ID: 323829
Sample Name:
SecuriteInfo.com.Generic.mg.7e26e87ab642008d.31908
Cookbook: default.jbs
Time: 15:56:17
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

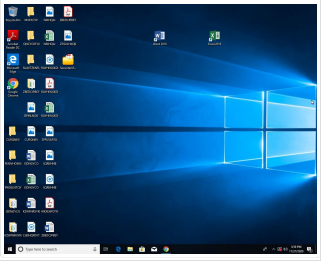
Analysis Report SecuriteInfo.com.Generic.mg.7e26e87a…

Overview

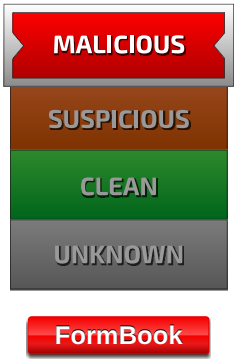
General Information

Sample Name:	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.31908 (renamed file extension from 31908 to exe)
Analysis ID:	323829
MD5:	7e26e87ab64200..
SHA1:	3d4dc73fee1b191.
SHA256:	3176528c561817..

Most interesting Screenshot:



Detection

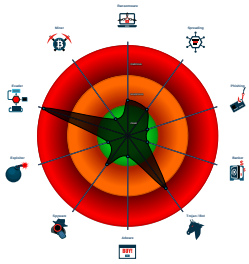


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe (PID: 7144 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe' MD5: 7E26E87AB642008D934824D509559859)
  - SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe (PID: 6460 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe MD5: 7E26E87AB642008D934824D509559859)
- vlc.exe (PID: 4544 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 7E26E87AB642008D934824D509559859)
  - vlc.exe (PID: 6504 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 7E26E87AB642008D934824D509559859)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 3424 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 7072 cmdline: /c del 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - wscript.exe (PID: 4624 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
- vlc.exe (PID: 6512 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 7E26E87AB642008D934824D509559859)
  - vlc.exe (PID: 6880 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 7E26E87AB642008D934824D509559859)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.603587464.0000000002FB0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.603587464.0000000002FB0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

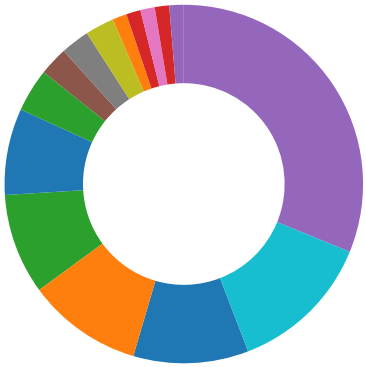
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vlc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vlc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vlc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
11.2.vlc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.vlc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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:

System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

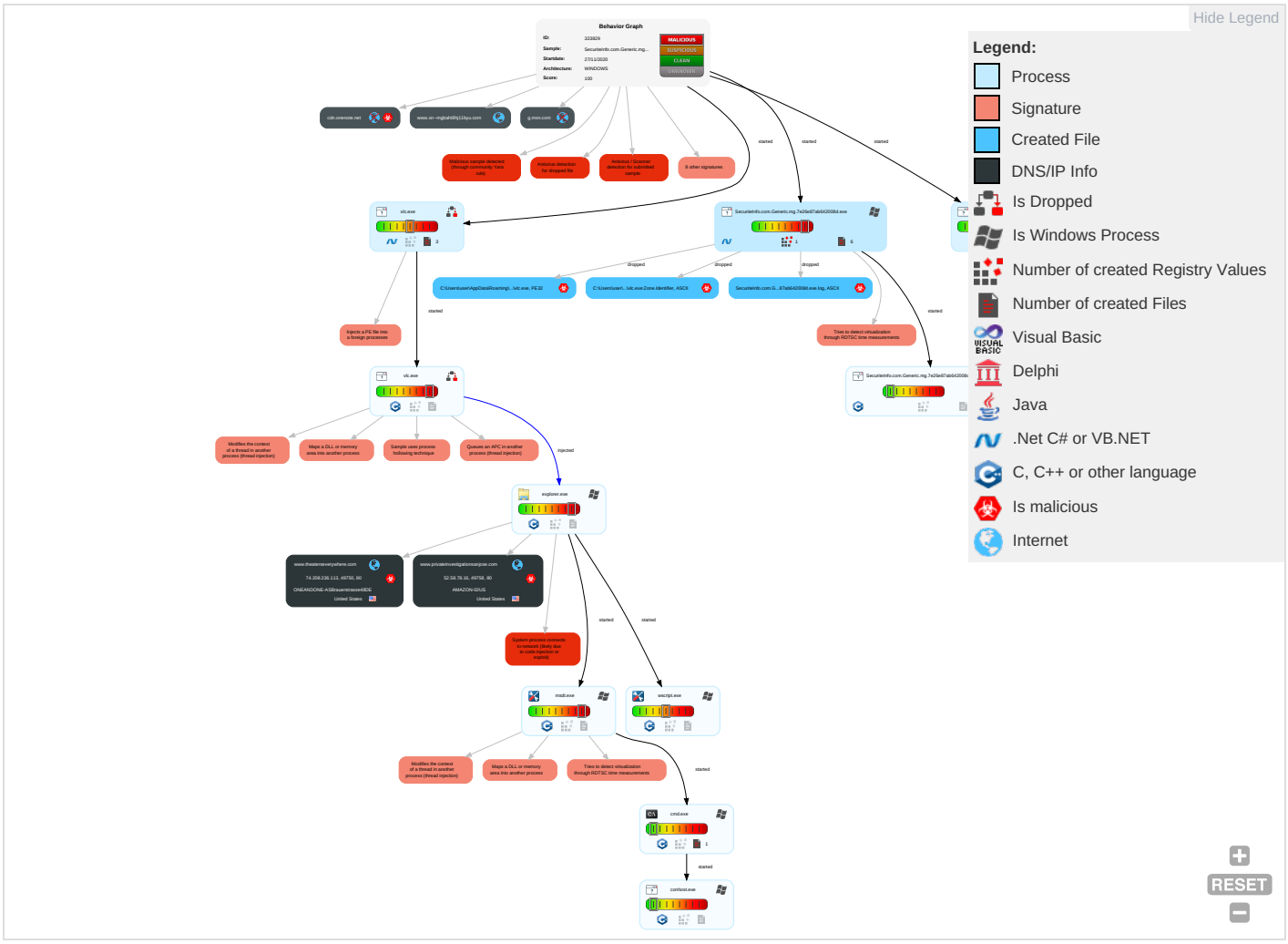
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	System Information Discovery 1 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

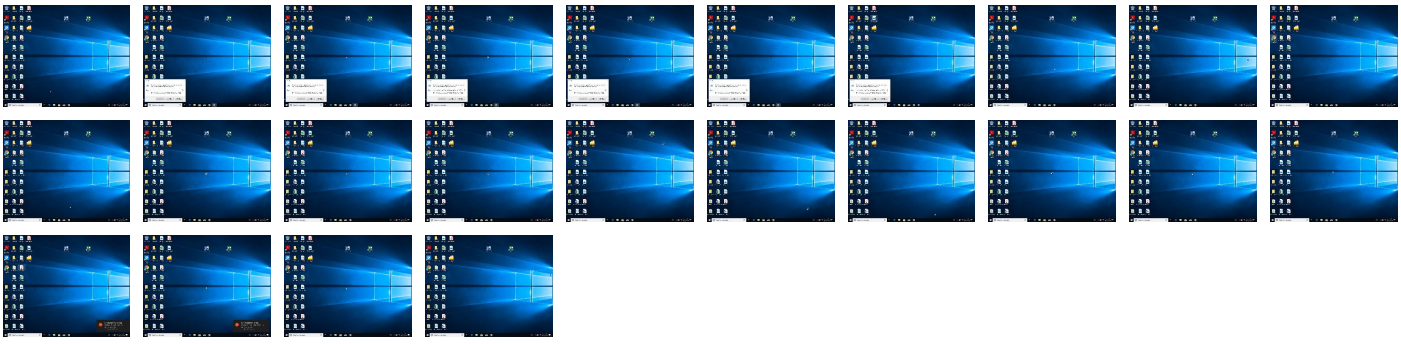
Behavior Graph



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.Generic.mg.7e26e87ab642008d.exe	30%	Virustotal		Browse
SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe	29%	ReversingLabs	Win32.Trojan.Bulz	
SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe	100%	Avira	HEUR/AGEN.1136389	
SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Avira	HEUR/AGEN.1136389	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	29%	ReversingLabs	Win32.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.930000.1.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
5.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.930000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
11.2.vlc.exe.f50000.1.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
0.2.SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.f20000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
11.0.vlc.exe.f50000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.vlc.exe.4e0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
5.2.vlc.exe.da0000.1.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
2.0.vlc.exe.ad0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
6.0.vlc.exe.4e0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
1.2.SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.vlc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vlc.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
0.0.SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.f20000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
2.2.vlc.exe.ad0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File

Domains

Source	Detection	Scanner	Label	Link
cdn.onenote.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.theaterseverywhere.com/gwg/?9rn=O2JDHJlpz2Rt546p&kzrh28=UuziJZlLt+87/GFWj6zrBRQcAJHtDZRD1SjQzE3VTJ8o0dUkW9Z3aESqk1e2d0LlVQYkCVOcaQ==	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/aU	0%	Avira URL Cloud	safe	
http://www.tiro.com4f	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comI1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.como)U	0%	Avira URL Cloud	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	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://fontfabrik.com	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html6	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.xn--mgbaht9hj11byu.com/?9rn=O2JDHJlpz2Rt546p&kzrh28=10pkrk8xXthsIzrXSR/95AORgXFPF0sL7LI6N	0%	Avira URL Cloud	safe	
http://www.privateinvestigationsanjose.com/gwg/?kzrh28=aQP8xClfH3FnyC2bbHADmWrvnT3A6FAlsj34gFGOFlECHJLTyiLQwMrWm8hFX/dhtuP/m5zmeg==&9rn=O2JDHJlpz2Rt546p	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.urwpp.deno	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comC.TTF	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	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.founder.com.cn/cn	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/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comWU	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.xn--mgbaht9hj11byu.com	185.88.152.152	true	false		unknown
www.theaterseverywhere.com	74.208.236.113	true	true		unknown
www.privateinvestigationsanjose.com	52.58.78.16	true	true		unknown
g.msn.com	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.theaterseverywhere.com/gwg/?9rn=O2JDHJlpz2Rt546p&kzrh28=UuziJZlLt+87/GFWj6zrBRQcAJHtDZRD1SjQzE3VTJ8o0dUkW9Z3aESqk1e2d0LlVQYkCVOcaQ==	true	• Avira URL Cloud: safe	unknown
http://www.privateinvestigationsanjose.com/gwg/?kzrh28=aQP8xClfH3FnyC2bbHADmWrvnT3A6FAlsj34gFGOFlECHJLTyiLQwMrWm8hFX/dhtuP/m5zmeg==&9rn=O2JDHJlpz2Rt546p	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/aU	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.340974188.00000000062C5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com4f	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.339567937.00000000062CA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high

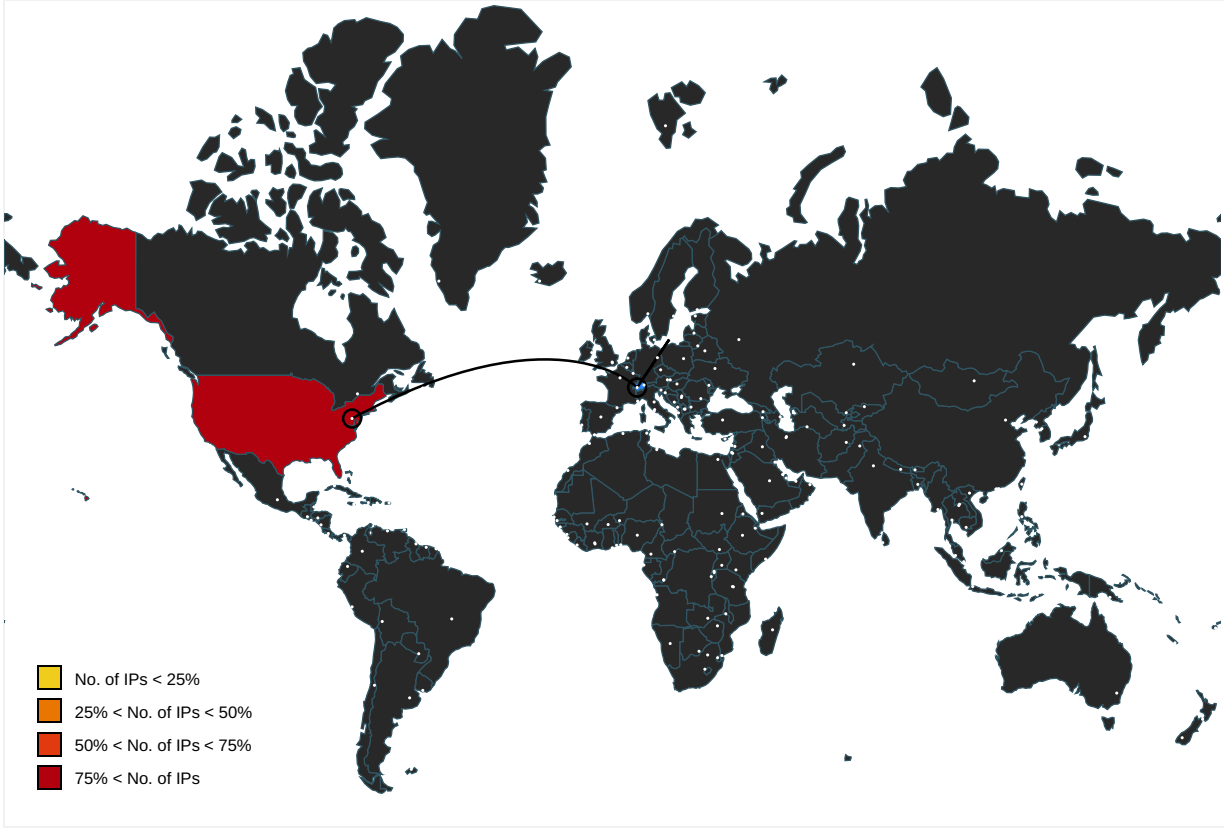
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coml1	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366812851.00000000062C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como)U	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html6	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.340913274.00000000062FB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.340974188.00000000062C5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.xn--mgbaht9hj11byu.com/?9rn=O2JDHJlpz2Rt546p&kzrh28=10pkrk8xXthsIzrXSR/95AORgXFPF0sL7LI6N	msdt.exe, 0000000C.00000002.606711985.0000000005A0F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com.TTF	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deno	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000007.00000000.397228054.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.agfamonotype.	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.346139320.000000000630A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcomd	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlU	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342152773.00000000062F3000.00000004.00000001.sdmp	false		high
http://www.fontbureau.coma	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366812851.00000000062C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comC.TTF	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.339694897.00000000062C9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.339567937.00000000062CA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.340974188.00000000062C5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366812851.00000000062C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000002.366962936.00000000063B0000.00000002.00000001.sdmp, vlc.exe, 00000002.00000002.399391314.0000000005FF0000.00000002.00000001.sdmp, vlc.exe, 00000006.00000002.426387479.0000000005910000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.426302286.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comWU	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalic	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe, 00000000.00000003.342799792.00000000062C6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	unknown	United States		16509	AMAZON-02US	true
74.208.236.113	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323829
Start date:	27.11.2020
Start time:	15:56:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.31908 (renamed file extension from 31908 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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@14/4@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.3% (good quality ratio 4.1%) • Quality average: 77.9% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.11.168.160, 40.88.32.150, 2.20.142.209, 2.20.142.210, 184.24.28.12, 51.103.5.159, 168.61.161.212, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.247, 92.122.213.194, 104.43.139.144, 23.210.248.85, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, cdn.onenote.net.edgekey.net, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
15:57:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
15:57:28	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	Shipping documents.xlsx	Get hash	malicious	Browse	• www.bigdillenergy.com/sqe3/?cB=WEY89Cif+pIi2MLF1zVwoU92FBjT7mYFKn7NGwcjA7VjLh+ShZmG13goYNxo9cFbZs7f6w==&NreT=XJE0G4nHflj
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.muvmiry.com/mfg6/?NL08b=bLXuQ0dQP6ytO8tJ9mzCKhtDbuPWwsM6hpNCZm/len/r8ZkHKew9l8wwKJGUhLNhJCA2aw==&Ab=JpApTx
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.besteggcreditcard.com/coz3/?RFN4=a/ztdlFJlhxM2r+IBkSOd/itNmg8ZT70AaNM2x+2BWn224IL+Pz//n0zCcYtSkXb1ACu/w==&RB=NL00JzKhBv9HkNRp
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.besteggcreditcard.com/coz3/?Cb=a/ztdlFMlmxI27yEDkSOd/itNmg8ZT70AaVcqyi3F2n32JkN5fizpjMxB6YSV0vQ3gqImPTq2A==&uVg8S=yVCTVPM0BpPlbRn
	ptFlhqUe89.exe	Get hash	malicious	Browse	• www.muvmiry.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=bLXuQ0dVP9ypOshF/mzCKhtDbuPWwsM6hpVSFljkaH/q8oIBNOhxz4IyJsqClbJSCBdG
	EME.39134.xlsx	Get hash	malicious	Browse	• www.intact.media/mfg6/?rF=_HCtZ4&yzux_nSp=b6HLQnr1nLoa39Ydr0IvZP1++AM1tzQXE0H5i/XdEnJw02jW6yMX/B+fWxmcOCSPLT01fg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?7nExDDz=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&znedzJ=zZ08lr
	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.hopeharboracademy.com/nwrr/?Rxo=L6hH4NIhfjzT&cj=Pi3dZNULKacZO0lwTZm3VIlJvRqy9WRTjR1P4HicrXgGmUrIoUMqJ7S/A3ArvLwtmevO+VO23g==
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?YnztXrjp=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TKSXSboJU2x&sBZxwb=FxlXFP2PHdiD2
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• www.viltais.com/nt8e/?7nwltvxh=lPNjsY1H0UkcK2guRo/z/De4MaZSsgXVmjo1l8Wqu/JQpRHkDmjuktjJMa7ZMKbETQi&org=3foxnfCXOnIhKD
	Order Specification Requirement With Ref. AMABINIF 38535.exe	Get hash	malicious	Browse	• www.stranded.xyz/utau/?p64=8prxehCX&2dZ8=dR3TRUG1QGrDYRBc9/3PRmogi1D8+kv0RMejNxu9Gn4uSO50WrJFoJLJiRJ5mGAJbjLS
	new file.exe.exe	Get hash	malicious	Browse	• www.sunflowersbikini.com/o1u9/?uFNH=XRlPhLopGJm&njkdnt=NfcJdyO4TBqmRNhg7R1KNJwTQ4N5hlclnZQkvT+zgqJmuxY/wV7RTlrJQJKYZhgz2gKA
	XCnhrl4qRO.exe	Get hash	malicious	Browse	• www.phybby.com/xnc/?iB=CnlpdrqHk6fHx&uN9da=KMkfkwH+qCev6y9SIhjzkdXaKQKuNlF/lv9fMwnf5/4ZPrTh2Mio2MF0cfaBEzR8Th1t

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?u6u4=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRIRvKc0H9QVN&J484=xPJtLXbX
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• www.jencian.com/t4vo/?t8S8=GNX37zD4+hCCMzbajgO2uA69rnGPPC6iQo0EFF7Ue/8gqGUBoM5ya+5BJI3qcC1vYrK1&Njfhlh=8p4PgtUX
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?1b8hnra=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&OZNPdr=iJEt_DFhGZplHfm0
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?DVB0=pTlpd6wHb&QR0=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRLxVaNU/n30K
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• www.centralproperties/vrf/?jVgH=aHUqqRuO6ZK9z0Ddr0bilnwC+HUi2BKQSuMw/XTnNfUykuBqiT/kuVIPFhCASh0TBUtx&-Zi=W6RxUV3PO
	Factura.exe	Get hash	malicious	Browse	• www.devcomunicacao.com/ve9i/?_f-tK4=pQO4LhLAXoDAWMXX61mXtQYyMLN+wLZ8Px2vxkY+llKJMI7QZndoWfY9jQFnQqWsTUfq&hvK8=Q4j0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?GPWlMXk=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TK4IiroNW+x&Ano=O2JpLTIpT0jt

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Direct Deposit.xlsx	Get hash	malicious	Browse	• 13.224.195.11
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 143.204.214.108
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 99.86.2.22
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 54.190.165.96
	DHL_Nov 2020 at 1.85_8BZ290_PDF.jar	Get hash	malicious	Browse	• 54.190.165.96
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 52.216.164.5
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 52.210.2.133
	http://https://rb.gy/flx7ju	Get hash	malicious	Browse	• 13.248.219.100
	Shipping documents.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	PO_0012009.xlsx	Get hash	malicious	Browse	• 99.79.190.44
	paperport_3753638839.exe	Get hash	malicious	Browse	• 13.224.89.193
	opzi0n1[1].dll	Get hash	malicious	Browse	• 13.224.89.96
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2FIf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 34.209.19.120
	http://searchlf.com	Get hash	malicious	Browse	• 13.224.93.71
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 13.224.93.10
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 52.33.248.165
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUeaIQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 44.236.72.93
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 13.224.93.77
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 54.77.92.238
	http://t.comms.officeworks.com.au/r/?id=hb22c4478,920a576c,91374a10&p1=developerhazrat.com/p13p13yu13/bGVnYWxpbnRAc2VhcnNoYy5jb20=%23#c13c13v13h13h13u13l13j13m##	Get hash	malicious	Browse	• 18.136.188.28
ONEANDONE-ASBrauerstrasse48DE	EME_PO.47563.xlsx	Get hash	malicious	Browse	• 74.208.236.61
	fSBya4AvVj.exe	Get hash	malicious	Browse	• 74.208.236.48
	PO987556.exe	Get hash	malicious	Browse	• 217.160.0.166
	Inv.exe	Get hash	malicious	Browse	• 217.160.0.173
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 74.208.236.115
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 217.160.0.74
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 74.208.236.115
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 217.160.0.92
	http://www.winter-holztechnik.de/	Get hash	malicious	Browse	• 217.160.0.67
	Re- attached Instruction.xlsx	Get hash	malicious	Browse	• 82.165.48.223
	docs.html	Get hash	malicious	Browse	• 74.208.236.216
	Prueba de pago.exe	Get hash	malicious	Browse	• 217.76.146.62
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 217.160.0.224
	Narud#U017eba 0521360021.xlsx	Get hash	malicious	Browse	• 74.208.22.240
	Quote Request.xlsx	Get hash	malicious	Browse	• 82.165.48.223
	anthony.exe	Get hash	malicious	Browse	• 217.160.0.199
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 74.208.5.21

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WO4jeXWl0L.exe	Get hash	malicious	Browse	• 74.208.45.104
	5YCsNuM4a9.exe	Get hash	malicious	Browse	• 74.208.45.104
	eLaaw7SqMi.exe	Get hash	malicious	Browse	• 74.208.5.22

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	5901777.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1391
Entropy (8bit):	5.344111348947579
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4W:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	E87C60A24438CC611338EA5ACB433A0A
SHA1:	E0C6A7D5CFE32BB2178E71DEE79971A51697B7DD
SHA-256:	80DAB47D7A9E233A692D10ACAF5793E34911836D36DB2E11BB7C5D42DE39782A
SHA-512:	3DBD6773153DC9D05558ED491A92C9B4B72D594263D7BD2D06BDDCF09BE55477D35041145219A5E9A46B38575E5B60DA91C6870B2CA29A83388695AD389B8EE
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\vlc.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	5.344111348947579
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4W:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	E87C60A24438CC611338EA5ACB433A0A
SHA1:	E0C6A7D5CFE32BB2178E71DEE79971A51697B7DD
SHA-256:	80DAB47D7A9E233A692D10ACAF5793E34911836D36DB2E11BB7C5D42DE39782A
SHA-512:	3DBD6773153DC9D05558ED491A92C9B4B72D594263D7BD2D06BDDCF09BE55477D35041145219A5E9A46B38575E5B60DA91C6870B2CA29A83388695AD389B8EE
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\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	552960

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Entropy (8bit):	7.182147023805618
Encrypted:	false
SSDEEP:	12288:MiUO3ly0AZNVNpiWbYOoa09FQFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxxZ:InULziIYpaIFq
MD5:	7E26E87AB642008D934824D509559859
SHA1:	3D4DC73FEE1B191C2B942E28920C37C82D38B0ED
SHA-256:	3176528C561817095AF859F4809A2091F8557F93C27A0FE32EE71C8FC3B71F33
SHA-512:	C51D64487F852B3D24C4F6B6C2EB79DEAC9394A607BE1B8287BD087398B17B5403DDACE34EB46FD0A5807E044ECC6869213CCEF9EEDA4604D7A1DF711B691A2C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Joe Sandbox View:	• Filename: 5901777.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....No... .....@.. ....@.....n..W..... .....H.....text...TO... ...P..... ..`.rsrc.....R.....@..@.rel oc.....n.....@..B.....0o.....H.....J..h$.....0.....0.....-.&(....+.&+.*....0..3.....(.....-.&..-.&..-.&.(....+.(....+.(....+.(....+.*..0 ....-.&s.....-.&sX....-.&.o....+..+...+...+..(.....o.....j2...+...(....r...p..H.....(.....(.....*.....o[.....o....t+...}....*...0.. .....{....r...po.....-.&&+.}....+.*.0..u.....{....(.....-.&~....-I+. .+. ....r_..p.....(.....-.&....(.....(....(....-.&+..+.....+.~....{!..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
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):	7.182147023805618
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
File size:	552960
MD5:	7e26e87ab642008d934824d509559859
SHA1:	3d4dc73fee1b191c2b942e28920c37c82d38b0ed
SHA256:	3176528c561817095af859f4809a2091f8557f93c27a0fe32ee71c8fc3b71f33
SHA512:	c51d64487f852b3d24c4f6b6c2eb79deac9394a607be1b8287bd087398b17b5403ddace34eb46fd0a5807e044ecc6869213ccef9eeda4604d7a1df711b691a2c
SSDEEP:	12288:MiUO3ly0AZNVNpiWbYOoa09FQFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxxZ:InULziIYpaIFq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....No... .....@.. ....@.....

File Icon

Icon Hash:	d098909eaab2a282

Static PE Info

General

Entrypoint:	0x446f4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC0BE0B [Fri Nov 27 08:51:23 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0x46ef4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x48000	0x41bd8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	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	0x44f54	0x45000	False	0.973933565444	data	7.97600028112	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x41bd8	0x41c00	False	0.411054836027	data	5.84744042564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x484c0	0x3acd	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x4bf90	0x668	data		
RT_ICON	0x4c5f8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4287137928, next used block 12320655		
RT_ICON	0x4c8e0	0x1e8	data		
RT_ICON	0x4cac8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x4cbf0	0x662a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x5321c	0xea8	data		
RT_ICON	0x540c4	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 15987957, next used block 16184308		
RT_ICON	0x5496c	0x6c8	data		
RT_ICON	0x55034	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x5559c	0x6014	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x5b5b0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 2533359616, next used block 620756992		
RT_ICON	0x6bdd8	0x94a8	data		
RT_ICON	0x75280	0x67e8	data		
RT_ICON	0x7ba68	0x5488	data		
RT_ICON	0x80ef0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16777215, next used block 520093696		
RT_ICON	0x85118	0x25a8	data		
RT_ICON	0x876c0	0x10a8	data		
RT_ICON	0x88768	0x988	data		
RT_ICON	0x890f0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x89558	0x11e	data		
RT_VERSION	0x89678	0x35c	data		
RT_MANIFEST	0x899d4	0x204	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

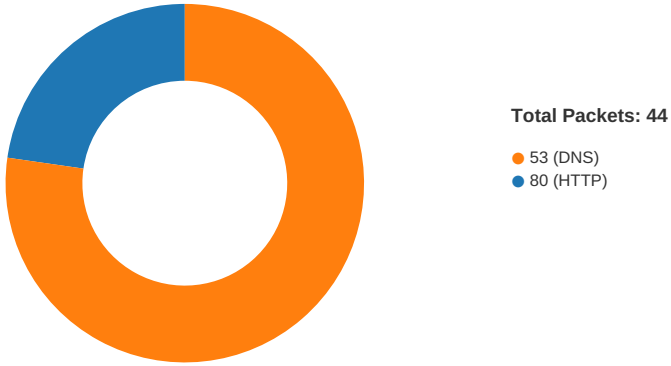
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	(c) 2020 Skype and/or Microsoft
Assembly Version	8.65.0.76
InternalName	Cxnjmhojuh1.exe
FileVersion	8.65.0.76
CompanyName	Skype Technologies S.A.
Comments	Skype Setup
ProductName	Skype
ProductVersion	8.65.0.76
FileDescription	Skype Setup
OriginalFilename	Cxnjmhojuh1.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:58:33.396914005 CET	49750	80	192.168.2.6	74.208.236.113
Nov 27, 2020 15:58:33.533881903 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:33.534008026 CET	49750	80	192.168.2.6	74.208.236.113
Nov 27, 2020 15:58:33.534207106 CET	49750	80	192.168.2.6	74.208.236.113
Nov 27, 2020 15:58:33.671035051 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:33.681374073 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:33.681425095 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:33.681441069 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:33.681639910 CET	49750	80	192.168.2.6	74.208.236.113
Nov 27, 2020 15:58:33.681781054 CET	49750	80	192.168.2.6	74.208.236.113
Nov 27, 2020 15:58:33.818573952 CET	80	49750	74.208.236.113	192.168.2.6
Nov 27, 2020 15:58:55.095927954 CET	49758	80	192.168.2.6	52.58.78.16
Nov 27, 2020 15:58:55.112649918 CET	80	49758	52.58.78.16	192.168.2.6
Nov 27, 2020 15:58:55.112831116 CET	49758	80	192.168.2.6	52.58.78.16
Nov 27, 2020 15:58:55.112926960 CET	49758	80	192.168.2.6	52.58.78.16
Nov 27, 2020 15:58:55.129580975 CET	80	49758	52.58.78.16	192.168.2.6
Nov 27, 2020 15:58:55.129667997 CET	80	49758	52.58.78.16	192.168.2.6
Nov 27, 2020 15:58:55.129729033 CET	80	49758	52.58.78.16	192.168.2.6
Nov 27, 2020 15:58:55.130250931 CET	49758	80	192.168.2.6	52.58.78.16
Nov 27, 2020 15:58:55.130465031 CET	49758	80	192.168.2.6	52.58.78.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:58:55.147123098 CET	80	49758	52.58.78.16	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:57:32.229760885 CET	53781	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:32.256953955 CET	53	53781	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:33.055875063 CET	54064	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:33.091309071 CET	53	54064	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:43.564912081 CET	52811	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:43.591944933 CET	53	52811	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:44.428431034 CET	55299	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:44.455573082 CET	53	55299	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:53.035280943 CET	63745	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:53.070861101 CET	53	63745	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:54.414926052 CET	50055	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:54.451869011 CET	53	50055	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:54.472253084 CET	61374	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:54.507540941 CET	53	61374	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:55.716264009 CET	50339	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:55.743356943 CET	53	50339	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:56.532305956 CET	63307	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:56.559402943 CET	53	63307	8.8.8.8	192.168.2.6
Nov 27, 2020 15:57:57.663681984 CET	49694	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:57:57.699119091 CET	53	49694	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:04.349950075 CET	54982	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:04.385519981 CET	53	54982	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:04.915282965 CET	50010	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:04.950737953 CET	53	50010	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:05.845258951 CET	63718	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:05.880856037 CET	53	63718	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:06.083427906 CET	62116	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:06.118822098 CET	53	62116	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:06.220453978 CET	63816	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:06.256165981 CET	53	63816	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:06.627125025 CET	55014	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:06.662755966 CET	53	55014	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:07.342999935 CET	62208	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:07.378743887 CET	53	62208	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:07.948687077 CET	57574	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:07.975754976 CET	53	57574	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:08.783049107 CET	51818	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:08.818336964 CET	53	51818	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:09.243026018 CET	56628	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:09.293510914 CET	53	56628	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:09.718720913 CET	60778	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:09.745874882 CET	53	60778	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:10.305634022 CET	53799	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:10.332758904 CET	53	53799	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:11.581770897 CET	54683	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:11.625076056 CET	53	54683	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:17.165414095 CET	59329	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:17.200875044 CET	53	59329	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:23.159578085 CET	64021	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:23.195239067 CET	53	64021	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:24.009538889 CET	56129	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:24.044955969 CET	53	56129	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:33.350066900 CET	58177	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:33.390670061 CET	53	58177	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:38.151173115 CET	50700	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:38.195622921 CET	53	50700	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:42.778146029 CET	54069	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:42.805150986 CET	53	54069	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:43.748873949 CET	61178	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:58:43.784307003 CET	53	61178	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:46.229530096 CET	57017	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:46.264960051 CET	53	57017	8.8.8.8	192.168.2.6
Nov 27, 2020 15:58:55.042613029 CET	56327	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:58:55.094605923 CET	53	56327	8.8.8.8	192.168.2.6
Nov 27, 2020 15:59:15.481240034 CET	50243	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:59:16.492161989 CET	50243	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:59:17.137989044 CET	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:57:54.414926052 CET	192.168.2.6	8.8.8.8	0x8c94	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:58:11.581770897 CET	192.168.2.6	8.8.8.8	0x45ec	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:58:33.350066900 CET	192.168.2.6	8.8.8.8	0x674d	Standard query (0)	www.theaterseverywhere.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:58:46.229530096 CET	192.168.2.6	8.8.8.8	0x6f22	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:58:55.042613029 CET	192.168.2.6	8.8.8.8	0x8a6f	Standard query (0)	www.privateinvestigationsanjose.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:59:15.481240034 CET	192.168.2.6	8.8.8.8	0x9a59	Standard query (0)	www.xn--mgbaht9hj11byu.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:59:16.492161989 CET	192.168.2.6	8.8.8.8	0x9a59	Standard query (0)	www.xn--mgbaht9hj11byu.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:57:54.451869011 CET	8.8.8.8	192.168.2.6	0x8c94	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:58:11.625076056 CET	8.8.8.8	192.168.2.6	0x45ec	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:58:33.390670061 CET	8.8.8.8	192.168.2.6	0x674d	No error (0)	www.theaterseverywhere.com		74.208.236.113	A (IP address)	IN (0x0001)
Nov 27, 2020 15:58:46.264960051 CET	8.8.8.8	192.168.2.6	0x6f22	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:58:55.094605923 CET	8.8.8.8	192.168.2.6	0x8a6f	No error (0)	www.privateinvestigationsanjose.com		52.58.78.16	A (IP address)	IN (0x0001)
Nov 27, 2020 15:59:17.137989044 CET	8.8.8.8	192.168.2.6	0x9a59	No error (0)	www.xn--mgbaht9hj11byu.com		185.88.152.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.theaterseverywhere.com
- www.privateinvestigationsanjose.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	74.208.236.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 15:58:33.534207106 CET	6858	OUT	GET /gwg/?9rn=O2JDHJlpz2Rt546p&kzrh28=UuziJZILt+87/GFWj6zrBRQcAJHtDZRD1SjQzE3VTJ8o0dUkW9Z3aESqk1e2d0LlVQYkCVOcaQ== HTTP/1.1 Host: www.theaterseverywhere.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 15:58:33.681374073 CET	6859	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 1364 Connection: close Date: Fri, 27 Nov 2020 14:58:33 GMT Server: Apache X-Frame-Options: deny Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 23 70 61 72 74 6e 65 72 2c 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 68 65 69 67 68 74 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 75 74 6c 69 6e 65 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 57 22 20 6e 61 6d 65 3d 22 65 78 70 69 72 65 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 6 5 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6c 6c 6f 77 69 6e 67 20 4d 65 74 61 2d 54 61 67 20 66 69 78 65 73 20 73 63 61 6c 69 6e 67 2d 69 73 73 75 65 73 20 6f 6e 20 6d 6f 62 69 6c 65 20 64 65 76 69 63 65 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 6 9 63 65 2d 77 69 64 74 68 3b 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 3b 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 73 72 63 3d 22 2f 2f 73 65 64 6f 70 61 72 6b 69 6e 67 2e 63 6f 6d 2f 66 72 6d 70 61 72 6b 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 77 69 6e 64 6f 77 2e 6c 6f 63 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <style type="text/css"> html, body, #partner, iframe { height:100%; width:100%; margin:0; padding:0; border:0; outline:0; font-size:100%; vertical-align:baseline; background:transpare nt; } body { overflow:hidden; } </style> <meta content="NOW" name="expires"> <meta content="index, follow, all" name="GOOGLEBOT"> <meta content="index, follow, all" name="robots"> ... Following Meta-Tag fixes scaling-issues on mobile devices --> <meta content="width=device-width; initial-s cale=1.0; maximum-scale=1.0; user-scalable=0;" name="viewport"> </head> <body> <div id="partner"></div> <script type="text/javascript"> document.write('<script type="text/javascript" language="JavaScript"' + 'src="//sedoparking.com/frmpark/' + window.loc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49758	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 15:58:55.112926960 CET	6927	OUT	GET /gwg/?kzrh28=aQP8xClfH3FnyC2bbHADmWrvnT3A6FAlsj34gFGOFlECHJLTyiLQwMrWm8hFX/dhtuP/m5zme g==&9rn=O2JDHJlpz2Rt546p HTTP/1.1 Host: www.privateinvestigationsanjose.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 27, 2020 15:58:55.129667997 CET	6927	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Fri, 27 Nov 2020 14:58:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 66 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 70 72 69 76 61 74 65 69 6e 76 65 73 74 69 67 61 74 69 6f 6e 73 61 6e 6a 6f 73 65 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 62 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 70 72 69 76 61 74 65 69 6e 76 65 73 74 69 67 61 74 69 6f 6e 73 61 6e 6a 6f 73 65 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>5f <meta http-equiv='refresh' content='5; url=http://www.privateinvestigationsanjose.com/' />a </head>9 <body>4b You are being redirected to http://www.privateinvestigationsanjose.coma </body>8</html>0

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

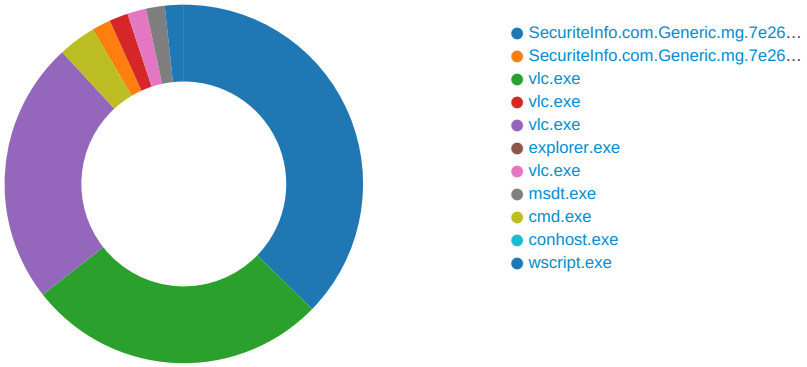
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEC
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEC
GetMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEC
GetMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEC

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe PID: 7144
Parent PID: 5992

General

Start time:	15:57:09
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe'
Imagebase:	0xf20000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.362182042.0000000004291000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.362182042.0000000004291000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.362182042.0000000004291000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7D94D23	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7D94D23	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0b be c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 50 04 00 00 1e 04 00 00 00 00 00 4e 6f 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P..........No... ....@.. ....@................	success or wait	3	7D94D23	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	7D94D23	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe.log	unknown	1391	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",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_v4.0.3	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	vlc	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"	success or wait	1	6CF1646A	RegSetValueExW

Analysis Process: SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe PID: 6460 Parent PID: 7144

General

Start time:	15:57:21
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.7e26e87ab642008d.exe
Imagebase:	0x930000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
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: 00000001.00000002.361705637.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.361705637.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.361705637.0000000000400000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: vlc.exe PID: 4544 Parent PID: 3440

General

Start time:	15:57:28
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xad0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.395346123.0000000003E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.395346123.0000000003E81000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.395346123.0000000003E81000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 29%, 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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	unknown	1391	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",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_v4.0.3	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D011B4F	ReadFile

Analysis Process: vlc.exe PID: 6504 Parent PID: 4544

General

Start time:	15:57:36
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0xda0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
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: 00000005.00000002.472784516.00000000016C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.472784516.00000000016C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.472784516.00000000016C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.472823831.00000000016F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.472823831.00000000016F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.472823831.00000000016F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.469558497.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.469558497.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.469558497.0000000000400000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: vlc.exe PID: 6512 Parent PID: 3440

General

Start time:	15:57:36
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0x4e0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.421292153.0000000003831000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.421292153.0000000003831000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.421292153.0000000003831000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E0CCF06	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	6E0CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D011B4F	ReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6504

General

Start time:	15:57:38
Start date:	27/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vlc.exe PID: 6880 Parent PID: 6512

General

Start time:	15:57:48
Start date:	27/11/2020

Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0xf50000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
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: 0000000B.00000002.430429619.0000000001580000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.430429619.0000000001580000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.430429619.0000000001580000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.429223817.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.429223817.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.429223817.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.430333784.0000000001550000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.430333784.0000000001550000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.430333784.0000000001550000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: msdt.exe PID: 3424 Parent PID: 3440

General

Start time:	15:57:50
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x920000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.602316294.0000000000C40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.603587464.0000000002FB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.603587464.0000000002FB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.603587464.0000000002FB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2FC9E57	NtReadFile

Analysis Process: cmd.exe PID: 7072 Parent PID: 3424

General

Start time:	15:57:56
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 7048 Parent PID: 7072

General

Start time:	15:57:56
Start date:	27/11/2020

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: wscript.exe PID: 4624 Parent PID: 3440

General

Start time:	15:58:09
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x12e0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000013.00000002.471808114.0000000000590000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.471808114.0000000000590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.471808114.0000000000590000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5A9E57	NtReadFile

Disassembly

Code Analysis