ID: 632606
Sample Name:
SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
Cookbook: default.jbs
Time: 21:02:03
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

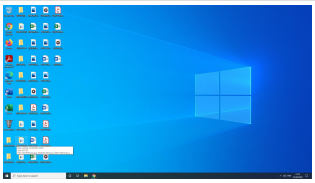
Windows Analysis Report

SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe

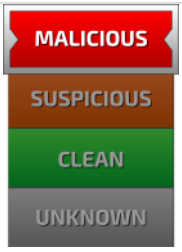
Overview

General Information

Sample Name:	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
Analysis ID:	632606
MD5:	09d431a8321ec7..
SHA1:	b709d7968897d7.
SHA256:	1be03967a61525.
Infos:	



Detection



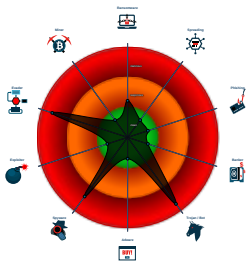
AgentTesla, GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe (PID: 8408 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe" MD5: 09D431A8321EC75D7FF057787C319897)
  - CasPol.exe (PID: 8888 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 3104 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 376 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1972606022",
  "Chat URL": "https://api.telegram.org/bot1977970812:AAHd8pA2REAwdAB_6eJ-9nZj90oz8OYGjrI/sendDocument"
}
```


Threatname: GuLoader


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


Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot1977970812:AAHd8pA2REAwdAB_6eJ-9nZj90oz8OYGjrI/sendMessage"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.1265287486.0000000000F00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.1924258276.00000000032A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 3 entries

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 Any.run

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

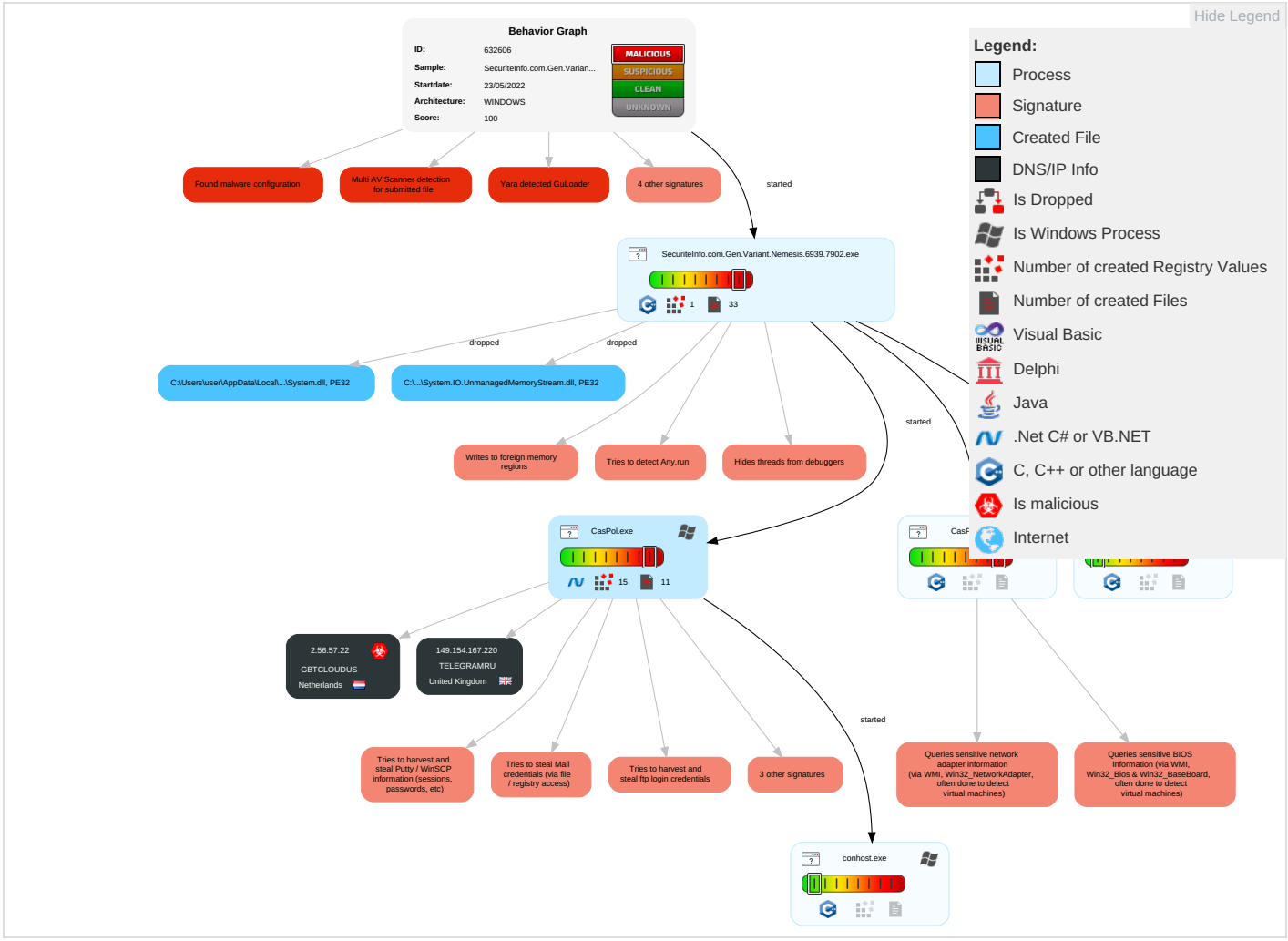
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 Access Token Manipulation	1 Disable or Modify Tools	2 OS Credential Dumping	4 3 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	3 5 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	3 5 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Timestomp	Cached Domain Credentials	1 1 7 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.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%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.IO.UnmanagedMemoryStream.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nse53CA.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nse53CA.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
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%	Avira URL Cloud	safe	
http://kUYmnxF1L3RMXTOEA.ne	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://kUYmnxF1L3RMXTOEA.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://zFeqMl.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

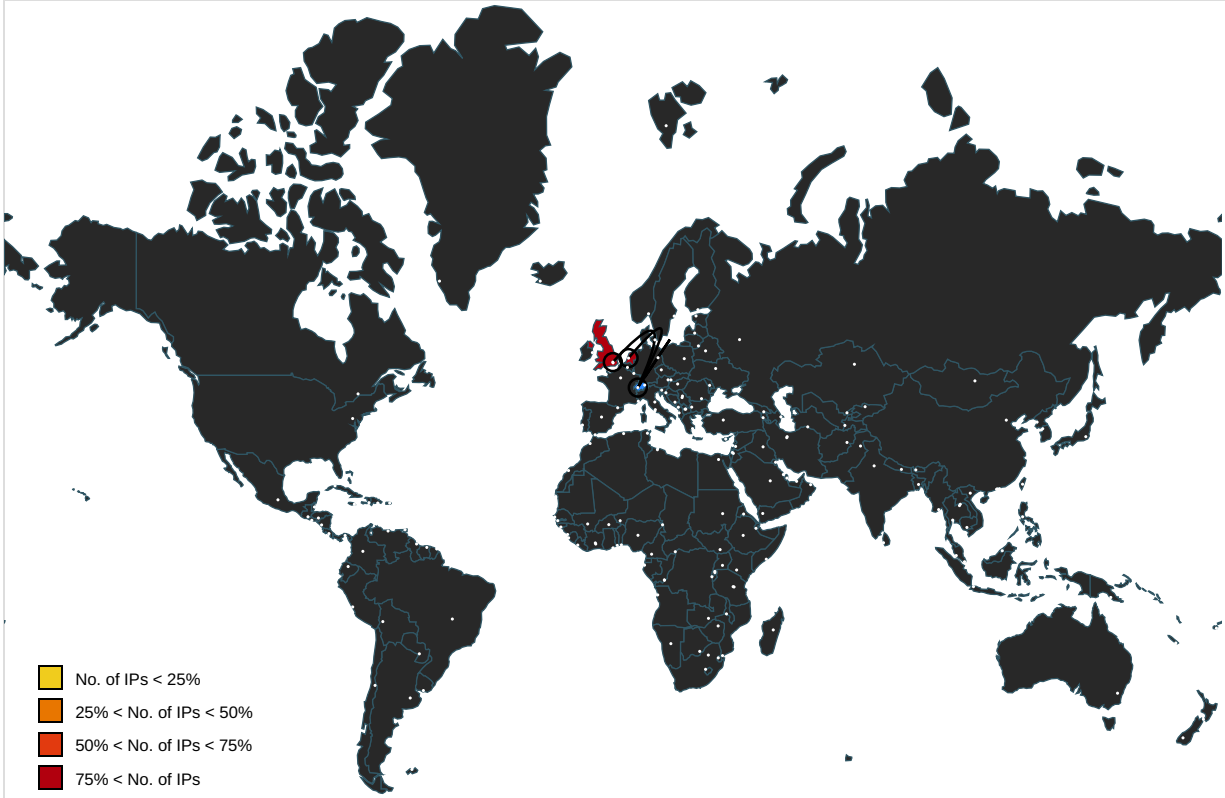
Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.22/MY%20AIRTEL%20TELEGRAM%20STUB_iHQdRhQNdR56.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.certum.pl/ctsca2021.crl0o	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://https://api.telegram.org/bot1977970812:AAHd8pA2REAwdAB_6eJ-9nZj90oz8OYGjrI/sendDocumentdocument-----	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://repository.certum.pl/ctnca.cer09	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://https://api.telegram.org	CasPol.exe, 0000000C.00000002.6153695657.000000001D6DD000.00000004.00000800.00020000.00000000.sdmp	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	• Avira URL Cloud: safe	unknown
http://kUYmnxF1L3RMXTOEA.ne	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false	• Avira URL Cloud: safe	unknown
http://kUYmnxF1L3RMXTOEA.net	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000C.00000002.6153633788.000000001D6D9000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000C.00000003.1443175396.000000001C411000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://zFeqMl.com	CasPol.exe, 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: 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://https://api.telegram.org/bot1977970812:AAHd8pA2REAwdAB_6eJ-9nZj90oz8OYGjrI/sendDocument	CasPol.exe, 0000000C.00000002.6153695657.000000001D6DD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe	false		high
http://api.telegram.org	CasPol.exe, 0000000C.00000002.6153855558.000000001D6F2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 0000000C.00000002.6153695657.000000001D6DD000.00000004.00000800.00020000.00000000.sdmp	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, 00000000.00000002.1921654388.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe, 00000000.00000002.1923518409.0000000002876000.00000004.00000800.00020000.00000000.sdmp, System.IO.UnmanagedMemoryStream.dll.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	unknown	United Kingdom		62041	TELEGRAMRU	false
2.56.57.22	unknown	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632606
Start date and time: 23/05/202221:02:03	2022-05-23 21:02:03 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	33

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/10@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.3% (good quality ratio 27.9%) • Quality average: 87.8% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, BackgroundTransferHost.exe, UserOOBEBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe, MusNotificationUx.exe
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:04:32	API Interceptor	2796x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\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:oXRlr7xecYaInXHtyMkC0RmLKZDjCYsPLclXSZVYLuL:KRVUUIXgMkCSoe7tL
MD5:	A509568F18F3FF9C50EBFB2ACD499AA5
SHA1:	624E862D51655A6759151252963354F1520F0097
SHA-256:	5DDAFCD2247F1945099ECDE40D93F60C55D0B27F83D46B602909D55399BA635B
SHA-512:	32D090B101DC16D6A464C2D67D7870CD46E334031EE4ADE0F6255952CEB7141118C595FB8ADAF1ED04BFAB88CFAF9856A2AE5C5315AB9A9AF3E299816AEDC22
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....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
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

<table>
<tr><td>Preview:</td><td>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.</td></tr>
</table>

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

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>14440</td></tr>
<tr><td>Entropy (8bit):</td><td>6.682915152434376</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:0BzGbXwRxx025WJ+WqlSWOL8/pCuPHnhWgN7aYWsB3gmZdGP2qnaj4FnH+a:oww7+25WJ+Wql+/uPHRN7BB3v3Llqea</td></tr>
<tr><td>MD5:</td><td>4075327E8E558810E05E67CE8E246864</td></tr>
<tr><td>SHA1:</td><td>F136E540C8439548EFF62BE1161F16A01CB0D060</td></tr>
<tr><td>SHA-256:</td><td>25211A075C941DFC9C363547A9EE4442981A4FBCA0C32EA705E94D086D57DAA3</td></tr>
<tr><td>SHA-512:</td><td>B557516E7121DEE78FA4D228FCF1351071D2AD6FC8F27142D4C6FB1B78F70DCB0993F8BE90F7247DBBEC3D3100307329F04F8EA90C9E93F7B618EFC7150D5A
D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Antivirus:</td><td>• Antivirus: Metadefender, Detection: 0%, Browse
• Antivirus: ReversingLabs, Detection: 0%</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....x..........."!..0..............)... ....@.. ....P...
..`................................|)..O....@.................h$...`.......(..8.. ....H...........text........ ....`.rsrc........@......................@..@.rel<br>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.^................</td></tr>
</table>

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

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe</td></tr>
<tr><td>File Type:</td><td>SVG Scalable Vector Graphics image</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>606</td></tr>
<tr><td>Entropy (8bit):</td><td>4.666157566747791</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:t4CDqW/ZWcdg+tKAPXUWU4NM0ByWoZLa8jCOopqGEA9A0/:t4CTg+tKA8WDec8YqGEAl/</td></tr>
<tr><td>MD5:</td><td>26B03DAAD39CD54B2343C49AF59F2091</td></tr>
<tr><td>SHA1:</td><td>D2C0728804B143D70A6BC6752A873BBA468C3E1D</td></tr>
<tr><td>SHA-256:</td><td>2EF30F51766DEAA27FECF4ECAF46404D0C37D902E39FE43E2F656CD488041FB2</td></tr>
<tr><td>SHA-512:</td><td>83C528C85B1F7067D134717AEC1638E8FA20E8DAA595E1FBA2F5ECEC747841E36B626C2026ECB61DE9F67A7E3C4D2B0992F71C11F76AA019D36A9E4C4A307C
A1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td><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></td></tr>
</table>

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

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

C:\Users\user\AppData\Local\Temp\nse53CA.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: 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 id ="content">.. <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">.. ..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 id ="content">.. <div class="co

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

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	• 23/05/2022 15:12:19 23/05/2023 15:12:19
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 00007F73D05E5BEAh
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 00007F73D05E5BBAh
and word ptr [ebp-00000132h], 0000h

Instruction
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
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

Name	RVA	Size	Type	Language	Country
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
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

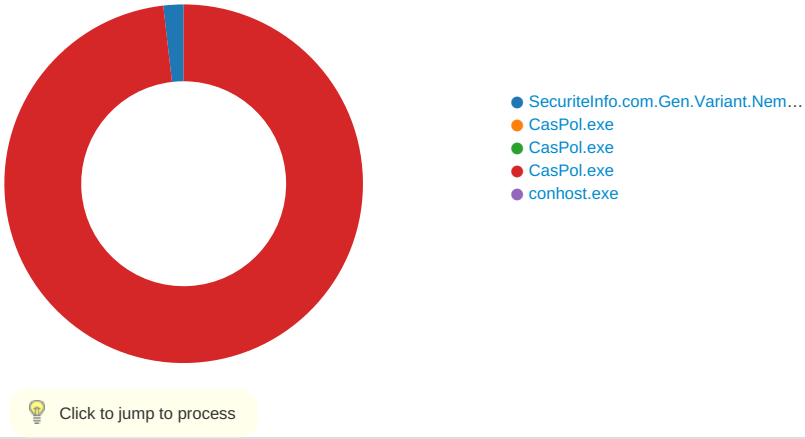
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe PID: **8408**, Parent PID: **6772**

General

Target ID:	0
Start time:	21:03:58
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: 00000000.00000002.1924258276.00000000032A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **8888**, Parent PID: **8408**

General

Target ID:	10
Start time:	21:04:15
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe"

Imagebase:	0x2b0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **3104**, Parent PID: **8408**

General

Target ID:	11
Start time:	21:04:16
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe"
Imagebase:	0x190000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **376**, Parent PID: **8408**

General

Target ID:	12
Start time:	21:04:16
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Nemesis.6939.7902.exe"
Imagebase:	0xa80000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000000.1265287486.0000000000F00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000C.00000002.6152117405.000000001D5A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC33263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC33263	unknown
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	6DC33263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC33263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CB99B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CB99B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC3099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC3D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC3D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DB862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB99B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CB99B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC3099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DB862DE	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB99B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CB99B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DC3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DC3099B	unknown
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CB99B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	6	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\a1cf1e70-4a2c-4749-a655-838520c71481	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CB99B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CB99B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	6BEBFDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	6BEBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BEBFDB8	unknown

Analysis Process: conhost.exe PID: **3384**, Parent PID: **376**

General

Target ID:	13
Start time:	21:04:16
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70de00000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly