000057C4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320289081.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320716381.00000000057BE000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320419124.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320513514.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320160969.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320652389.00000000057BE000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320327067.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320085368.00000000057C6000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319864076.00000000057C4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320019809.00000000057C4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319971645.00000000057C4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320556591.00000000057C6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comc&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000B.00000000.37779063.000000000091F000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000000.460452224.000000000ED27000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000B.00000000.445459434.000000000091F000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000B.00000000.479699094.000000000091F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.317991275.00000000057C8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322074460.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322109625.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322153903.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321820881.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362488084.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.351725281.00000000057C7000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321913738.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321855758.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321967040.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323229165.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322047224.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323259594.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.00000000057D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324285201.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324559034.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324418155.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324662108.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.324459395.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/X&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319941075.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320055869.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319986515.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/u&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319310856.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319212503.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319392230.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319015579.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319279685.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319941075.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318849645.00000000057D1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320055869.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319986515.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318972157.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320263598.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319492794.00000000057CA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319310856.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319212503.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319392230.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319015579.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319279685.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320191564.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320099257.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319941075.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319762053.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318849645.00000000057D1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.320055869.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319986515.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318642829.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319836497.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318619322.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.318972157.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319601112.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362488084.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.351725281.00000000057C7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.322074460 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.322109625.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322153903.000000000 57D2000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.321820881 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.322386330.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321668227.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.321913738 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.321855758.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.321967040 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.Win 32.CrypterX-gen.24274.13707.exe, 0000000 0.00000003.322281913.00000000057D3000.00 000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321718791.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000003.322047224 .00000000057D3000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321668227.000000000 57D3000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000000 69C2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.317261346.000000000 57B2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.000000000 69C2000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.317261346.000000000 57B2000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000002.362716051 .00000000069C2000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322181268.000000000 57C4000.00000004.00000800.00020000.00000 000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.2427 4.13707.exe, 00000000.00000002.362716051 .00000000069C2000.00000004.00000800.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/s	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319310856.00000000057D4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319212503.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319392230.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319279685.00000000057D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlx#	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322807447.00000000057D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322807447.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322861249.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323229165.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322929853.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323259594.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.00000000057D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comt	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323136860.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322807447.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322861249.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323229165.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322929853.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323259594.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323310351.00000000057D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comm	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322243437.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322074460.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322109625.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322153903.00000000057D2000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321820881.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322386330.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321913738.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321855758.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322323380.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321967040.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322281913.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.321718791.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322047224.00000000057D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.319559496.00000000057D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000002.362716051.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalsu&	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323023842.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.322929853.00000000057D3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, 00000000.00000003.323078179.00000000057D2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756016
Start date and time:	2022-11-29 14:00:02 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 19s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/9@0/0
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 100% (good quality ratio 90.7%) • Quality average: 75.2% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe, PID 5808 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:01:11	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe modified
14:01:16	Task Scheduler	Run new task: owFIYUUG path: C:\Users\user\AppData\Roaming\owFIYUUG.exe
14:01:16	API Interceptor	19x Sleep call for process: powershell.exe modified
14:01:28	API Interceptor	1x Sleep call for process: owFIYUUG.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.24274.13707.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.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**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\AppData\Roaming\owFIYUUG.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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	21832
Entropy (8bit):	5.601252470026008
Encrypted:	false

SSDEEP:	384:htCRDuWQai1oxW1b+RgSBxnoG7iJ9gNSJ3uyVc+m0CP1AVrdYqsRgA+inYM:va4oxA4xoG7NcuSCqOCM
MD5:	8A0EBD4F63004083D9E1B87EADB8F420
SHA1:	DB20459DCEB8FFC473A557BDCB846B4FF6E6CB15
SHA-256:	6CBBAF5136896652C6BB53005B42E35A4D2E17504420BF82A56E3EF55F1C5922
SHA-512:	163A3F16437EAF6B419EBCD271B56990B628D93696CB5F334294D844328CB0047B3C7517E9C797FA415D3AAE91A315785E2E16D55C886FCA101FB23DB4BE857
Malicious:	false
Preview:	@...e.....Z.V.K.)...6.M.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.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_hwzfto0e.i5p.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iwi5re21.2w2.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp

Process:	C:\Users\user\AppData\Roaming\owFIYUUG.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.133232133416081
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNtjxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTdv
MD5:	3C7813180DB11C81533084FF4928074F
SHA1:	7775FC8013D2C8AE41FD46E208914762FDBE285E
SHA-256:	F7D0D79388EBA3CD3BA2E062BB6806198C306B2431C3C4DE175ED35BAF2AA151
SHA-512:	5C8F15B20752FD1D6F46917EC98F39A9DDE3E42D388D80BEAF27606A514798F68A9BE3978DF0074E34C167329D5B81538D062EDEAEBA40E06454D0EBB5F1BD B
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmpE80B.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.133232133416081
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtjxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTdv
MD5:	3C7813180DB11C81533084FF4928074F
SHA1:	7775FC8013D2C8AE41FD46E208914762FDBE285E
SHA-256:	F7D0D79388EBA3CD3BA2E062BB6806198C306B2431C3C4DE175ED35BAF2AA151
SHA-512:	5C8F15B20752FD1D6F46917EC98F39A9DDE3E42D388D80BEAF27606A514798F68A9BE3978DF0074E34C167329D5B81538D062EDEAEBA40E06454D0EBB5F1BDB
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	906240
Entropy (8bit):	7.6340340391964485
Encrypted:	false
SSDEEP:	24576:hIVD2ISXOaDU11ecODssqm/6rw5Roa/W9DdEPf:ha2RXOKcLsq46s5RoafP
MD5:	630FFD21C1DE8A583A4E1627B8AC6534
SHA1:	7CDB7D33A07326FA3B2699BB7308889A0920541A
SHA-256:	02B628DCBFAA0CAD2CCDE62B1CFB16425A8D40B4CAD9DE200569CE1B84981612
SHA-512:	9EE857113DF144F0FED19C1C831CF4731B866E8B5A92417B11C445D2CB9A374C430A6C2FC4A7318BD01A0FDC756132D7F4895F0798A3FDF194AC3B223F10CD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...D..c.....0.....R.... .....@.. .....@..... ..@.....O..... ....H.....text...X.... ....`.rsrc.....@..@.reloc..... .....@..B.....4.....H.....<.....I...8u...u.....^..}.....(.....(.....*.0.....s.....o.....(.....*...0.....s.....o.....(.....*...0.....s.....o..... (.....*...0.....s.....o.....(.....*...0..+.....,..{.....+.....,..{....o.....(.....*..0..r.....(....s.....s....}.....s....}.....s....}.....s....}.....(.....{....(....o.....{.....o.....{.....o .....{....r...p "..@A...s!...o".....{....(#...o$.....{.... .... ..

C:\Users\user\AppData\Roaming\owFIYUUG.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
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]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6340340391964485
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.24274.13707.exe
File size:	906240
MD5:	630ffd21c1de8a583a4e1627b8ac6534
SHA1:	7cdb7d33a07326fa3b2699bb7308889a0920541a
SHA256:	02b628dcbfaa0cad2ccde62b1cfb16425a8d40b4cad9de200569ce1b84981612
SHA512:	9ee857113df144f0fed19c1c831cf4731b866e8b5a92417b11c445d2cb9a374c430a6c2fc4a7318bd01a0fdc756132d7f4895f0798a3fdf194ac3b223f10cd68
SSDEEP:	24576:hIVD2ISXOaDU11ecODssqm/6rw5Roa/W9DdEPf:ha2RXOKcLsq46s5RoafP
TLSH:	F615DF903366AFB1F5286BF37521900827B63C6FA5E1D2295DDDB0CE2A71B4149F0B27
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...D..c.....0.....R.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4deb52
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:	0x6385B444 [Tue Nov 29 07:27:00 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdeb00	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xdcb58	0xdcc00	False	0.819646712202718	data	7.640989875299505	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x388	0x400	False	0.369140625	data	2.8465332420355964	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xe2000	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	0xe0058	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

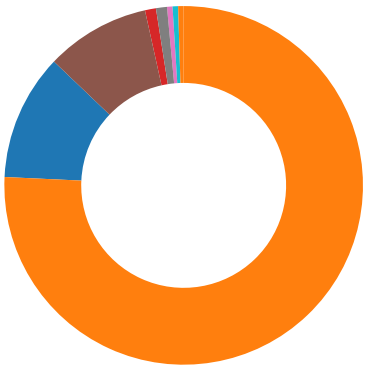
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE2

Statistics

Behavior

- SecuriteInfo.com.Win32.CrypterX-g…
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- owFIYUUG.exe
- SecuriteInfo.com.Win32.CrypterX-g…
- schtasks.exe
- conhost.exe
- owFIYUUG.exe
- explorer.exe
- msiexec.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe PID: 5808, Parent PID: 3324

General

Target ID:	0
Start time:	14:01:03
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Imagebase:	0x400000
File size:	906240 bytes
MD5 hash:	630FFD21C1DE8A583A4E1627B8AC6534
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: 00000000.00000002.358868037.0000000002ACB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.356409073.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.360338705.0000000003A33000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.360338705.0000000003A33000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.360338705.0000000003A33000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.360338705.0000000003A33000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: 1436, Parent PID: 5808

General

Target ID:	1
Start time:	14:01:13
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\owFIYUUG.exe
Imagebase:	0x8d0000
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	6B775B28	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	6B775B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_hwzfto0e.i5p.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6B811E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iwi5re21.2w2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6B811E60	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	6C9CCF06	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	6C9CCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_hwzfto0e.i5p.ps1	success or wait	1	6B816A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iwi5re21.2w2.psm1	success or wait	1	6B816A95	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	6B775B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6B775B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_hwzfto0e.i5p.ps1	0	1	31	1	success or wait	1	6B811B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iwi5re21.2w2.psm1	0	1	31	1	success or wait	1	6B811B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 0b 14 00 00 18 00 00 00 fd 0e 5a 05 56 09 4b 09 29 09 00 00 36 01 4d 00 07 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eZVK)6M@	success or wait	1	6CC976FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-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 3c 00 00 00 0e 00 20 00	H<@^L"My:<	success or wait	17	6CC976FC	WriteFile
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	6CC976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6CC976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6CC976FC	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 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 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 68 54 40 01 fd 53 40 01 fd 53 40 01 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 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 16 3b 40 01 1b 3b 40 01 19 3b 40	T@>@Xd@Vd@*@g@@@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@ M@!M@;M@D@D@@M@<M@$M@8M?MBMDmE;@;@;@	success or wait	11	6CC976FC	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	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C9A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C9003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C9ACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6C9003DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6C9B1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22428	success or wait	1	6C9B203F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9003DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6B811B4F	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	6B811B4F	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	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	112	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6B811B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6B811B4F	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	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C9A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6B811B4F	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	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6B811B4F	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	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6B811B4F	ReadFile

Analysis Process: conhost.exe PID: **3492**, Parent PID: **1436**

General

Target ID:	2
Start time:	14:01:13
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **1092**, Parent PID: **5808**

General

Target ID:	3
Start time:	14:01:13
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\owFIYUUG" /XML "C:\Users\user\AppData\Local\Temp\tmpE80B.tmp
Imagebase:	0xd90000
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\tmpE80B.tmp	unknown	2	success or wait	1	D9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE80B.tmp	unknown	1600	success or wait	1	D9ABD9	ReadFile

Analysis Process: conhost.exe PID: **2960**, Parent PID: **1092**

General

Target ID:	4

Start time:	14:01:13
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: owFIYUUG.exe PID: **5580**, Parent PID: **1084**

General

Target ID:	5
Start time:	14:01:16
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\owFIYUUG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\owFIYUUG.exe
Imagebase:	0xb00000
File size:	906240 bytes
MD5 hash:	630FFD21C1DE8A583A4E1627B8AC6534
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: 00000005.00000002.376634128.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.379609104.00000000032CA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, 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	6C9CCF06	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	6C9CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B817038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\owFIYUUG.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp	success or wait	1	6B816A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp	0	1599	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 61 6c 66 6f 6e 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	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	6B811B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\owFIYUUG.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6CCDC907	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	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C9A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C9003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C9003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C9003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C9A5705	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	6C9A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B811B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B811B4F	ReadFile

Analysis Process: SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe PID: **1044**, Parent PID: **5808**

General

Target ID:	6
Start time:	14:01:18
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.CrypterX-gen.24274.13707.exe
Imagebase:	0x640000
File size:	906240 bytes
MD5 hash:	630FFD21C1DE8A583A4E1627B8AC6534
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.350969233.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.350969233.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.350969233.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.350969233.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: schtasks.exe PID: **2204**, Parent PID: **5580**

General

Target ID:	8
Start time:	14:01:31
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\owFIYUUG" /XML "C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp
Imagebase:	0xd90000
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\tmp2BCB.tmp	unknown	2	success or wait	1	D9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2BCB.tmp	unknown	1600	success or wait	1	D9ABD9	ReadFile

Analysis Process: conhost.exe PID: **2940**, Parent PID: **2204**

General

Target ID:	9
Start time:	14:01:31
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: owFIYUUG.exe PID: **4764**, Parent PID: **5580**

General

Target ID:	10
Start time:	14:01:32
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\owFIYUUG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\owFIYUUG.exe
Imagebase:	0xf20000
File size:	906240 bytes
MD5 hash:	630FFD21C1DE8A583A4E1627B8AC6534
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: **3324**, Parent PID: **4764**

General

Target ID:	11
Start time:	14:01:34
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.488494638.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.454264842.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000000.454264842.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.454264842.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.454264842.00000000079B3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: msiexec.exe PID: **5544**, Parent PID: **3324**

General

Target ID:	14
Start time:	14:02:38
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x1110000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.576589100.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.576589100.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.576589100.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.576589100.0000000000980000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.578229480.0000000004870000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.578229480.0000000004870000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.578229480.0000000004870000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.578229480.0000000004870000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.578188907.0000000004840000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.578188907.0000000004840000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.578188907.0000000004840000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.578188907.0000000004840000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	99A427	NtReadFile

Analysis Process: cmd.exe PID: **1380**, Parent PID: **5544**

General

Target ID:	15
Start time:	14:02:44
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Roaming\owFIYUUG.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3492**, Parent PID: **1380**

General

Target ID:	16
Start time:	14:02:45
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly