ID: 634320
Sample Name:
SecuriteInfo.com.generic.ml.10062.6710
Cookbook: default.jbs
Time: 22:33:09
Date: 25/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

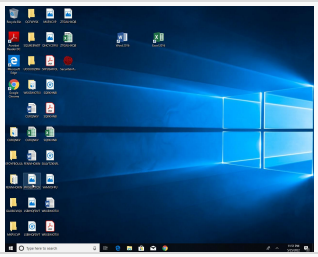
Windows Analysis Report

SecuriteInfo.com.generic.ml.10062.6710

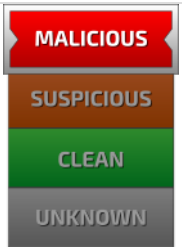
Overview

General Information

Sample Name:	SecuriteInfo.com.generic.ml.10062.6710 (renamed file extension from 6710 to exe)
Analysis ID:	634320
MD5:	95050a1e0c7d4c..
SHA1:	baa57d1bf6d8a4..
SHA256:	458597ef683513..
Tags:	exe
Infos:	



Detection



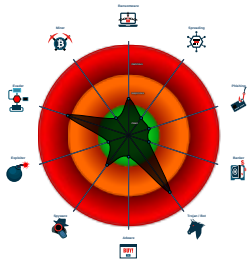
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.generic.ml.10062.exe (PID: 6288 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe" MD5: 95050A1E0C7D4C57F62E26967B3B0BFD)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://2.56.57.22/yendexoriginwithoutfilter_rtSDhNF87.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.761431234.0000000003170000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

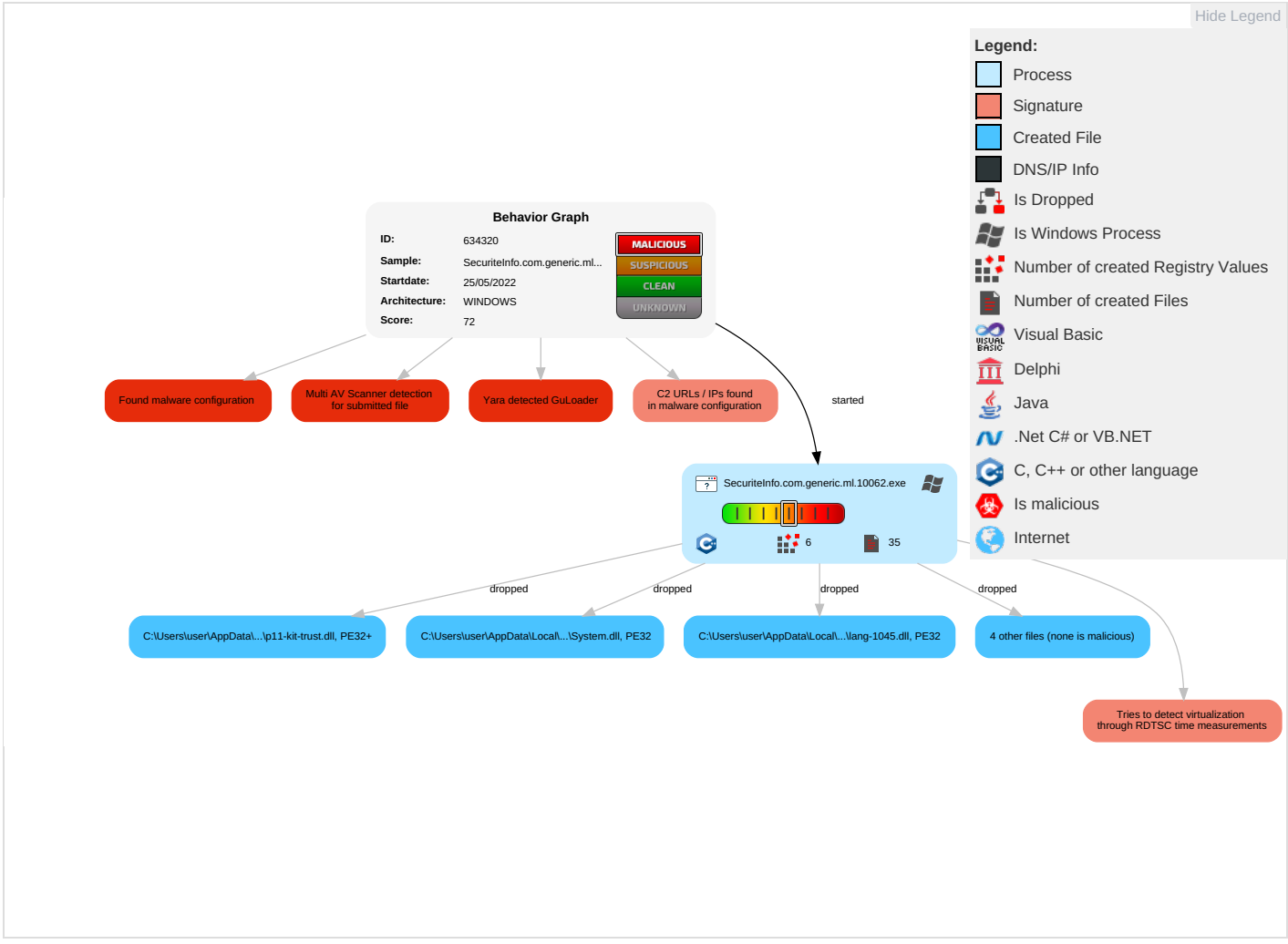
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Obfuscated Files or Information	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Timestomp	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

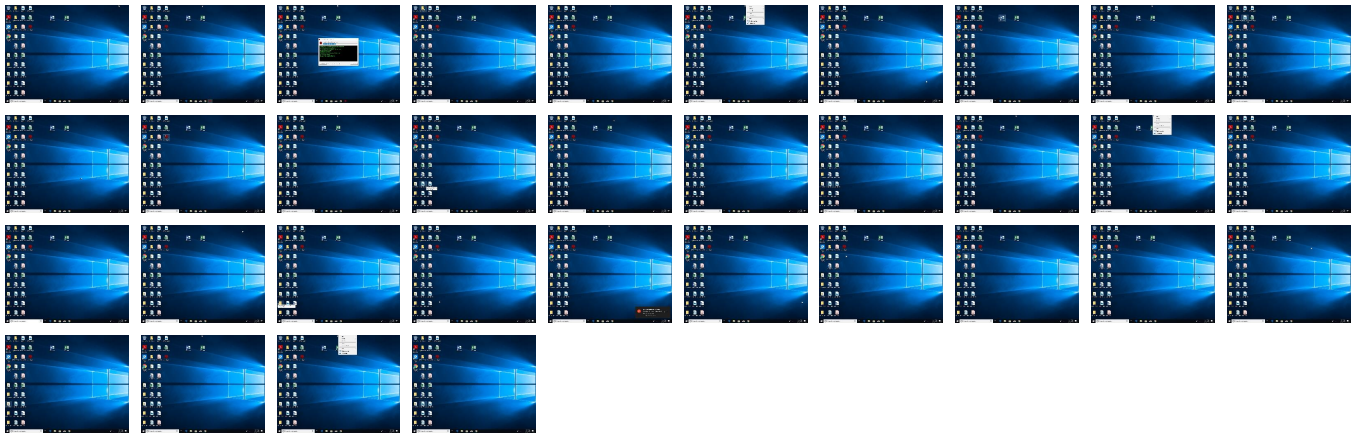
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.generic.ml.10062.exe	12%	Virustotal		Browse
SecuriteInfo.com.generic.ml.10062.exe	7%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0%	Virustotal		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://2.56.57.22/yendexoriginwithoutfilter_rtSDhNF87.bin	2%	Virustotal		Browse
http://2.56.57.22/yendexoriginwithoutfilter_rtSDhNF87.bin	0%	Avira URL Cloud	safe	
http://www.avast.com0/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.22/yendexoriginwithoutfilter_rtSDhNF87.bin	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctsca2021.crl0o	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://creativecommons.org/licenses/by-sa/4.0/	folder-publicshare.png.0.dr	false		high
http://repository.certum.pl/ctnca.cer09	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, avutil-54.dll.0.dr	false		high
http://repository.certum.pl/ctsca2021.cer0	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://crl.certum.pl/ctnca.crl0k	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://subca.ocsp-certum.com05	SecuriteInfo.com.generic.ml.10062.exe	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, avutil-54.dll.0.dr	false		high
http://ocsp.thawte.com0	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, avutil-54.dll.0.dr	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com02	SecuriteInfo.com.generic.ml.10062.exe	false	• URL Reputation: safe	unknown

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nero.com	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, avutil-54.dll.0.dr	false		high
http://subca.ocsp-certum.com01	SecuriteInfo.com.generic.ml.10062.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://repository.certum.pl/ctnca2.cer09	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://www.avast.com0/	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, lang-1045.dll.0.dr	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://www.symauth.com/cps0(	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.761266919.0000000002AE3000.00000004.00000800.00020000.00000000.sdmp, avutil-54.dll.0.dr	false		high
http://www.certum.pl/CPS0	SecuriteInfo.com.generic.ml.10062.exe	false		high
http://https://github.com/dotnet/runtime	SecuriteInfo.com.generic.ml.10062.exe, 00000000.00000002.760785382.0000000002830000.00000004.00000800.00020000.00000000.sdmp, System.IO.FileSystem.Watcher.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634320
Start date and time: 25/05/202222:33:09	2022-05-25 22:33:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.generic.ml.10062.6710 (renamed file extension from 6710 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/14@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.8% • Quality standard deviation: 21.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, time.windows.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1955040
Entropy (8bit):	6.826653374498559
Encrypted:	false
SSDEEP:	49152:T3VwASOuGtlq2flU6iFm7+BSGYsFoXOh5PGP1T/eacB4dPFPxat:vw+FDKXkuLPxS
MD5:	39981C2A1465413B506246DA3721D9A1
SHA1:	213C41C908F9A7C62C4D5D8079FC17188066CB3B
SHA-256:	19AE2C74ECE76F6AE7074AC31B198D6BF201DDE201B5B31EACA023877241F7B9
SHA-512:	F047681FF16D7C428E39D6A705BDD290B7EA227AC8176E69B989B90297541CD2A596B71673E6DFA0ACB83B201EB815E0518D52169D9FC48C6AEBF78DCB998DD
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8.}.k.}.k.}.k..Rk.}.k...j.}.k...j.}.k...j.}.k...j.}.k...j.}.k.}.k.|.k.} .k.}.kg..j3|.kf..j.}.kf.>k.}.k.}Vk.}.kf..j.}.kRich.}.k.....PE..d....j.`.....".....@.....0.....`.....c..... .....L.....p.....@..... .....text..... ..`.rdata..*j... ...I.....@..@.data...0e.....".z.....@....pdata..... .....@..@.rsrc.....b.....@..@.reloc...L.....N...h.....@..B.....

C:\Users\user\AppData\Local\Temp\Ddsstivhed9.non

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	data
Category:	dropped
Size (bytes):	13978
Entropy (8bit):	7.983903298012058
Encrypted:	false
SSDEEP:	384:g/fHDCOQD/zKzAwhZMiZY79lBpsIyK0Xqv:g/fjdQTzKzBhZMw+IfsIyBW
MD5:	6CEA9045463D0C5D27E1A89AE139E33F
SHA1:	64A5497F8D154AEEF22F7CAC3F72F4D2FC5F9D62
SHA-256:	D532BF8700F1B322DCF738AF6EF2DAB7FE5328DCBA0C4ED04227AF6BA4F1A1BD
SHA-512:	B20D641DD59247BE2E75EA0F96408949EFE40864058B3D0938E3DBFA2F8AC960CB2F2E52E62FBE42DEC2C93EF4D9B89CF44BA31E102C3BBB7C3B726EDE77B ACA
Malicious:	false
Reputation:	low
Preview:	..8S/or.>;.K4C...Z.r7..0Yk.A.>....X\.{....Q...9.2..J|.0.a.8...h.v.m.?X.f.1....F&..y;..3.1../..eH.L.~...@..Fs6H..b..x....AA.q.+.j.z|.....g.&n...9..B.s.....I.....R...m.*1...f?.....W... ..~}._..M.r.....}}:.....%.7...7....9.....(.$.|r6...~8..3.p!xM2.....m..9..C..Us.8..+.lp+.e'..x.g.....9....x.?.}.q.\...`.....0...M'2..}(\|.=.uB..k..}..=:.BG\..?.P.a.!.V....v.....?.>.....zG..... d.D.jP..wD.pM..{h....'T.....>Fy.9.K.Q...af....Fyra.\...Pe..G.oR.d...a5.\|...FPTT{["..;hz`....(....9..r.[]F.$.A+bdz....'&TeQ.G?..7...f.O{.a!!?...[X?.j+.[9 ....QL}!u...1/:>.:6%.6.A....N. ...#..1.8P.2Q,.QYxk'.2D.....C?..g....Y..z3W...h..5..L.i....m..a.5.$.....z...S...'lB..S.....F.e...>.8.....\|.6.*.-srN&.]....s.....Lou:z..h..v.-..9.K....^.G.Qc..G.'.s....=U.-....''..ja..7.Oj..[.k,. ti(.-p.\|....8..g...y..`.....Q`X.....cT.I.*...6.r..$.....&.....1J.....R.#..-U..h.B.....L../../{Kk.....f....g%.....#..["....lj..P..N...F.".0.'..H:U.JowM./L.....Q.3

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun D ec 31 23:06:32 1600, length=0, window=hide
Category:	modified
Size (bytes):	960
Entropy (8bit):	3.032437182506048
Encrypted:	false
SSDEEP:	12:8wl0YsXowAOcQ/tz+7RafgKDq9XKNPRKQ18/3NJkKAd4t2Y+xIBjK:8XLDaRMgKsKt9S9HAv7aB
MD5:	01CA7DE8916567057D034EA4F9D7CF05
SHA1:	718CA646F335D986482BF4B0F3A4C0DEC38EF5AA
SHA-256:	BA6C443CEAC015CFEC4589BB445C52AC1DA3411BF3357FE0D55B62081B169361
SHA-512:	1A1D64966B0B2F85BA663E37F71EB76191A703A3C07F2B827BD109BB3765416D23C9350FD1FDBA5EF0B75B8F5B0E09470811148A17C6C361138ECEB7F3CD3B8 9
Malicious:	false
Reputation:	low
Preview:	L.....F.....;....P.O. .:i....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....j.o.n.e.s.....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.....x.2.....Unoppignorated.exe..V.....U.n.o.p.p.i.g.n.o.r.a.t.e.d...e.x.e..."......\.U.n.o.p.p.i.g.n.o.r.a.t.e.d...e. x.e.!.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.- .2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	20008
Entropy (8bit):	6.8686823517057265
Encrypted:	false
SSDEEP:	384:xWgEHWp1v7S+10QnqiZwtfXbMpBjn0aq8f0DBRJYHClXLRXoS:nEijw8Be1PqspoS
MD5:	797476E8813090CC62D574BB9B59F2DD
SHA1:	BDBBBFD1B3B2E8B2CCF368815DCF06247FC08C14
SHA-256:	85C2314ECAA192D438DEBFAB7490E047C7780EB59A115DFEB68E36BF84CFAC22
SHA-512:	42A6AC5750DC4F8D533AD03098348732519AE27C0EE002C4B5953205D5108EAE24C09BFFD587874FCB1DA422152A5B71DD778B58BFA760683C0A565B09C7F93
Malicious:	false

Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....+..... .....0.....c....`..... ..P.....(<.....8.....rdata..... ....@..@.rsrc...P.... .....@..@.....+.....T...8...8.....+.....$.....8....rdata..8...x....rdata$zzzdbg.... ..0....rsrc$01....0!.. ....rsrc$02.... ....n->..;..^.....=1. [.$H.m...+..... .....

C:\Users\user\AppData\Local\Temp\Sognefogedernes.Run6

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	data
Category:	dropped
Size (bytes):	85509
Entropy (8bit):	6.463912993297197
Encrypted:	false
SSDEEP:	1536:5qygxpRYb3MSYnrlZw4DLqn2l/G9jlJoHNAU4npu:2XAcSYnpZJ22dG9j6ONAUWu
MD5:	B13B974324F63044A880BC84365A0BD0
SHA1:	F7DABC096172A0A09C89628D830E067CC97A8E88
SHA-256:	A34D0845D289E5A64498E4F6BF5A30A17C3F187FB292CCF5B1057D81D467E63D
SHA-512:	B5B841042500D623161916CAD991A4F5561649BA14E609EF79958CAF4D7A95403190C187330330F10A1426F7AB9AFCA2B2ABEF9F1326580E57480D79408A455E
Malicious:	false
Reputation:	low
Preview:	....f.e.....7.B8C.....<....f.k.f.n.f.b.,...K".....%.PO@.....!..q.b...f...f.s.3.4...\OOOOOOOOOOO OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO!..r.o.....#.1d^.....f.....!. .R.....f...f....f.c....#|.8;..... ....f.t....c..b...k.]^.....f....3..Z.....f.v..n.....P.....f..... p.j&.....'r.....d..r .....5...|.....&&/.s.M..f.f.....(.x.o.....g.....e....4w.....f.d.....0.Cs..... (.efQ.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	71280
Entropy (8bit):	6.498681502225803
Encrypted:	false
SSDEEP:	1536:OOsuxD2ljgTCcxduILBZIdf7lgzd/l0bWBuMp/xj0:OMxyold9lZI7lOpl0bauH
MD5:	BBA87C141D8F08D86033E05DAAC57D5D
SHA1:	1EA5B7EE9B5C418FB4B15EE91F7524F5DB0D96D1
SHA-256:	EFD311B206AB942C188C3F83AEBE13AEF1D475CB5D822CF3B70AB162DCDC6FF7
SHA-512:	20581E2243E5FE63174EAB6A4424C6F3B06D5582984FBF35707C00813FF662F3232C06160A5365B14F1E7FD7D861CA1702B974B3C2D8DA5C3340D6588CA0C82C
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....\..... ..`...@.....@..... .....L...d(.....p$.....p.....T.....P...H.....text..... ..`.data..... .....@....reloc..p.....@..B.....0.....<.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....T.....S.t.r.i.n.g.F.i.l.e.I.n.f.o...0.....0.0.0.0.0.4.b.0.....d...C.o.m.m.e.n.t.s...I.n.t.e.r.n.a.l. .i.m.p.l.e.m.e.n.t.a.t.i.o.n. .p.a.c.k.a.g.e. .n.o.t. . m.e.a.n.t. .f.o.r. .d.i.r.e.c.t. .c.o.n.s.u.m.p.t.i.o.n... .P.l.e.a.s.e. .d.o. .n.o.t. .r.e.f.e.r.e.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.256149238118269
Encrypted:	false
SSDEEP:	3:TFXV4ovxEun:Plv5n
MD5:	CEA246A40ED9A68F27EEC9458A18DEEF
SHA1:	3E210EBBD8F29926A51BA1074FAD9A22D53659D2
SHA-256:	2F37518683B8AA7E7C81B0F07A42B2A2692CA32FE4DEEB6618470A5EB245B2EC

SHA-512:	DD12CD2ECC855C0089E641986318FAF183E48798D5EE6F55BADF652186B8177D719FC2E631EF5C6353290827E96ADB59A715E3B82E956908D15012F01A91F9AE
Malicious:	false
Reputation:	low
Preview:	[Fortovsretter]..Tagged=SNIPPENS..

C:\Users\user\AppData\Local\Temp\avutil-54.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	714072
Entropy (8bit):	6.248486521119856
Encrypted:	false
SSDEEP:	12288:1nBVHwA0eIjodibcTTMIVNQdqu8JbHfySBpHdiChBA:FBVJVNQoL1
MD5:	19ED470A232B01BB34B7F85288B017F0
SHA1:	4AE08D71FB45055FCCB0D86174150082A39881F1
SHA-256:	CF17BEE0C9479D7AAED9D3399E79FD89ED9535175C9AEEA73C54E48124D6C81A
SHA-512:	5EBC96C5B13A0D79C0C149C59E30AFC28AECC0FBA543A018551A1F83CEE0111EABAED8400B92694739A3734BDE64F23334BBEAEE28AACBC99358CCA075C82682
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L./B-B\|B-B\|B-B\|..\|G-B\|..\|k-B\|..\|.-B\|..\|.-B\|B-C\|(-B\|.Z.\|G-B\|B-B\|A-B\|a.\|.-B\|$.|C-B|$.|C-B|RichB-B|.....PE..L.....V....."!.....J.....o.....`.....p.....@..... ...=... ..<.....X3...0..P0..Pk..8..... .....x...@....."..P.....text....I.....J..... ..`.rdata.....`.....N.....@..@.data...@....`.....L.....@....idata..... .....h.....@....reloc...9...0...:...x.....@..B.....

C:\Users\user\AppData\Local\Temp\folder-publicshare.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	585
Entropy (8bit):	6.901794968845596
Encrypted:	false
SSDEEP:	12:6v/7X0Z7HBwN1+swFIzRqwnN14BZlEcFCF2BoCaTxT4:C0BqEWqQ8YGCgBoCaT14
MD5:	1D98E1B2D84D7B9D0927F6B651EDE827
SHA1:	A1F77FF7EC77865AEF6A4C1B64CC4E3C492090A5
SHA-256:	A9109F45EFD9920700AAF489167AE647FB0BF88CE12AAF69502AD6D1505CB7B3
SHA-512:	A13756009BC37481EBA3B8523EC0458A43459E34F8A81CFC924E20F9B7A68936DF4B321376B5C4DFE464E5AE403876EBB3CE96EE394C7BF1B46094CE9BC2E958
Malicious:	false
Preview:	.PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Folder Icons.._.....tEXtAuthor.Lapo Calamandrei..*..RtEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb....~PLTE.....~.....l.....tRNS.@NS.....{IDAT.WU....0..#....9..!B...Aj)..Sv.,.....`....q..h..w..g..u.4X.x~...#S..d)...D..-W.[A4.ea...nf./.....`..|...W.}.e<.:\.....~..%....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.853055907333276
Encrypted:	false
SSDEEP:	3:rqh2mJUKMJjwD:raJ8JjI
MD5:	6EA2EDF492D8337635DDCD02048BFA32
SHA1:	3F86F5C6398972128ABD8822B5BD1BFE446C6517
SHA-256:	35E1C059B4E54107456E898FBED2CFA59289F9272495014B4396C8ED427EBC95
SHA-512:	56EC3DBDA7B837E26520F90E4D336FDB95D0789BE8A15E034526ED4553683E93F9C116FC57BCAC2C37DAEA516AFAC48CEE39F5BA6363415A4DA68806E1F6BAF9
Malicious:	false
Preview:	[ARBEJDSKLIMA]..Sporangia57=SPOTTEFUGL..

C:\Users\user\AppData\Local\Temp\lang-1045.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	174600
Entropy (8bit):	3.9275478025543364
Encrypted:	false
SSDEEP:	1536:lkoZp1DEqOBdglkr6myEGXRC5bWgiViQFpETgevYNBVe/d:qoZHq+4UXRC5b0ViQFpNQd
MD5:	E10F0042C0EE3B2DE59BEC61D3811C6A
SHA1:	0F75AEEE0338D2E563FD146847E21187C68FD75F
SHA-256:	20DA8A600117A2ACC6A66AD493390D1DA3F8A9CC7FF13A8185EC02A0E5C93B2B
SHA-512:	BA174D089A52135E9CEE8704749D9C44C4EC361C34E09C26CCFB4A34EB69590FCA77250E17B1ED68506B4C0EC958A2B17DED25741177D77CA68D05CDB1ED2BC
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • 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..... .....!.....@..... ..h..... .....rdata..p..... .....@..@.rsrc...h.... .....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@...d...rsrc$02..... ....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.661593260259915
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllE+UwHndZxx3hYB84wXKYAIk9d0LPoBHlNHbEezI:6v/lhPysHUunYBcXKYA59dPFxRbZofp
MD5:	E91514290CFC6F38580278374D3C6B0F
SHA1:	068CB1200349717E8D2EE64475F480C850A85099
SHA-256:	0DE516FC5D5A233BC240F055C70B004160CE4FA2364C93CC12D7D1A60C23420D
SHA-512:	A6C1523D984857924FDDEFD48741B6FB552CAC220D53619F3E572799DACC0EE06B1FBF75D9CDC127BB685BADB4933FFD4F4923E341492307C55BE4C196510C7
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?..A...O...V..D.t...8..Y.n....V.$...../..e...of.g.pm..pF(.,..Oq8.xb.....~....$.]....y..".(..7.-._....0...eUS.c..Y....}.J..p...M.. ...q=.=.B`....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	243209
Entropy (8bit):	5.969458574226536
Encrypted:	false
SSDEEP:	6144:RPVByzfb1YfMq48FKMqCQQU7k1TAH1OobTrEPvQvHk8hep:RPKqUjHM/PvQvHk8hep
MD5:	2510EF915FD96CB0C5D947BA98CB751D
SHA1:	AE10088DD6EC5BD0607FD5848A746AE57DCDC20E
SHA-256:	02528C6E3F317B8FA9010BED22383D9BF696CC3DC9B97CC7FF81A445BE470FA1
SHA-512:	ACA3ED02461EB0D70EF7BF5A74F1E9C7D20446349A02485A49BE3530F9C7CCEEE8F74A412FA8FD9002A815762F240C3C89AEACC97FF84130BE428F8C9ED73E05
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....P.....C.....0..... ..`... .....V.....p..p..... .....T..(.....8.....text.....`..`.data..... .....@. ...rdata..`9...0...:.....@..@.pdata..p....p.....N.....@..@.xdata..\.....f.....@..@.bss....P.....edata..V.....~.....@..@.idata.. .....@....CRT....X.....@....tls.....@....reloc..... .....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9195774738294356
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.10062.exe
File size:	1447056
MD5:	95050a1e0c7d4c57f62e26967b3b0bfd
SHA1:	baa57d1bf6d8a41ba89c6d09bfc4ec2bc986830c
SHA256:	458597ef68351368264111179f244673d5b2702e906bedb3e470786eb455d98ce
SHA512:	a659747a264aa16304d2d246faa277c415011ffd9c7376ac641a1193dc48c9efbbab745d9874a8aae8c4d53f050d32a2973633aab07618a2977e8502c4773549
SSDEEP:	24576:4Y9Mbnf2fKJdodBzdf1JJNVwYFsTtflc4DJQCXzDt+Y9O1/euTLXwwUBg/:p9Mbnf8yeBzzJJe7FXzDtr0Pfwvq/
TLSH:	8C65234D7B38D42BD1477B323D66CA3AADB4DA603565D75F728993EA0AE3305CD22230
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:	38f8cecadad4cca2

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="Brechernes6 originalbillederne Brazing Jagtdistrikter3 ", O=Gennemloebe, L=Saint-FrÃ©zal-d'Albuges, S=Occitanie, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/25/2022 6:12:28 PM 5/25/2023 6:12:28 PM
Subject Chain	• CN="Brechernes6 originalbillederne Brazing Jagtdistrikter3 ", O=Gennemloebe, L=Saint-FrÃ©zal-d'Albuges, S=Occitanie, C=FR
Version:	3
Thumbprint MD5:	8E7DC2F9F1AD6C2CDA6D266EDBD6ABFD
Thumbprint SHA-1:	E691195416A055DD79B76CC251E1145D615EB842
Thumbprint SHA-256:	F9208891F5FE35BC2ACD0351EC70F6955E51D254E0E594A885A216DFBEAFB35E
Serial:	3583CC204911C9D6

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 00007F07E04849DAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx

Instruction
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F07E04849AAh
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	0x5b000	0x22d68	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x15f580	0x1f10	
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	0x30000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5b000	0x22d68	0x22e00	False	0.596998207885	data	6.16097805989	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5b2f8	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

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6bb20	0xd4b1	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x78fd8	0x25a8	data	English	United States
RT_ICON	0x7b580	0x10a8	data	English	United States
RT_ICON	0x7c628	0x988	data	English	United States
RT_ICON	0x7cfb0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x7d418	0x100	data	English	United States
RT_DIALOG	0x7d518	0x11c	data	English	United States
RT_DIALOG	0x7d638	0xc4	data	English	United States
RT_DIALOG	0x7d700	0x60	data	English	United States
RT_GROUP_ICON	0x7d760	0x5a	data	English	United States
RT_VERSION	0x7d7c0	0x264	data	English	United States
RT_MANIFEST	0x7da28	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	Myotoniasgrupp96
FileVersion	0.2.16
CompanyName	PARACHROMELI
LegalTrademarks	brnesa
Comments	ansp
ProductName	tomtersselv
FileDescription	Polstrende
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.generic.ml.10062.exe PID: 6288, Parent PID: 5868

General

Target ID:	0
Start time:	22:34:11
Start date:	25/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe"
Imagebase:	0x400000
File size:	1447056 bytes
MD5 hash:	95050A1E0C7D4C57F62E26967B3B0BFD
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: 00000000.00000002.761431234.0000000003170000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nstEC39.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Sognefogedernes.Run6	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Ddsstivhed9.non	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\avutil-54.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\folder-publicshare.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\lang-1045.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\multimedia-volume-control-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaFB7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	486	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstEC39.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
unknown	44810	24250	75 6e 6b 6e 6f 77 6e	unknown	success or wait	146	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Sognefogedernes.Run6	0	16384	fd fd fd fd 66 0f 65 fd fd fd fd fd 0f fd fd fd 37 fd 42 38 43 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 3c fd 0f fd fd 66 0f 6b fd 66 0f 6e fd 66 0f 62 fd fd 2c 1f fd 4b 22 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0f fd fd fd fd fd fd fd 25 fd 50 4f 40 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 21 fd 0f 71 fd 62 0f fd fd 66 0f fd fd 66 0f 73 fd 33 fd 34 16 fd 2e 5c 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f 4f	fe7B8C<fkfnfb,K"%PO@! qbffs34.\ OOOOOOOOOOOOOO OOOOOOOOOOOOOO OO OOOOOOOOOOOOOO O	success or wait	6	406224	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 1c fd 38 fd 7d fd 6b fd 7d fd 6b fd 7d fd 6b fd 05 52 6b fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 1f fd 6a fd 7d fd 6b fd 1f fd 6a fd 7d fd 6b fd 7d fd 6b fd 7c fd 6b fd 7d fd 6b fd 7d fd 6b 67 14 fd 6a 33 7c fd 6b 66 14 fd 6a fd 7d fd 6b 66 14 3e 6b fd 7d fd 6b fd 7d 56 6b fd 7d fd 6b 66 14 fd 6a fd 7d fd	MZ@!L!This program cannot be run in DOS mode.$8}k}k}kRk}kj}kj}kj}kj}kj}k}k|k}k}kgj3|kfj}kf>k}k}Vk}kfj}	success or wait	120	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Ddsstivhed9.non	0	13978	44 fd 38 53 2f 6f 72 09 3e 3b a9 4b 34 43 fd fd 0a 5a 11 72 37 09 fd 30 59 6b fd 41 fd 3e 09 fd fd 11 58 5c fd 7b fd fd fd fd 51 fd fd 2e 39 fd 32 fd 00 4a 7c 00 30 fd 61 fd 38 fd fd 1f 68 fd 76 fd 6d 0e 3f 58 0d 66 01 31 fd fd 0a fd 46 26 fd fd 79 3b fd fd 33 fd 31 18 fd 2f 2e fd 65 48 fd 4c 15 7e fd 18 fd 40 fd 7d 46 73 36 48 07 fd 62 00 fd 78 fd e6 1a fd 41 41 fd 71 fd 2b fd 6a fd 7a 7c fd fd fd 1c fd 67 fd 26 6e fd fd fd 39 15 fd 42 73 fd fd fd fd 00 14 fd fd fd 49 fd fd fd 09 7f fd 52 09 fd fd 6d fd 2a 31 05 1d fd 66 3f fd fd fd 07 fd fd fd fd 57 fd fd fd 20 fd fd 7e 7d 0f 5f fd fd 4d fd 72 0a fd fd fd fd 7d 7d 3a ed fd 0f 0b 12 1f 06 25 fd 37 fd fd fd 37 fd fd 03 fd 39 fd fd fd fd fd fd fd fd 28 fd 24 11 7c	8S/or>;K4CZr70YkA>X\{Q.92J|0a8hvm?Xf1F&y;31/.eHL~@Fs6HbxAAq+jz|g&n9BsIRm*1f?W~}_Mr}}:%779($|	success or wait	1	406224	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd 2b fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 03 00 00 00 00 00 00 30 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichRPEd+" 0	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 03 00 fd 5c fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 fd 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 57 fd 01 00 03 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd\" W`@@	success or wait	5	406224	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\avutil-54.dll</td><td>0</td><td>16384</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 06 4c 2c 2f 42 2d 42 7c 42 2d 42 7c 42 2d 42 7c 0d fd 7c 47 2d 42 7c fd fd 7c 6b 2d 42 7c fd fd 7c 03 2d 42 7c fd fd 7c fd 2d 42 7c 42 2d 43 7c 28 2d 42 7c fd 5a fd 7c 47 2d 42 7c 42 2d 42 7c 41 2d 42 7c 61 8c 7c 03 2d 42 7c 24 c8 7c 43 2d 42 7c 24 ce 7c 43 2d 42 7c 52 69 63 68 42 2d 42 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05</td><td>MZ@!L!This program cannot be run in DOS mode.$L,/B-B|B-B|B-B ||G-B||k-B||-B||-B|B-C|(-B|Z|G-B|B-B|A-B|a|-B|$|C-B|$|C-B|RichB-B|PEL</td><td>success or wait</td><td>44</td><td>406224</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\folder-publicshare.png</td><td>0</td><td>585</td><td>fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 03 00 00 00 28 2d 0f 53 00 00 00 03 73 42 49 54 08 08 08 fd fd 4f fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 1a 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 46 6f 6c 64 65 72 20 49 63 6f 6e 73 fd 07 5f fd 00 00 00 17 74 45 58 74 41 75 74 68 6f 72 00 4c 61 70 6f 20 43 61 6c 61 6d 61 6e 64 72 65 69 d1 1a 2a 00 00 00 52 74 45 58 74 43 6f 70 79 72 69 67 68 74 00 43 43 20 41 74 74 72 69 62 75 74 69 6f 6e 2d 53 68 61 72 65 41 6c 69 6b 65 20 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69 63 65 6e</td><td>PNGIHDR(-SsBITOpHYs+tEXtSoftw a rewww.inkscape.org<tEXtTitleAdwaita Folder Icons_tEXtAuthorLapo Calamandrei*RtEXtCopyrightCC Attribution-ShareAlike http ://creativecommons.org/licen</td><td>success or wait</td><td>1</td><td>406224</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 0e 5c 29 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL\)b!	success or wait	11	406224	WriteFile
C:\Users\user\AppData\Local\Temp\multimedia-volume-control-symbolic.symbolic.png	0	225	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3f 0e 01 41 1c fd fd 4f fd fd fd 56 1a fd 44 fd 74 04 17 fd 38 fd fd 59 fd 6e fd 12 fd fd 56 fd 24 fd fd 0d fd fd fd fd 0d 2f fd fd 65 fd fd fd 6f 66 fd 67 0d 70 6d 1b fd 70 46 28 fd 07 2c fd fd 4f 71 38 05 78 62 fd 0a fd fd fd fd 70 fd 7e fd 06 fd fd 24 fd 5d 1b fd 0d fd fd fd 79 fd fd 22 fd 28 fd fd 37 fd 2d fd fd 5f fd 1a fd fd 30 fd fd fd 65 55 53 fd 63 01 fd 59 fd fd fd fd 7d 1c 4a 00 fd 70 fd 1e fd 4d fd 7f fd 17 fd 71 3d fd 3d 0d 42 60 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8?AOVDt8YnV$/eofgpmpF(,Oq8xb~$]y"(7-_0eUScY}JpMq==B`IENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 fd 03 00 7f 00 00 00 fd 00 26 22 0b 02 02 25 00 0a 02 00 00 fd 03 00 00 12 00 00 50 13 00 00 00 10 00 00 00 00 43 09 03 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 30 04 00 00 04 00 00 fd 16 04 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd&"%PC0`	success or wait	15	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nspFBDC.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe	unknown	512	success or wait	387	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	18548	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	4	success or wait	10	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.10062.exe	unknown	16384	success or wait	77	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	16384	success or wait	206	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	4	success or wait	2	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Ddsstivhed9.non	unknown	2	success or wait	252	40275E	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nseEC79.tmp	unknown	4	success or wait	484	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Sognefogedernes.Run6	unknown	1048576	success or wait	1	732A2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112\ADVERTENCY	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204\MORTIFICEREDE	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Pezizaceae207	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Pezizaceae207\anticapital	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING\inditch	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\NONESUCHES	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\NONESUCHES\Nugatoriness	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Botanicas	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Botanicas\Antilapse	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112\ADVERTENCY	Balsamo11	unicode	TUBERCULOTROPHIC	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204\MORTIFICEREDE	Expand String Value	expand unicode	%WINDIR%\glyceryl.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Pezizaceae207\anticapital	Forsikringsaftalelovenes242	binary	FF DD 39 BE	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING\inditch	CAMPINGPLADS	binary	22 14 89	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\NONESUCHES\Nugatoriness	Nopredes	binary	FF A4 CA 7F	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Botanicas\Antilapse	Expand String Value	expand unicode	%WINDIR%\Aflste11.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly

Copyright Joe Security LLC 2022