ID: 632606
Sample Name:
SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.26603
Cookbook: default.jbs
Time: 20:14:36
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.26603 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 7
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 9
Dropped Files 9
Created / dropped Files 10
C:\Users\user\AppData\Local\Temp\Adventure_12.bmp 10
C:\Users\user\AppData\Local\Temp\Lydabsorberende2.Eks 10
C:\Users\user\AppData\Local\Temp\Pilkedes4.AFM 10
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll 11
C:\Users\user\AppData\Local\Temp\applications-utilities-symbolic.svg 11
C:\Users\user\AppData\Local\Temp\camera-photo-symbolic.symbolic.png 11
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll 12
C:\Users\user\AppData\Local\Temp\resume-vm-default.bat 12
C:\Users\user\AppData\Local\Temp\wab32res.dll.mui 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Authenticode Signature 13
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 16
Possible Origin 16
Network Behavior 16
Statistics 16
System Behavior 16
Analysis Process: SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exePID: 7156, Parent PID: 2508 16
General 17
File Activities 17

File Created 17
File Deleted 19
File Written 19
File Read 23
Registry Activities 23
Key Created 23
Key Value Created 23
Disassembly 23

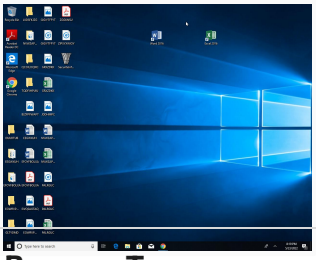
Windows Analysis Report

SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.26603

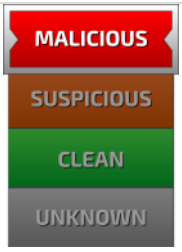
Overview

General Information

Sample Name:	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.26603 (renamed file extension from 26603 to exe)
Analysis ID:	632606
MD5:	09d431a8321ec7..
SHA1:	b709d7968897d7.
SHA256:	1be03967a61525.
Tags:	exe signed
Infos:	



Detection



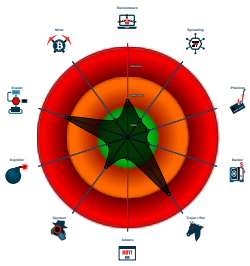
GuLoader

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 …
- Drops PE files
- Tries to load missing DLLs
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Binary contains a suspicious time s…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe (PID: 7156 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe" MD5: 09D431A8321EC75D7FF057787C319897)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://2.56.57.22/MY%20AIRTEL%20TELEGRAM%20STUB_iHQdRhQNdR56.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.883009053.0000000003140000.00000040.00001000.00020000.00000000.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

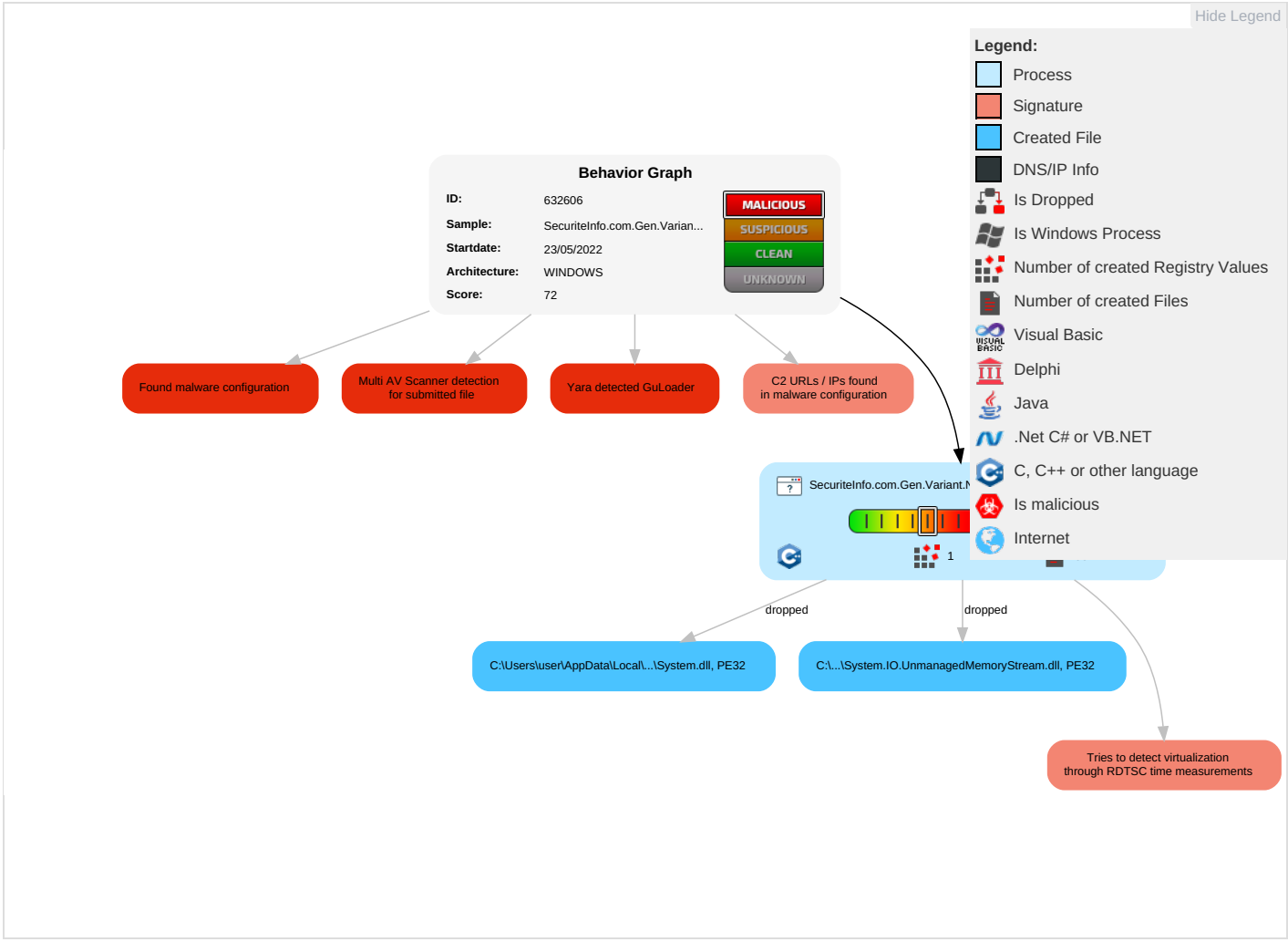
Malware Analysis System Evasion

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 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Timestomp	LSASS Memory	2 File and Directory 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)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	1 3 System Information Discovery	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)	1 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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.Gen.Variant.Nemesis.6939.7902.exe	22%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://2.56.57.22/MY%20AIRTEL%20TELEGRAM%20STUB_iHQdRhQNdR56.bin	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.22/MY%20AIRTEL%20TELEGRAM%20STUB_iHQdRhQNdR56.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctsca2021.crl0o	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://repository.certum.pl/ctnca.cer09	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://crl.certum.pl/ctnca.crl0k	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://subca.ocsp-certum.com05	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com02	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://repository.certum.pl/ctnca2.cer09	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://www.certum.pl/CPS0	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://https://github.com/dotnet/runtime	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe, 00000000.00000002.882784474.0000000002862000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe, 00000000.00000002.882292421.000000000040A000.00000004.00000001.01000000.00000003.sdmp, System.IO.UnmanagedMemoryStream.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:	632606
Start date and time: 23/05/202220:14:36	2022-05-23 20:14:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.26603 (renamed file extension from 26603 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:	20
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@1/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.7%) • Quality average: 87.7% • Quality standard deviation: 21.4%
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, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.54.113.53
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\Adventure_12.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	9906
Entropy (8bit):	7.910073068079041
Encrypted:	false
SSDEEP:	192:oXRlr7xecYaInXHtyMkC0RmLKZDjCYsPLcIXSZVYLuL:KRVUUIXgMkCSoe7tL
MD5:	A509568F18F3FF9C50EBFB2ACD499AA5
SHA1:	624E862D51655A6759151252963354F1520F0097
SHA-256:	5DDAFCD2247F1945099ECDE40D93F60C55D0B27F83D46B602909D55399BA635B
SHA-512:	32D090B101DC16D6A464C2D67D7870CD46E334031EE4ADE0F6255952CEB7141118C595FB8ADAF1ED04BFAB88CFAF9856A2AE5C5315AB9A9AF3E299816AEDC22
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....4.....s...*...`..Ki.#.....>N....H.).T... ."..S5..A..,.../W.3...|.q...1.;O...../.I.....2...oT..1...Y..;....be.Y.qE~w...,..w.....d.....q{ymo....D...V\K.H...F....,6....i...9..._. .....L....%....I..+.0..C\....bs.R....?....<W.3..+..._.W_...~.....f.....3i...F.".z.FkX..DF.....R.....?k

C:\Users\user\AppData\Local\Temp\Lydabsorberende2.Eks

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	data
Category:	dropped
Size (bytes):	23181
Entropy (8bit):	**7.990994965748802**
Encrypted:	**true**
SSDEEP:	384:84XmU94OtQbjBI9OrBQo6+inPK/smjmMA+9dFkj80lAug7woAR/vZKoF08HQDxFd:bb6jBqPocK/smBAGdFylld79/woCzN8U
MD5:	0D972D4681D2BDD6A506A86DA5A1C85E
SHA1:	84662467F7DA4A541729A3A2174E8373F7B7BBCD
SHA-256:	6303DF45ACDC13A98D4208F1A56AE86BB051ED3E6F2EEF4650ABCEDB34AEADFA
SHA-512:	9BEB7191CCF7B75255BA17AD11BF437864EC9471DC5DBE9FC9EAD3A8692A9C8E69246DA9A679F78A426184DDB7850E4875720D20423F2B2B53ACF313626AC8A
Malicious:	false
Reputation:	low
Preview:	......z.U...U.....[.b..BI.n.. H....D.....K:.|7.>43..wII.....!..!~Fr^"Q..b:...-.....y).s....e?....:.[.v)iz..G.Q...&.I>.\..O.J...E..C.....X..8.We}R.rH.b.....Q{.I.c..P&Q.;...y..<f".u>.M. ...u{v+.).....).9 .....G:.IH.V..0bsk..n.S[&$..Qpo....m.}.0LN.H!..t.(.....y!.....>o...P.....z{.?.e.=....b.....k$..~l7R@.....9..q_.....P...=..._.v...|..,U6....6....J1.8....$..`[...C...a$.... j..f.Y.k.w..+.3:V.Z...Gs.e(.*.F....^...a.....L$,....:V=._.^.b/.f..c...X.....d.....i....v=.Sc..t....{8.....P4..M.2.X9...g...{.52..a%y.6..'*\|8*.....!3~[.t.w...7w...M...a.j=....$u{...^..)J.J..-.I...)C7..J.p.a....#.IT.s1.0..K..#V.7.L.| .}..Z.Q\;..|.i.4..}H..!.I."?....C~.....%..n.b..E.3..P.....,.}. 5{.E....p.r)..L<.*.@zu7j..7h$DV.hO."...1..8U.[....r4.I$W.U.. M.$.i+...[..kEz.t;..<A..*[E..R.}z...a.3..,.,.E...!.5...f..FC...z.....g./..KK.r..(`..'...L.LC.....Ntz|..V+....}iK.;X/.},..Lp;-K.....~.Ro&40..."L..Zx....X..."-=t.^!...<

C:\Users\user\AppData\Local\Temp\Pilkedes4.AFM

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	data
Category:	dropped
Size (bytes):	85536
Entropy (8bit):	6.450553024590124
Encrypted:	false
SSDEEP:	768:qwz+WsmsiZUL3RDSQLefRLp3zFXs98T/ExDNnHBRXKiN9OOWp7wPkomrptIepi+s:qwz+wUjfLeLBXnLw/7gcPMIP+hO
MD5:	FC18E33AF950762F0854EE273723A9D5
SHA1:	CF2D571EF653FA35F961587296B26018F6D0C64A
SHA-256:	3C55B767A8B4E82B4607EF9CDC48C212D7CDAE3830E567F4A9C2C46A34E3BEAD
SHA-512:	E974480F6E9A96A69D46411A195E75BF8E32528417C7865C7847E9C6CDD4B712CECACC0C26C4800075947088D3617409C5BC3FF57119D819D2D7C0B18F55990
Malicious:	false
Reputation:	low

Preview:	f.u.f.f...f.t......&.U...................................4...f.i............pJ...............................f.........&?ix..:.n...............................f.d.......7..Pv............ ....f.k.........nz................................n.....f....43.R][[f.....f.........-"..!\\\f..M......f.n..3..:uu uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuf................6.[ao}}...f.........3n.5j..:F.........r..f .d..5.o.`................................................!............(.>.U..............................................f.q.7...4..e9...................................................................`F............................f.........`...... (X.Q,...f.n.

C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14440
Entropy (8bit):	6.682915152434376
Encrypted:	false
SSDEEP:	192:0BzGbXwRxx025WJ+WqlSWOL8/pCuPHnhWgN7aYWsB3gmZdGP2qnaj4FnH+a:oww7+25WJ+Wql+/uPHRN7BB3v3Llqea
MD5:	4075327E8E558810E05E67CE8E246864
SHA1:	F136E540C8439548EFF62BE1161F16A01CB0D060
SHA-256:	25211A075C941DFC9C363547A9EE4442981A4FBCA0C32EA705E94D086D57DAA3
SHA-512:	B557516E7121DEE78FA4D228FCF1351071D2AD6FC8F27142D4C6FB1B78F70DCB0993F8BE90F7247DBBEC3D3100307329F04F8EA90C9E93F7B618EFC7150D5A6 D
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....$.......PE..L.....x..........."!..0..............)... ....@.. ....P... ..`.................................\|)..O....@..................h$...`.......(..8.. ....H............text........ ....`.rsrc........@......................@..@.rel oc.......`......................@..B.................)......H........ ....P ....L....c.y.....>(#W..!...h...$...4V.I..4..w..?'....4a\..F..SG..rH.y......zy...:...C'..t$...6.? yrlQ..D..9...OM....<G.k....B.BSJB............v4.0.30319......`.......#~..<.......#Strings....,.......#GUID...<.......#Blob......................3...,............E........ ...p.......W.................^...+.^.....^...e.^.....^.....^.....^...L.^...Y.^................

C:\Users\user\AppData\Local\Temp\applications-utilities-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	606
Entropy (8bit):	4.666157566747791
Encrypted:	false
SSDEEP:	12:t4CDqW/ZWcdg+tKAPXUWU4NM0ByWoZLa8jCOopqGEA9A0/:t4CTg+tKA8WDec8YqGEAl/
MD5:	26B03DAAD39CD54B2343C49AF59F2091
SHA1:	D2C0728804B143D70A6BC6752A873BBA468C3E1D
SHA-256:	2EF30F51766DEAA27FECF4ECAF46404D0C37D902E39FE43E2F656CD488041FB2
SHA-512:	83C528C85B1F7067D134717AEC1638E8FA20E8DAA595E1FBA2F5ECEC747841E36B626C2026ECB61DE9F67A7E3C4D2B0992F71C11F76AA019D36A9E4C4A307C A1
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2.934 0h.132C4.692 0 6 1.332 6 2.986v10.028C6 14.668 4.692 16 3.066 16h-.132C1.308 16 0 14.668 0 13.014V2.986C0 1.332 1.308 0 2.934 0zm2.594 0c.878.714 1.469 1.793 1.469 3v1h2.125c-.075-1.092 1.248-2 2-2 .68 0 1 .012 1 1v1h1.218c1.229-.6 1.782-1.969 1.782-2.687 0-.736-2.386-1.312-3.688-1.312zM7 5v4.313c2.766 2.662 6.125 2.406 6.125 2.406s.353-1.52-1.906-4.03L8.844 5H7.063C7.04 5.003 7.02 4.999 7 5zm2.975 2.532L11.66 9.27c-1.8.166-2.151-.856-1.684-1.737z" style="marker:none" overflow="visible" color="#000" fill="#474747"/></svg>

C:\Users\user\AppData\Local\Temp\camera-photo-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	226
Entropy (8bit):	6.609529349840206
Encrypted:	false
SSDEEP:	6:6v/lhPysfQu6kkLKgiFG34McOULPqSax5na/p:6v/7FPk9iHMUeSauR
MD5:	AFE0B10777804AE446C5E4A3F3C2E3B5
SHA1:	0252C67682C9A5D7260BA70DC03E4091ED9A0923
SHA-256:	4C42D37B6A5ED6F3230A1506A6BC4687AEF8146174666C0BCCAD8FE2E6DD75B5
SHA-512:	D76318428038B81D1C29C5812BD22F53DFF53AE93FE86305CD76B750F39BD785EBB9CA69475137CE9A00A4DC588DB4D0C077B723AC847782123C3359E981A9E
Malicious:	false

Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1..P.C_.Aj.....O.A..KY.|...b.VS.7x...../...BG.n.z.Tu.....9.....X.V.pD....W...(...e...V...{..0...&...|2.l.+m..3..i..3.....?[. ...u....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.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
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\resume-vm-default.bat

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.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
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\wab32res.dll.mui

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	modified
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

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">.. ..body{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;margin: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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.737885668413826
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.Gen.Variant.Nemesis.6939.7902.exe
File size:	150224
MD5:	09d431a8321ec75d7ff057787c319897
SHA1:	b709d7968897d774676194b9708f304a6a472086
SHA256:	1be03967a615254ca0b3eba8b5aaa6b5f5c91c9f03d4fe2692b3675f93c0b26d
SHA512:	da58f66d20a061f973ce18c894d00279a5b47f8e49b09fd08a6f17ac9c42a806d857709c6e89e30ebe8b4d124a11c15df80459579ffe5ac751a7c80f5798c925
SSDEEP:	3072:AfY/TU9fE9PEtu22bTj/eZsl2JhPa0TeYFv8YARZ/KtWquoJTvJfS:WYa6LTkXPderR9KLLvJ
TLSH:	CAE3F1147770E8A3F9731B71AE7597A6AFB2EA021875974F13202A9C3D91380DB1D713
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.....Oa.....h...*.....

File Icon

Icon Hash:	9ad8d87078697939

Static PE Info

General

Entrypoint:	0x403640
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:	0x614F9B1F [Sat Sep 25 21:56:47 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:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Hovedbundens1 alerters SPORTELLNNEDE Bowenite ", O=neglecting, L=Myrtle, S=Mississippi, 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	• 5/23/2022 7:12:19 AM 5/23/2023 7:12:19 AM

Subject Chain	• CN="Hovedbundens1 alerters SPORTELLNNEDE Bowenite ", O=neglecting, L=Myrtle, S=Mississippi, C=US
Version:	3
Thumbprint MD5:	C16E17A3C8D303B21C04B936BB6E0DCB
Thumbprint SHA-1:	08759A518D93EEE4FA4E210966C67D44DAFF49A8
Thumbprint SHA-256:	DB0429D568507771A725F6E9BCCA1523C3D67F56B97DB4214D1703A8779161C1
Serial:	FE464BE9561F856B

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], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
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 00007F9C08D6EB0Ah
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
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F9C08D6EADAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], 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

Instruction
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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x53000	0x14d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x22c08	0x1ec8	.data
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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x28000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x53000	0x14d0	0x1600	False	0.302734375	data	3.56713195596	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x53208	0x8a8	data	English	United States
RT_DIALOG	0x53ab0	0x100	data	English	United States
RT_DIALOG	0x53bb0	0x11c	data	English	United States
RT_DIALOG	0x53cd0	0xc4	data	English	United States
RT_DIALOG	0x53d98	0x60	data	English	United States
RT_GROUP_ICON	0x53df8	0x14	data	English	United States
RT_VERSION	0x53e10	0x37c	data	English	United States
RT_MANIFEST	0x54190	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

DLL	Import
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, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, 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	Copyright 1997-2013, Nullsoft, Inc.
FileVersion	10.28.31
CompanyName	Thermo Electron Corporation
LegalTrademarks	StringFileInfo: U.S. English
Comments	VF Corporation
ProductName	Prudential Financial Inc.
FileDescription	LegalTrademarks,Nullsoft and Winamp are trademarks of Nullsoft, Inc.
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.Gen.Variant.Nemesis.6939.7902.exe PID: **7156**, Parent PID: **2508**

General

Target ID:	0
Start time:	20:15:44
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe"
Imagebase:	0x400000
File size:	150224 bytes
MD5 hash:	09D431A8321EC75D7FF057787C319897
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: 00000000.00000002.883009053.0000000003140000.00000040.00001000.00020000.00000000.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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsdEA1F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsdEA20.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	4	405C22	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	4	405C22	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	4	405C22	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	4	405C22	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	4	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsyEAEC.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	405BE2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	2	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\adits	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\adits\Virginalets80	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\adits	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\adits\Virginalets80	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405C22	CreateDirectoryW
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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Pilkedes4.AFM	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Adventure_12.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Lydabsorberende2.Eks	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\applications-utilities-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\camera-photo-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\resume-vm-default.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\wab32res.dll.mui	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsjF964.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	488	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsdEA1F.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsyEAEC.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsyEAEC.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 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	406224	WriteFile
unknown	47241	24639	75 6e 6b 6e 6f 77 6e	unknown	success or wait	6	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Pilkedes4.AFM	0	16384	66 0f 75 fd 66 0f 66 fd fd 66 0f 74 fd fd fd fd fd 26 fd 55 fd 01 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 34 00 fd fd 66 0f 69 fd fd fd fd fd fd fd fd fd 1f fd 03 70 4a 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 66 0f fd fd fd 5b fd fd fd 2e 26 3f 69 78 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 fd fd fd 0f fd fd fd fd 0f fd fd fd fd fd fd 1d fd 3a fd 6e fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0f fd fd fd 0f fd fd 66 0f 64 fd fd fd 0f fd fd fd 37 fd fd 50 76 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	fuffft&U4fipJf.&?ix:nfd7Pv	success or wait	6	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Adventure_12.bmp	0	9906	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Lydabsorberende2.Eks	0	16384	25 fd fd fd fd 17 7a fd 55 09 fd fd 55 fd fd fd fd fd fd 5b fd 62 fd fd 42 49 fd 6e fd 07 20 48 fd fd fd 09 44 fd 18 2e fd 03 11 00 fd fd 4b 3a fd 7c 37 0e 3e 34 33 fd fd 77 49 49 fd 1c fd fd fd fd 21 fd fd 21 7e 46 72 5e 22 51 03 fd 62 3a 1c 5b fd 2d fd 16 fd 13 04 79 29 fd 73 fd 00 fd fd 65 3f fd fd fd 3a c5 5b 1d 76 29 69 7a fd fd 47 fd 51 fd c5 fd 26 fd 49 3e fd 5c fd 0c 4f fd 4a fd fd fd 45 fd fd 43 fd fd fd fd fd 58 18 fd 38 fd 57 65 7d 52 10 72 48 0d 62 1c fd 2e fd 1f fd fd fd 0a fd fd fd fd fd fd fd 03 51 7b fd 49 fd 63 16 fd 50 26 51 fd 3b fd 06 fd 79 fd fd 3c 66 22 fd 75 3e fd 4d fd fd 17 e8 75 7b 76 2b 69 29 fd 17 fd 0c 18 15 1a fd fd fd 29 17 39 20 fd 40 1f fd fd fd 47 3a fd 49 48 fd 56 fd	zUU[bBIn HD.K:|7>43wII!!~Fr^"Qb:-y)se?:[v)izGQ&I>\OJECX8We}R rHb.Q{IcP&Q;y<f"u>Mu{v+))9 G:IHV	success or wait	12	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	0	14440	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 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 fd 78 fd 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 30 00 00 0a 00 00 00 08 00 00 00 00 00 00 fd 29 00 00 00 20 00 00 00 00 00 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 fd 00 00 00 02 00 00 50 15 01 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.$PELx"!0) @ P`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\applications-utilities-symbolic.svg	0	606	3c 73 76 67 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 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 70 61 74 68 20 64 3d 22 4d 32 2e 39 33 34 20 30 68 2e 31 33 32 43 34 2e 36 39 32 20 30 20 36 20 31 2e 33 33 32 20 36 20 32 2e 39 38 36 76 31 30 2e 30 32 38 43 36 20 31 34 2e 36 36 38 20 34 2e 36 39 32 20 31 36 20 33 2e 30 36 36 20 31 36 68 2d 2e 31 33 32 43 31 2e 33 30 38 20 31 36 20 30 20 31 34 2e 36 36 38 20 30 20 31 33 2e 30 31 34 56 32 2e 39 38 36 43 30 20 31 2e 33 33 32 20 31 2e 33 30 38 20 30 20 32 2e 39 33 34 20 30 7a 6d 32 2e 35 39 34 20 30 63 2e 38 37 38 2e 37 31 34 20 31 2e 34 36 39 20 31 2e 37 39 33 20 31 2e 34 36 39 20 33 76 31 68 32 2e 31 32 35 63 2d 2e	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2.934 0h.132C4.692 0 6 1.332 6 2.986v10.028C6 14.668 4.692 16 3.066 16h-.132C1.308 16 0 14.668 0 13.014V2.986C0 1.332 1.308 0 2.934 0zm2.594 0c.878.714 1.469 1.793 1.469 3v1h2.125c-.	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\camera-photo-symbolic.symbolic.png	0	226	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 51 31 0e fd 50 0c 43 5f fd 41 6a fd 14 fd 0b 12 fd 07 2e fd 0e 1f 83 0e fd fd 4f 13 41 fd 0a 4b 59 fd 7c fd 87 fd 62 02 56 53 fd 37 78 09 04 80 fd fd 2f fd fd 11 42 47 fd 6e 02 7a fd 54 75 fd fd 39 02 09 fd 39 ef fd fd 0a fd fd fd fd 0b 58 fd 56 fd 70 44 fd 14 fd 18 57 00 fd 15 28 fd 0d 6f 65 fd fd fd 56 2e 12 08 7b 1c fd 30 fd 1d 22 26 fd 15 0a 7c 32 0f 6c fd 2b 6d fd fd 33 fd fd 69 fd fd 33 fd fd 7f fd 06 fd 3f 5b fd 08 fd 07 75 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT81 PC_Aj.OAKY |bVS7x/BGnzTu9XVpDW (eV.{0&|2l+m3i3? [uIENDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\resume-vm-default.bat	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	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wab32res.dll.mui	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	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	unknown	512	success or wait	84	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsdEA20.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsdEA20.tmp	unknown	19976	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsdEA20.tmp	unknown	4	success or wait	14	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	unknown	16384	success or wait	6	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Lydabsorberende2.Eks	unknown	2	success or wait	345	40275E	ReadFile
C:\Users\user\AppData\Local\Temp\Pilkedes4.AFM	unknown	1048576	success or wait	1	72492C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Architectonica49	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Architectonica49\Ukraine93	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Architectonica49\Ukraine93	Expand String Value	expand unicode	%WINDIR%\alioth.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly