ID: 634648
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.20966.21933
Cookbook: default.jbs
Time: 15:44:13
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.W32.AIDetect.malware2.20966.21933 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\Users\user\AppData\Local\Temp\Bolson210.ini 10
C:\Users\user\AppData\Local\Temp\Efterkommelserne.lnk 10
C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib 10
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll 11
C:\Users\user\AppData\Local\Temp\NMDllHost.exe 11
C:\Users\user\AppData\Local\Temp\Nonarguable.JAP 11
C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf 12
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll 12
C:\Users\user\AppData\Local\Temp\athcfg20U.dll 12
C:\Users\user\AppData\Local\Temp\audio-volume-high.png 13
C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png 13
C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png 13
C:\Users\user\AppData\Local\Temp\farme.Fej5 14
C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png 14
C:\Users\user\AppData\Local\Temp\nsaD009.tmp\System.dll 14
C:\Users\user\AppData\Local\Temp\vmmemctl.inf 15
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Authenticode Signature 16
Entrypoint Preview 16
Rich Headers 17
Data Directories 17
Sections 17
Resources 17
Imports 18
Version Infos 18

Possible Origin 18
Network Behavior 19
Statistics 19
System Behavior 19
Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.20966.exePID: 7152, Parent PID: 1212 19
General 19
File Activities 19
File Created 19
File Deleted 21
File Written 21
File Read 27
Registry Activities 27
Key Created 27
Key Value Created 28
Disassembly 28

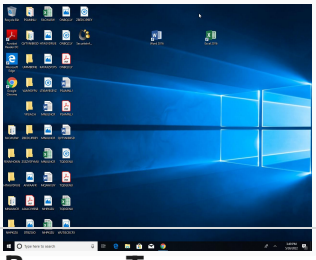
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.20966.21933

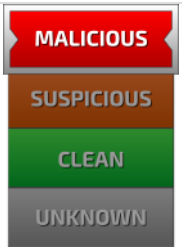
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.20966.21933 (renamed file extension from 21933 to exe)
Analysis ID:	634648
MD5:	64d7de9ac60040..
SHA1:	961f113b32ce2f0..
SHA256:	da36f8024e0a8b..
Tags:	exe
Infos:	



Detection



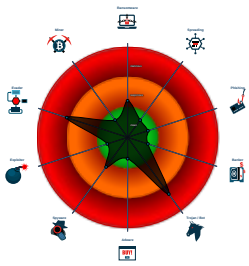
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetect.malware2.20966.exe (PID: 7152 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe" MD5: 64D7DE9AC600402C1F3E5B9849CBD12C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.912152970.00000000028F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

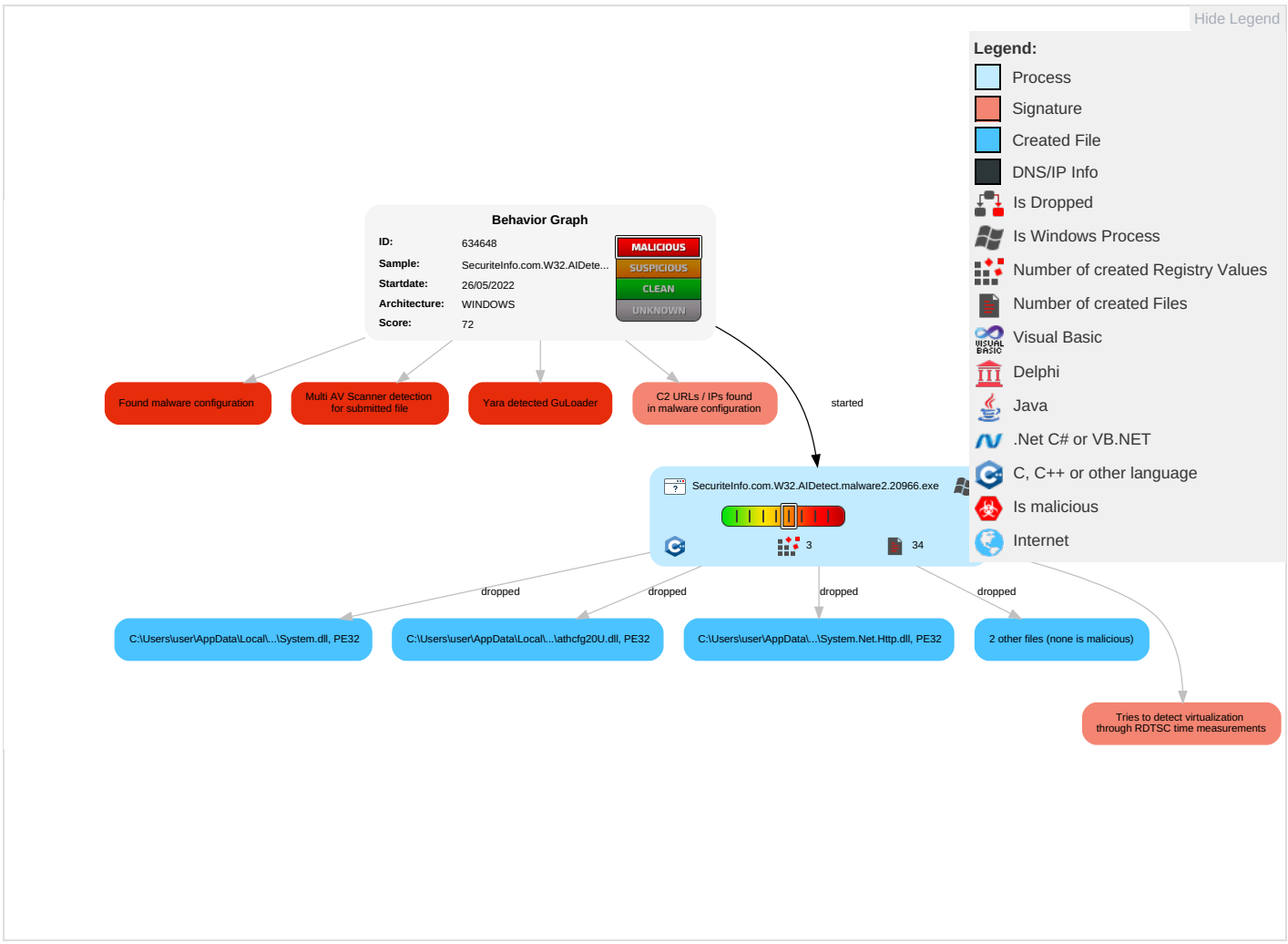
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Query Registry	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	LSASS Memory	1 1 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	1 Obfuscated Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

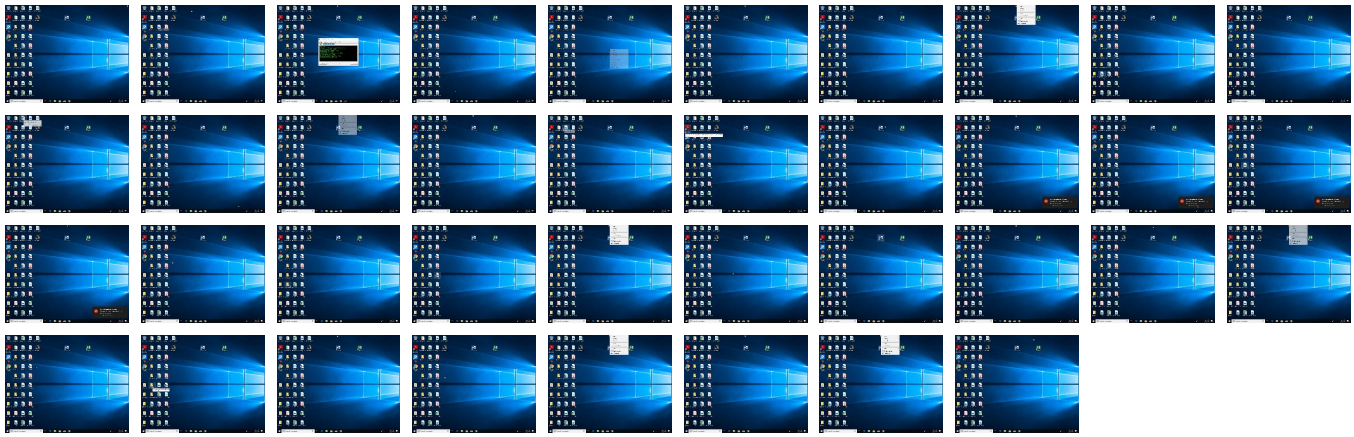
Behavior Graph



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.W32.AIDetect.malware2.20966.exe	7%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	7%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/963535165500588126/979323922124263434/NANO_uyUuDnXlo102.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	NMDllHost.exe.0.dr	false		high
http://ocsp.sectigo.com0	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	NMDllHost.exe.0.dr	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	NMDllHost.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.nero.com	NMDllHost.exe.0.dr	false		high
http://https://sectigo.com/CPS0D	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://scripts.sil.org/OFLSource	SourceCodePro-Medium.otf.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Lib.Platform.Windows.Native.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.symauth.com/cps0(	NMDllHost.exe.0.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	Lib.Platform.Windows.Native.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	634648
Start date and time: 26/05/202215:44:13	2022-05-26 15:44:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.20966.21933 (renamed file extension from 21933 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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/16@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.1% • Quality standard deviation: 21.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Bolson210.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.540402352056965
Encrypted:	false
SSDEEP:	3:5CeXAYpqyn:5CeWy
MD5:	D5E9EF9561789A05AFB528A1E6C7D9B7
SHA1:	B2C92096EE4103A58B41A0754F2E1F1BB823392C
SHA-256:	8D2AE334DCB01E0A5EE1F9CA0689E68743E851B96E48A75ED5E20515D03D7FF5
SHA-512:	09FC8CF87BA6D12D744D5560B14DC8CFBCE9F9DA4EAAF36C1F6176AA56C0F40129F0B231C373E7BE1206F0209137782615FB60FFCD4A184D5131FD073A6586
Malicious:	false
Reputation:	low
Preview:	[Disjunction33]..kanone=BLINDFOLDER..

C:\Users\user\AppData\Local\Temp\Efterkommelserne.lnk

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	930
Entropy (8bit):	2.9877459496241774
Encrypted:	false
SSDEEP:	12:8wl02sX2lw/tz+7RafgKDKmY1oQ18/+CNJkKAb4t2Y+xIBjK:8NTaRMgK0nSPHAJ7aB
MD5:	B72A15FCF169B17EF75614082A0E692F
SHA1:	70A6565C47FD468711002EF46D6957684299422D
SHA-256:	6268FF1957A7EE405135802328B6A1EEA3D8152CD0596E7F30DF788152FB4D61
SHA-512:	CC9C453032EDE3AD18316E922218A28B6A24E37461A8069FC52D723ABC5B2289ADDFC0DFAAC5BB3E11E6260A4FE8C840B9D04BDD2C87F2D60432F3A77E3F7C9
Malicious:	false
Reputation:	low
Preview:	L.....F.....)....P.O. .:i.....+00../C:\.....P.1.....Users.<.....U.s.e.r.s.....Z.1.....user..B.....e.n.g.i.n.e.e.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....\.2.....horla.exe.D.....h.o.r.l.a...e.x.e.....\.h.o.r.l.a...e.x.e.$.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5

MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	515816
Entropy (8bit):	6.444433831771789
Encrypted:	false
SSDEEP:	12288:hY/Hjc0/Lf7vjm4GjDL7ROBM1SMzRJTp4g4D:hY/Dc+LDLmVL7QMx9Np4g4D
MD5:	232371076A23379753EB776CF06FBE5D
SHA1:	6A5EA5D44E555AD392725E5AC3D80AF0137386E9
SHA-256:	5940F9D18B9439ECBFCD6EDC60563D6F56623D03F09EAFA786C436185EF156BB
SHA-512:	590F67E8455DCFE57795F17C94E6082B54C1FEAEF81942B1E92EFC7905E3E6B6EC7A05EEF12A8F0483B5DC1928DC9E7645A74BAE31E77F7AC403C64344F0962 5
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..'~..'~..'~....-.1~..f...N~..... ~...y. ~.....6~...../~.....#~..|...)~..'~.. .~.....#~.....&~...A.&~.....&~..Rich'~.....PE..d.....J`....." .....T).....`.....I.....I.....(A.....$.....0... ....p.....p...8.....text...F..... ..`.rdata...q.....r.....@..@.data...H.....j.....@....pdata..(A.....B...p..... .....@..@.rsrc.....@..@.reloc..0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\NMDllHost.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116720
Entropy (8bit):	5.889271571414613
Encrypted:	false
SSDEEP:	3072:g3nqpX2I6OhctR+lCTD01Lcy4J93TnCx86:L2W1oy4J93TCT
MD5:	DBF787BD6E5CE77FB34FF281A144EB96
SHA1:	50B7799ECCA566BE35429828245D44CB04AD8885
SHA-256:	CCBACEEA04837229C95C08274C747ABE069279AFB990DDD89EC743C42ADC0AD9
SHA-512:	07949EC3882D9CB6E2341CE60C6E911F24463B01F484C037E65A2A8F3495543A096B632E01F8480D03FF388D1E811ECF760155F97F1D5329785C506603BB18A7
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.L.u.L.u.LF.bL.u.LF.aL.u.LF.dL.u.LF.`L.u.L..,L.u.L..<L.u .L.u.L.t.Lu.|L.u.L...L.u.Lu.`L.u.Lu.fL.u.Lu.cL.u.LRich.u.L.....PE..L.....U.....@.....@.....E.....p..... .....`...8.....0&..@.....text..... ..`.rdata...N.....P.....@..@.data...p....`.....T.....@....shared..... .....^.....@....rsrc...p.....`.....@..@.reloc...K.....L...d.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Nonarguable.JAP

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	data
Category:	dropped

Size (bytes):	104885
Entropy (8bit):	6.616929267685571
Encrypted:	false
SSDEEP:	1536:zHdJZGScq/G0IQMvlBQ0SqfxeDnSpKJfyTB2jEyGIMe:zHseGdQoBtorHpGIz
MD5:	783896AB4BF80A78F5D6EF8CD5E67835
SHA1:	46C7FAB858B604A8CF50FE0F6612152A0D6743CA
SHA-256:	49B6243080ED1C14B192FA5D7D9FC04C8A9992AD81E088C4B58B4934877F4618
SHA-512:	7AED4B10EFA8E359FB00B83429EE0363EADD53A7A51AFB622F2B7FEFF195739B0A0BBD96E6D7098E697ECE7E92C4E6E4A72606C8BE6620719CF940A110FC29B3
Malicious:	false
Preview:	.......b.. I..@RRRRRRRRRRRRRRRRRRRRRRRRRRRR!.f.u......f......8 .S.CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC.......f...f ....$hm..f....=%f.f8888888888888888888888888888888888888888888888888888888f......f.......s....).T\|b<<<<<<<<<<<<<<<<<<<<<<<<< <<<<<<<<<<<<....v..g.f.....f...f.c.f.c..(.......................................r.......f....e..f......e...........................f.j............t.M...........................f...f.e.......i..3.\|..&&&&&&&&&&&&&&&&&& &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.......h....=.2...f...f...........f....7....ssssssssssssssssssssssssssssssssssssssssssssssss ....f.u....q.......B..qs...f!.f......k.f....!,..A...................................f..........-K..=...f.r.H..........3[..Y......................... ....f...f...f....@$...

C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	132096
Entropy (8bit):	7.120290023334178
Encrypted:	false
SSDEEP:	3072:r8z0aOC7z/raqtHAGoJaw10xCMZvMfz+7zDxKlJgWbAh2+b:rY7z/GqtgF43Qi7XxKlJhevb
MD5:	75D305F30919530A2C49AC362D2E2D34
SHA1:	B9EE4ACF9AC299FCADC4A074AEA0C0FD7888AA1D
SHA-256:	CF5676ADA0FF425860EE60E3EE7AC4091C568D9FD9E3562D4BC7F06D5A78AD15
SHA-512:	6DB2CE736A5F735FCE1AE4D3573E4E03B3E2F605A39280FC30FF28879130B5F4F2BE45C541D30FC6C29718009FEFC40CEFB2E4F267CFAE3ECFBD8949F48CD37B
Malicious:	false
Preview:	OTTO.......`BASEe.]........FCFF ......FT..|.DSIG............GDEF......@....GPOS......x...8GSUB..]....,...JOS/2.E....P...`cmap.spB......3fhead..h........6hhea.3.....$...$hmtx.:.%... ....Bmaxp. P....H....name:,.]........post...3..F4... ....Q.X_.<.....................;.:...$......................X.;.;.....................P.. .....X.........X...K...X...^.2.%........... .....8.........ADBO... . ...`............. .....J.~................................$............<..........H..........T..........`..........l.........&.~.........&..........*..........6..........D.*.........:.n....................2..........$............ ..........D.*.....................,......................J..........,..........d.\.........(......................4..........4..........2.......... .B.........4.b.. ....*..........<.........$.N......... .r.........,..........0...........

C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	204192
Entropy (8bit):	6.237429214447198
Encrypted:	false
SSDEEP:	3072:HzS560/yk/J3HssPqqGLgl+zX3FKZzSzvG7mH28dZOjc/2r6MqRo9HYzsQb5878:HqJ3HssPqqGLgl+zXkZzt84a84
MD5:	DA9015DF320DCC2EDDEE493E20F639BA
SHA1:	5732E5722D2CB5A668ABC19AED6434852D0A4FC8
SHA-256:	2294EBB89E749E7145628164913251B563EA6641A6CD1AE03FBCE55DA43F9B17
SHA-512:	AF2C0E289665378428171741 46DEDEA93A00BDBACF97FFAAECE878E3191D3719BF9A2B1618AB645CB68D2039B4EB16524B309A2BF0D76DDCA6AE09708CD2CBFA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....o.\.........." ..0......".......... ....a. ....`...............................r...O......................_.......................................................... .............. ..H...........text....... ..................... ..`.rsrc............ ....@..@.reloc........... ....@..B........................H.......8...0...........h...x...((...*.0..-.......~P...- r...p.....()...o*...s+......P...~P...*.~Q...*...Q...*V(....r'..p~Q...o,...*V(....re.. p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,...*V(....rA..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,...*V(....r%..p~Q...o,...*V(....re..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~ Q...o,...*V(....r!..p~Q...o,...*V(....rW..p~Q...o,...*V(....r...p~Q...o,...*V(....r...p~Q...o,..

C:\Users\user\AppData\Local\Temp\athcfg20U.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	311390

Entropy (8bit):	6.361387975641255
Encrypted:	false
SSDEEP:	6144:U/Vk7bUkU6FA8p/eE7Zfjaehfp49MQJZMCJkp5kUKFhRY2:wV8qgZfhhfp49MQJZMCJC5YFZ
MD5:	96CF937BBA21CB4D3203E15246837AE9
SHA1:	08B9BF57F8942CA98077B62BB0DBA0BD0AF2C952
SHA-256:	398185CE130D689D5D2B2C3F179F540715F030D91246C876675E84456F1BA488
SHA-512:	C9E3B60B266ED39B85E87B083EED132441FB364D443AC60F5C4A1BC7B59595FE97387B00BA6817265DC7BF30F3FFAA4F3DF1385327F85C083B51F91CA169D28
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q.Z.0...0...0.....0...,...0.../...0..(,...0.../...0.../...0...0...1..Q....0.... ...0..l6...0.....0..T....0..Rich.0.....PE..L....}.I.....!.....G..... .....p...:..X...@....p.....3..0%..... ....(.....text..... ..`.rdata..`.... ....@..@.data....i.....p.....@....rsrc.....p.....p.....@..@.reloc...:..... .@.....@..B.....

C:\Users\user\AppData\Local\Temp\audio-volume-high.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	725
Entropy (8bit):	7.612179564723704
Encrypted:	false
SSDEEP:	12:6v/7skki3PkFefEst0cNLbh4rbRiUq4reba3XECLR9ZFahsWujm9dcKjnpdwlkc:VkkMPkxc04Lbh4rViH4rEalLHnWVujuS
MD5:	5CE69BDF1125A922B6ED1FE28DCAF92B
SHA1:	10C925FAD32D7071A3D96608FD1A04ECDA1B4820
SHA-256:	0537CF9335394EA509ED23021DAA44F781D380FEAA3947B9DD31C290BE706E1A
SHA-512:	E4F76572FE9613BA184E7988533BC434B61FDD0544C148DFB53EB7691590232A2930515B70F61B9696980EE6FA01202C861BEB9A1AEE859C3ECCDD795BBA75E8
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx....t.`...p....Em.k.m.8.m.m.7.9.m4..K..$bbb.}..T9.....k.....Mu.....]...-(...8o8.B.^.B....4r..e...6.c.....B=.....P]`D....A.*W.]s....g.!...z..?< w...o..\%..r...a.)..X.N.y...u.h..!...r..._.R..}.v.{..).l._.A.j~.ZE?d.....L.(.ZmL.....3....P.....,.(.3.,D..]K....9Y..1c..K..i....w...s.....K.._5 M..1r...].'.|..5v__..#....X8w..`.u=..+..... ..K.!Y9..<EN.m./....r.....,....#F.....]....{...2..A.)Y..W.. r.v.o..]..['.V.....I3T.U.....A.=.T.\.....X."..P...\..Y?..4.P(..i..y...;..oP@.i..l.<.O...%KZ.....-w...<<<...|_..=...?..Ol{r!.. .Z...k..|.....].v..V..no.[....j..z..N...n.%Opip3.88..9...L.....(UG.h:u....[..u ...^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	207
Entropy (8bit):	6.561784186830513
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllJF5peNf2J+Ej+hdc45kjv/iW8DFWwd5sXGQ4Hh9:6v/lhPysPwXx5kjSW8DF3dyTKhAq7p
MD5:	EBBCB008023C6C1B4EFAB0774A4BB19E
SHA1:	7C657C976D7D728E9D6D8F6A603F50B42D86C321
SHA-256:	5FD17A236AF8B520DB2E34E44E71C3634CB8221E0A27617E522ECB8D0FF8EFF8
SHA-512:	DCEDCF09A83F2350D42001CFD009B395F8CA7B9B33F4B7CC3C1C787EDCE9749030EB54AC8D90645F92C141C8D882A4F0AB9A32F274320DE260CD3DF37CED7CE
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..S1..0.<..._..>..q3&n..X(.&F.!!@.....8.....b.W...r.`*t.|....a4l....&..|.B...6.F..'Yk$....e_a.y..I...8.D..~..=.9...eE/....5.x.B.B.O. "J....IEND.B`.

C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	255
Entropy (8bit):	6.804661221546568
Encrypted:	false
SSDEEP:	6:6v/lhPEkME03pQi22U1mw7vgdLSPhZjp7YlHgX+nSbw/Vp:6v/7CE03p829ovCAYlNnScz
MD5:	0D948AEE5693D469DA3F0DCC0FCC009D
SHA1:	61A9DA78E129B3A98855E54F837025CA20DF8017
SHA-256:	85D3314527708E953C393ABE52AD6A7AD63BDA7A31353CE0380CC775AA781A6F

SHA-512:	C7E601DF3F09BCF1D144F35CF9402E00CCDE7C3CB705D5EC39787F526158DE4110CEE10965DDCBD64BC65B3DC97CD8E504BBFEF20ACF045D0851441C691C605
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx..C.CQ..{.me.;.....6..a.;..A...x_..*....9\.....o...8.>.Y..I.I....m!..BJ...C.u.(.H.H.W...U?...w.N....)AP(da...;.8k....7.}.a.j.....C.d.`0i{.r..b1Gz..w2 .IBH<.T`..;....x .e`.O{.W..7...W..O?.c$+..8.....IEND.B`.

C:\Users\user\AppData\Local\Temp\farme.Fej5

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	46132
Entropy (8bit):	3.999752590177944
Encrypted:	false
SSDEEP:	768:1KZto2j5sElk5yRgKwA6/eyPRR0jvf4VDJOPYK/+bszhsAyN/Abdfl82y:OLKkzw3PRRmoV9OPYnbsq1Cpfl8f
MD5:	B067370FD071B16223FA8E1E5A1474EE
SHA1:	4460E6972EE4AEC56907FC10879ED2616E10409A
SHA-256:	57197A007044FBC9E7EE63D5C69291EF7A6241C9A71EFAC545C02D18966BFD7C
SHA-512:	0BB027C330FB598F63FE0623757DF31AB6CEF7710AD351DCEB285FFA679C3611EB3275C59DBBDAA5C17B138595A1E9AFB06DB417F6186C0F05265F43A130795D
Malicious:	false
Preview:	58A4253FD3B42F5FA91C8D12804FC6FA7A4BA0D0C5675ED8B152B9CF952E74D3ACB2B1AE281C08CB7B4A10D6E77A1ED827491B0174924D5C0FDFC76E AB79539C2E408937D181CE65C580DC683E3C1F747263B7C1BC97F0CCFE3BAE949ED844F1CE40DDF7A1CB503C7F53DD27F459AA87AC386D602DC5F65F 7CF26CBF9683B8C79C49B7563BAB64F868407CCCABB98836E49F8E8FF7D31CA43B296089394127E874EA38CFD73E2EF63547C416152B9A5322FD6B41 3CFF7A2AD4005384C177912551247CB1ABA7D4861704502D4B845D5547A86813F138CE4771495C8079E83BBB042E20D68AF4F48DC8786A6E7942362C 024A6FC9FE2E3DF2AD69F0C0DE0DCE25BB73FBCFFCD93FB1CE3C597CC6F9EC70A0D3A8D9684E850B17C0C49304AEF2FEBA909C2C718B01247CCE6B8F 00D0850C519099FDE101CB71B47DE3CA4F8385EF71ED7B6853C6100F552930CD83034C3E88E267A39EE17E526F3A9BA68E28A68EA1E9C02B6FEE73C8 8DC4BB79CD0C6E01D143152E009B736DD0875C4504997D16C70D3CDB35094575CC795BE60A043D9A722C66052915B4AEC63EED9B54C6D6169E182FB6 C30C4003DCD50C7CA0D80AA913F01B1D9BE81A015EA5CF013E6B394F53BE66DF67904060547AF417B637957A5FBBD1B6D975B830D96A83C55F8AC667 61ABC06F8B2DDCD28E3DEC89011288E226A17B9B

C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	274
Entropy (8bit):	6.700098934002617
Encrypted:	false
SSDEEP:	6:6v/lhPysPQcxtmxnHmYR3o5dEYBgQin+ErxwfHDYnIp:6v/7lxUhH/N9YB/inDwfHwi
MD5:	D8FFE7BA5669DE024607E64126DDFFEC
SHA1:	D1993BB12041E4C3F7CF45AFB2DBCFB74A544C0D
SHA-256:	2A6FD48DE810DE4BD61BD26DDAECCB6C6C9204CB4D213EBE1ACB560054911CDD
SHA-512:	47C6D898DE3DFC27E63563F7723F8F690156FBF0F45470FF0DD2FE4E75D4B7108D9700E34E14890DB95C9D20A9D77D7429B32044B2E58708984A4014D35760BD
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0.E_.%.P&#.d.6.....3..A....B.".-t."vd.c..}.d...g...b.B4.k.....l..W'..Q"F.K.;.ez.+D...D..S...h.1b.."..w.E..T`u@..c.s..#+..<.. |....b.Q.8^.9P.u...s.... T...W.A.....2.V..P.....{../.....$.....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsaD009.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text... .....".....`.rdata..c...@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\vmmemctl.inf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	5.060293593237505
Encrypted:	false
SSDEEP:	48:uTHxDxX7Nrh4sRIjan3/CpUlOpUjWQ05+N2iNM0zjjf47GvSzRU:gxDl7Nl4sDvvOK0/mMu4C5
MD5:	4BCE488F7C4E00ED71170C7D0A593663
SHA1:	F49F1FD072D650A8A5DD1F026E003CEE85420BC8
SHA-256:	17365C633230CD05375125AA6C710B76900E2B93D87D14E1F9F2338C3B3BEA1A
SHA-512:	E570D618B14A39F319DC12F0332BA62E8387C5A9F8104AEC7263F89B806CA7E501DD9762B8B117B34E5F8E401564C015FF269BC432776327C7768C3B67087F7E
Malicious:	false
Preview:	..;----------..; vmmemctl.inf..;..; Copyright (c) 1993-1999, Microsoft Corporation..; Copyright (c) 1999-2019 VMware, Inc. All rights reserved...;----------.....[version]..Signature="$Windows NT$"..Class = System..ClassGUID = {4d36e97d-e325-11ce-bfc1-08002be10318}..Provider = %VMwareProvider%..DriverVer = 08/12/2019, 7.5.5.0..CatalogFile = vmmemctl.cat..DriverPackage DisplayName = %loc.VMMemCtlServiceDisplayName%..DriverPackageType = KernelService....[DestinationDirs]..DefaultDestDir = 12....[SourceDisksNames]..1 = %loc.Disk1%,,,""....[SourceDisksFiles]..vmmemctl.sys = 1....;..;; Default install sections..;;....[DefaultInstall]..OptionDesc = %loc.VMMemCtlServiceDesc%..CopyFiles = VMMemCtl.DriverFiles....[DefaultInstall.Services]..AddService = %VMMemCtlServiceName%,0x800,VMMemCtl.S

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.7061727765713295
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
File size:	1007944
MD5:	64d7de9ac600402c1f3e5b9849cbd12c
SHA1:	961f113b32ce2f0958ec5fcccf5489524cf30348
SHA256:	da36f8024e0a8b325dbd71aceed611d0cc8000af85346ceea1bd2a2cf1a73eb6
SHA512:	d2bb0170b1fa8afbabe8a0e2265f29a9bff07879082f25c7d0183b64c60fb2508af985fa5acef8d31e5ffd0f279f55ef831576cb4bad5d94a19da102c1889bff
SSDEEP:	24576:gbgt9utUghMeF3HVojgCpaxMiicfJuAJB:qgiUgXXujhpaCib
TLSH:	D12523153F9CCE22C4A00DB5B9F2C6496BB4ED00065D6A437351783EFEFE6576A0A11B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	34d2c6c3c7c6bc58

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN="kontorrekvisits Oppugned ", O=Ballant5, L=Elizabethtown, S=Kentucky, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/26/2022 3:05:17 AM 5/26/2023 3:05:17 AM
Subject Chain	• CN="kontorrekvisits Oppugned ", O=Ballant5, L=Elizabethtown, S=Kentucky, C=US
Version:	3
Thumbprint MD5:	B5BE6BA51DC7F328E361775F3AFB98CE
Thumbprint SHA-1:	2BCE3B99E9132A3E6375A192F9D0C64AEF4D8E7B
Thumbprint SHA-256:	9645B569EF57649368EF203133C795CF98EBD15713833D5B5C737859188A2774
Serial:	F81B94967AC0A1CA

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FF8E8BE178Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx

Instruction
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FF8E8BE175Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x60000	0x3a278	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xf4938	0x1810	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x2a000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0x3a278	0x3a400	False	0.578342945279	data	6.13676898317	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x60388	0x11db7	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x72140	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x82968	0x94a8	data	English	United States
RT_ICON	0x8be10	0x5488	data	English	United States
RT_ICON	0x91298	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 234938623, next used block 4294909696	English	United States
RT_ICON	0x954c0	0x25a8	data	English	United States
RT_ICON	0x97a68	0x10a8	data	English	United States
RT_ICON	0x98b10	0x988	data	English	United States
RT_ICON	0x99498	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x99900	0x100	data	English	United States
RT_DIALOG	0x99a00	0x11c	data	English	United States
RT_DIALOG	0x99b20	0xc4	data	English	United States
RT_DIALOG	0x99be8	0x60	data	English	United States
RT_GROUP_ICON	0x99c48	0x84	data	English	United States
RT_VERSION	0x99cd0	0x264	data	English	United States
RT_MANIFEST	0x99f38	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	unawarelymed
FileVersion	8.3.15
CompanyName	uvanligereomk
LegalTrademarks	INSTRUKTIONS
Comments	NONSTIC
ProductName	Anti60
FileDescription	Meousgavebo
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.20966.exe PID: 7152, Parent PID: 1212

General

Target ID:	0
Start time:	15:45:33
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe"
Imagebase:	0x400000
File size:	1007944 bytes
MD5 hash:	64D7DE9AC600402C1F3E5B9849CBD12C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.912152970.00000000028F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nssBB48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW

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	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Nonarguable.JAP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\farme.Fej5	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\athcfg20U.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\audio-volume-high.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vmmemctl.inf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaD009.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
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	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaD009.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaD009.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaD009.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nssBB48.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsaD009.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nonarguable.JAP	0	27131	fd fd fd fd fd fd 0f 62 fd fd 20 49 fd fd 40 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 52 21 fd 66 0f 75 fd 0f fd fd fd fd 66 0f fd fd fd fd fd 38 20 fd 53 0a 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 fd fd fd fd fd fd 66 0f fd fd 66 0f fd fd fd 24 68 6d fd 0f fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 fd fd fd fd fd fd 0f fd fd 66 0f fd fd fd 3d 25 66 fd 66 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 66 fd fd 00 0f	b I@RRRRRRRRRRRRRRRRRRRRRRRRRRRRR!fuf8 SCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCC Cff$hmf=%ff8888888888888888888 8888888888888888888888888888888888888f	success or wait	4	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\GooCanvas-3.0.typelib	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns ="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\farme.Fej5	0	28091	35 38 41 34 32 35 33 46 44 33 42 34 32 46 35 46 41 39 31 43 38 44 31 32 38 30 34 46 43 36 46 41 37 41 34 42 41 30 44 30 43 35 36 37 35 45 44 38 42 31 35 32 42 39 43 46 39 35 32 45 37 34 44 33 41 43 42 32 42 31 41 45 32 38 31 43 30 38 43 42 37 42 34 41 31 30 44 36 45 37 37 41 31 45 44 38 32 37 34 39 31 42 30 31 37 34 39 32 34 44 35 43 30 46 44 46 43 37 36 45 41 42 37 39 35 33 39 43 32 45 34 30 38 39 33 37 44 31 38 31 43 45 36 35 43 35 38 30 44 43 36 38 33 45 33 43 31 46 37 34 37 32 36 33 42 37 43 31 42 43 39 37 46 30 43 43 46 45 33 42 41 45 39 34 39 45 44 38 34 34 46 31 43 45 34 30 44 44 46 37 41 31 43 42 35 30 33 43 37 46 35 33 44 44 32 37 46 34 35 39 41 41 38 37 41 43 33 38 36 44 36 30 32 44 43 35 46 36 35 46 37 43 46 32 36 43 42 46 39 36 38 33 42 38 43	58A4253FD3B42F5FA91C8D12804FC6FA7A4BA0D0C5675ED8B152B9CF952E74D3ACB2B1AE281C08CB7B4A10D6E77A1ED827491B0174924D5C0FDFC76EAB79539C2E408937D181CE65C580DC683E3C1F747263B7C1BC97F0CCFE3BAE949ED844F1CE40DDF7A1CB503C7F53DD27F459AA87AC386D602DC5F65F7CF26CBF9683B8C	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.Native.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 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 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 63 1f 33 27 7e fd fd 27 7e fd fd 27 7e fd fd 2e 06 2d fd 31 7e fd fd 66 19 fd fd 4e 7e fd fd fd 0f fd fd 20 7e fd fd fd 79 fd 20 7e fd fd fd 0f fd fd 36 7e fd fd fd 0f fd fd 2f 7e fd fd fd 0f fd fd 23 7e fd fd 7c 16 fd fd 29 7e fd fd 27 7e fd fd fd 7e fd fd 0c fd fd 23 7e fd fd 0c fd fd 26 7e fd fd 0c 41 fd 26 7e fd fd 0c fd fd 26 7e fd fd 52 69 63 68 27 7e fd	MZ@!L!This program cannot be run in DOS mode.$c'~'~'~.-1~fN~ ~y ~6~/~#~|)~'~~#~&~A&~& ~Rich'~	success or wait	21	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\NMDllHost.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 14 fd 1f fd 75 fd 4c fd 75 fd 4c fd 75 fd 4c 46 fd 62 4c fd 75 fd 4c 46 fd 61 4c fd 75 fd 4c 46 fd 64 4c fd 75 fd 4c 46 fd 60 4c fd 75 fd 4c fd 0d 2c 4c fd 75 fd 4c fd 0d 3c 4c fd 75 fd 4c fd 75 fd 4c fd 74 fd 4c 75 fd 7c 4c fd 75 fd 4c fd fd 04 4c fd 75 fd 4c 75 fd 60 4c fd 75 fd 4c 75 fd 66 4c fd 75 fd 4c 75 fd 63 4c fd 75 fd 4c 52 69 63 68 fd 75 fd 4c 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$uLuLuLFbLuLFaLuLFdLuLF`LuL,LuL<LuLuLtLu|LuLL uLu`LuLufLuLucLuLRichuL	success or wait	6	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SourceCodePro-Medium.otf	0	30139	4f 54 54 4f 00 0e 00 fd 00 03 00 60 42 41 53 45 65 1e 5d fd 00 02 03 fd 00 00 00 46 43 46 46 20 fd fd fd 01 00 00 46 54 00 01 7c fd 44 53 49 47 00 00 00 01 00 02 03 fd 00 00 00 08 47 44 45 46 fd fd fd 00 01 fd 40 00 00 02 fd 47 50 4f 53 fd fd fd 00 01 fd 78 00 00 14 38 47 53 55 42 01 fd 5d 05 00 01 fd 2c 00 00 1d 4a 4f 53 2f 32 fd 45 fb 00 00 01 50 00 00 00 60 63 6d 61 70 07 73 70 42 00 00 12 fd 00 00 33 66 68 65 61 64 19 fd 68 fd 00 00 00 fd 00 00 00 36 68 68 65 61 06 33 00 fd 00 00 01 24 00 00 00 24 68 6d 74 78 fd 3a 01 25 00 01 fd fd 00 00 0c 42 6d 61 78 70 06 20 50 00 00 00 01 48 00 00 00 06 6e 61 6d 65 3a 2c fd 5d 00 00 01 fd 00 00 11 1a 70 6f 73 74 fd fd 00 33 00 00 46 34 00 00 00 20 00 01 00 00 00 02 09 fd 14 51 fd 58 5f 0f 3c fd 00 03 03	OTTO`BASEe]FCFFFT|DSIGGDEF@GPOSx8GSUB],JOS/2EP`cmapspB3fheadh6hhea3$$hmtx:%Bmaxp PHname:,]post3F4QX_<	success or wait	6	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\System.Net.Http.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 6f fd 5c 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 02 00 00 22 00 00 00 00 00 00 b9 02 00 00 20 00 00 00 fd 02 00 00 00 fd 61 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 03 00 00 02 00 00 fd fd 03 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELo\" 0" a `	success or wait	10	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\athcfg20U.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 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 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 51 fd 5a fd 30 fd 09 fd 30 fd 09 fd 30 fd 09 fd 16 fd 09 fd 30 fd 09 fd 2c fd 09 fd 30 fd 09 fd 2f fd 09 fd 30 fd 09 28 2c fd 09 fd 30 fd 09 fd 2f fd 09 fd 30 fd 09 fd 2f fd 09 fd 30 fd 09 fd 30 fd 09 fd 31 fd 09 51 13 fd 09 fd 30 fd 09 fd 16 fd 09 fd 30 fd 09 6c 36 fd 09 fd 30 fd 09 fd 16 fd 09 fd 30 fd 09 54 10 fd 09 fd 30 fd 09 52 69 63 68 fd 30 fd 09 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$QZ0000,0/0(,0/0/001Q00l600T0Rich0	success or wait	16	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\audio-volume-high.png	0	725	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 02 fd 49 44 41 54 78 01 fd fd 03 74 fd 60 10 fd fd 70 fd fd b6 fd 45 6d fd 6b fd 6d fd 38 f6 6d f6 6d fd 37 fd 39 fd 6d 34 fd fd 4b fd fd 24 62 62 62 fd 7d 0f fd 54 39 0f fd fd fd fd 6b fd fd fd 11 16 fd 0b fd fd 4d 75 05 fd a4 fd fd 1e 5d fd 20 fd 2d 28 fd 12 fd 38 6f 38 fd 42 fd 5e 1f 42 fd 18 fd fd 34 72 fd fd 65 fd fd fd 36 fd 63 fd fd 08 fd fd 42 3d fd fd fd fd fd 5b 50 5d 60 44 1f 9d fd fd 41 fd 2a 57 fd 5d 73 fd fd fd fd 67 ac 21 10 0a fd 7a fd 1f 3f 3c 77 fd fd fd 6f ff fd 5c 25 fd fd 72 fd fd fd 61 fd 29 13 1e 58 fd 4e fd 79 08 7f fd 75 fd 68 fd 03 21 fd fd fd 72 fd fd 5f fd 52 fd fd 7d 07 76 7f 7b fd fd 29 fd	PNGIHDRaIDATxt`pEmkm8mm79m4K$bbb}T9kMu]-(8o8B^B4re6cB=P]`DA*W]sg!z?<wo\%ra)XNyuh!r_R}v{)	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\battery-level-10-symbolic.symbolic.png	0	207	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd 53 31 0e fd 30 08 3c fd fd fd 5f fd 07 3e fd fd 71 33 26 6e fd fd 58 28 fd 26 46 fd 21 21 40 fd 16 fd fd 02 38 01 fd fd 1d fd 62 fd 57 fd 2e fd 72 fd 60 2a 74 0e 7c fd 7f fd 14 61 34 6c fd fd fd 0b 26 fd 19 7c fd 42 0b fd fd 36 03 46 02 fd 27 59 6b 24 fd fd 19 1a 65 5f 61 fd 79 06 fd 49 fd fd 16 38 fd 44 fd fd 7e 06 fd 3d fd 39 17 62 04 65 45 2f fd 09 fd fd 35 fd 78 01 42 fd 42 fd 4f 1b 22 4a 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8S10<_>q3&nX(&F!!@8bW.r`*t|a4l&|B6F'Yk$e_ayI8D~=9eE/5xBBO"JIENDB`	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\edit-clear-rtl.png	0	255	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 fd 49 44 41 54 78 01 53 43 fd 43 51 10 fd 7b fd 6d 65 14 3b fd fd fd 1d fd 36 1f fd 61 fd 3b fd fd 41 fd fd fd 78 5f fd fd 2a fd 1e fd fd 39 5c 1e fd fd fd fd 6f 7f fd 0d 38 2e 3e 08 59 03 fd 49 fd 49 fd fd fd fd 6d 21 fd fd 42 4a fd 0c fd 43 fd 75 fd 28 fd 48 fd 48 fd 57 0d fd 06 55 3f fd fd fd 77 fd 4e fd 01 0c fd 29 41 50 28 64 61 10 fd fd 3b fd 38 6b 00 7f fd 6e 37 fd 7d 08 61 fd 6a fd fd fd fd fd 43 fd 64 0d 60 30 69 7b fd 72 fd fd 62 31 47 7a fd fd 77 32 20 fd 49 42 48 3c fd 54 60 fd fd 3b fd 11 fd fd 78 20 fd 65 60 fd 4f 7b fd 57 fd 0b 37 fd fd fd 57 fd fd 4f 3f fd 63 24 2b 1d fd 38 fd fd fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRaIDATxCCQ{me;6a;Ax_*9\o 8.>YIIm!BJCu(HHWU? wN)AP(da;8k7 }ajCd`0i{rb1Gzw2 IBH<T`;x e`O{W7WO? c$+8IENDB`	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\network-wireless-hotspot-symbolic.symbolic.png	0	274	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd fd 0d fd 30 10 45 5f 12 25 13 50 26 23 fd 64 04 36 fd 00 14 fd fd 33 03 0b 41 fd 00 43 04 42 fd 22 05 2d 74 fd 22 76 64 fd 63 11 fd 7d fd 64 fd fd fd 67 fd 0e fd 62 fd 42 34 fd 6b fd 10 fd 0b fd 0e fd 6c 78 00 57 27 fd 12 51 22 46 fd 4b 13 3b fd 65 7a 00 2b 44 fd fd 13 44 fd fd 53 fd fd 03 68 fd 31 62 fd fd 22 fd fd 77 fd 45 07 0b 54 60 75 40 fd 10 63 fd 73 fd fd 23 2b 00 fd 3c fd fd 7c fd fd 03 fd 62 11 51 1c 38 5e 03 39 50 00 75 fd fd fd 73 fd 17 fd 0c 20 54 fd 00 fd 57 fd 41 fd fd fd fd fd 02 0b 18 32 07 56 17 17 50 fd 0e fd fd 07 fd fd fd 7b fd fd 2f fd 7f 01 7f	PNGIHDRasBIT|dIDAT80E_%P&#d63AB"-t"vdc}dgbB4klW'Q"FK;ez +DDSh1b"wET`u@cs#+ <|bQ8^9Pus TWA2VP{/	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vmmemctl.inf	0	2250	0d 0a 3b 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 3b 20 76 6d 6d 65 6d 63 74 6c 2e 69 6e 66 0d 0a 3b 0d 0a 3b 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 31 39 39 33 2d 31 39 39 39 2c 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 0d 0a 3b 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 31 39 39 2d 32 30 31 39 20 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 3b 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	;------------------------------------ ------------------------------------ ; vmmemctl.inf;; Copyright (c) 1993-1999, Microsoft Corporation; Copyright (c) 1999-2019 VMware, Inc. All rights reserved.;--------------------- ----------------------	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsaD009.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	unknown	512	success or wait	560	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	unknown	4	success or wait	65	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\farme.Fej5	unknown	2	success or wait	1023	40275E	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.20966.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Nonarguable.JAP	unknown	1048576	success or wait	1	72972C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Indianerhvding	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ESPOUSES	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ESPOUSES\Blehavers	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\ESPOUSES	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\ESPOUSES\Blehavers	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Indianerhvding	flbes	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ESPOUSES\Blehavers	Verdea209	unicode	Muntins147	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\ESPOUSES\Blehavers	Verdea209	unicode	Muntins147	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly