ID: 612103
Sample Name:
FRACCIONAMIENTO
1722403906461L.exe
Cookbook: default.jbs
Time: 15:18:00
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

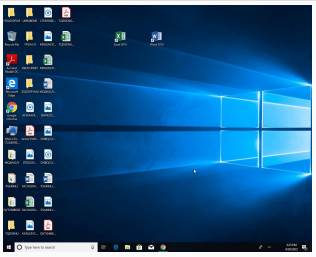
Windows Analysis Report

FRACCIONAMIENTO 1722403906461L.exe

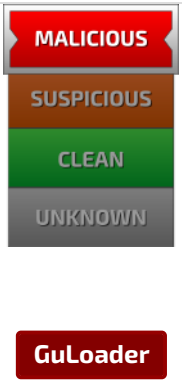
Overview

General Information

Sample Name:	FRACCIONAMIENTO 1722403906461L.exe
Analysis ID:	612103
MD5:	04e8c57a5df183..
SHA1:	b53b20975776cc..
SHA256:	345aa66f6945c8..
Tags:	exe guloader signed
Infos:	



Detection



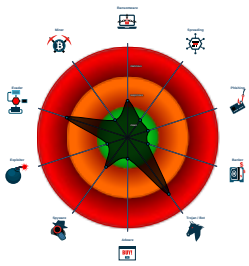
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Tries to load missing DLLs
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- FRACCIONAMIENTO 1722403906461L.exe (PID: 6260 cmdline: "C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe" MD5: 04E8C57A5DF1834C590C49CCC8734D6E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1p1TrvkFKYHzlCDSRi8V2K0EcN7S0sk7E"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.801228236.000000000325C000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

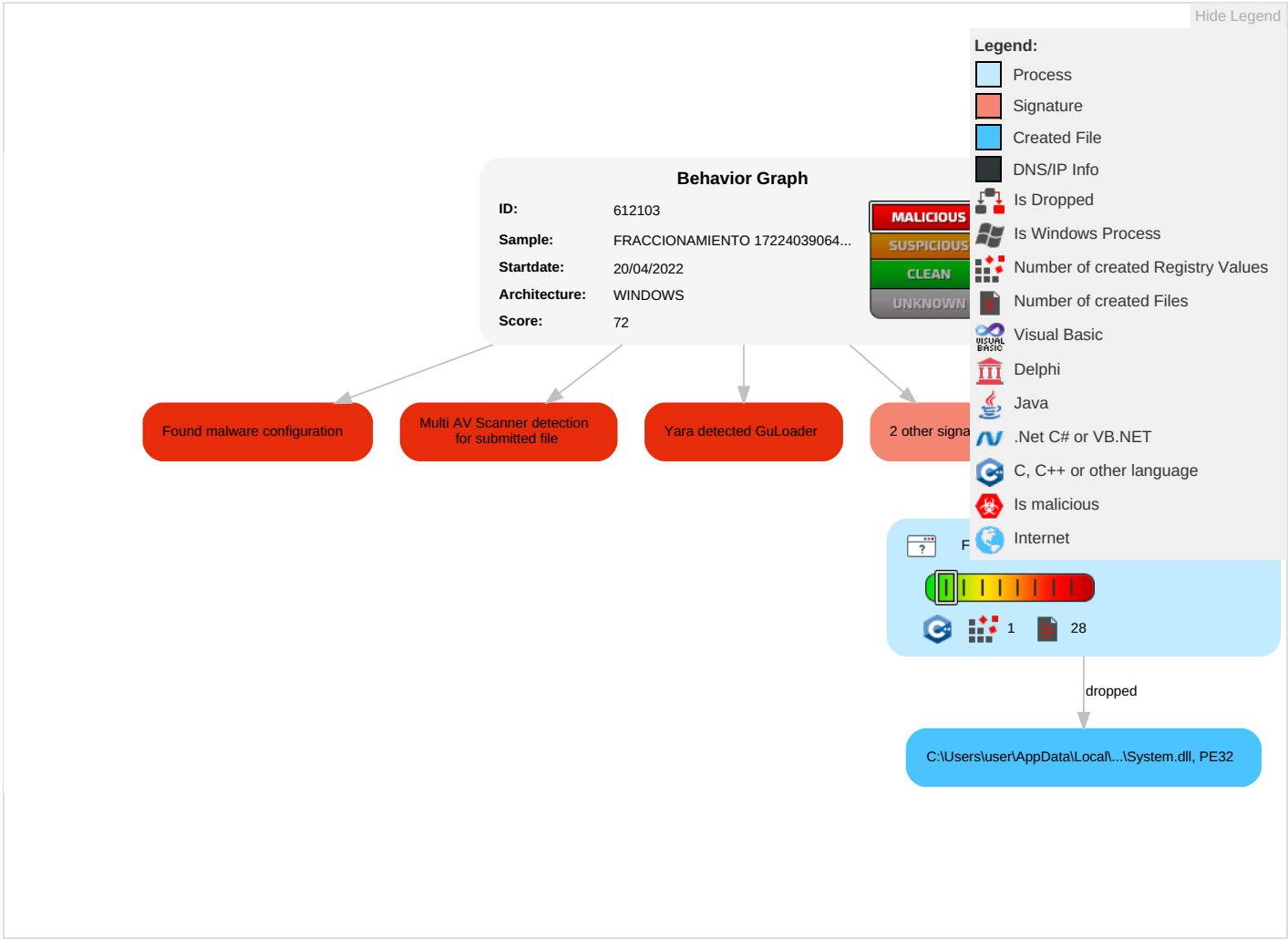
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Windows Service	1 DLL Side-Loading	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

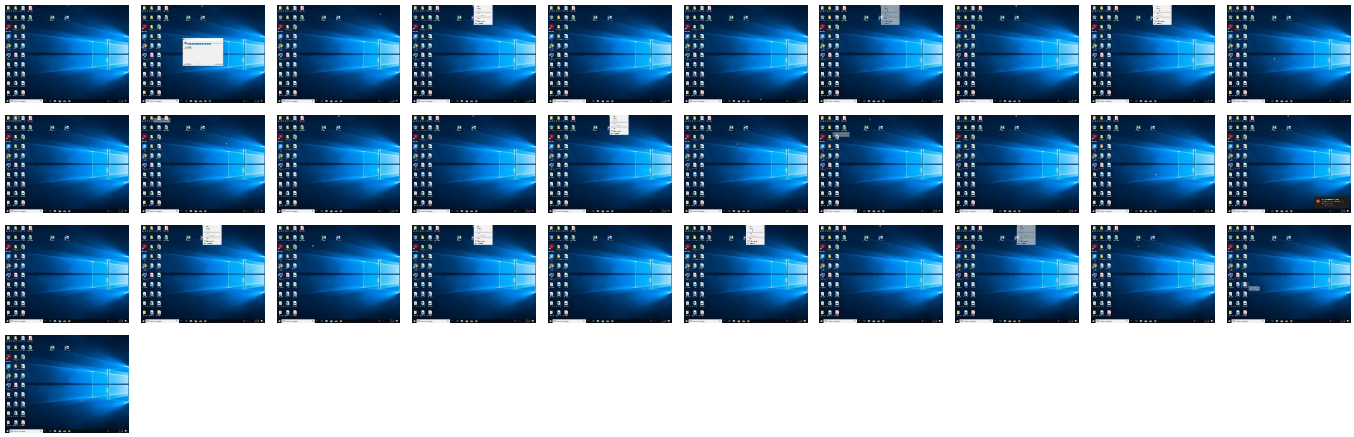
Behavior Graph



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
FRACCIONAMIENTO 1722403906461L.exe	28%	Virustotal		Browse
FRACCIONAMIENTO 1722403906461L.exe	13%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsa7A50.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsa7A50.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://jimmac.musichall.czif	0%	Avira URL Cloud	safe	
http://crl.mesince.com/ms.crl0	0%	Virustotal		Browse
http://crl.mesince.com/ms.crl0	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms.cer0	0%	Virustotal		Browse
http://aia.mesince.com/ms.cer0	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0)	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms-tsa.cer02	0%	Avira URL Cloud	safe	
http://crl.mesince.com/ms-tsa.crl0F	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0-	0%	Avira URL Cloud	safe	
http://www.mesince.com/policy/0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://jimmac.musichall.czif	emblem-unreadable.png.0.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	media-removable.png.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	FRACCIONAMIENTO 1722403906461L.exe	false		high
http://crl.mesince.com/ms.crl0	FRACCIONAMIENTO 1722403906461L.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://aia.mesince.com/ms.cer0	FRACCIONAMIENTO 1722403906461L.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0)	FRACCIONAMIENTO 1722403906461L.exe	false	• Avira URL Cloud: safe	low
http://aia.mesince.com/ms-tsa.cer02	FRACCIONAMIENTO 1722403906461L.exe	false	• Avira URL Cloud: safe	unknown
http://crl.mesince.com/ms-tsa.crl0F	FRACCIONAMIENTO 1722403906461L.exe	false	• Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0-	FRACCIONAMIENTO 1722403906461L.exe	false	• Avira URL Cloud: safe	low
http://www.mesince.com/policy/0	FRACCIONAMIENTO 1722403906461L.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	612103
Start date and time: 20/04/202215:18:00	2022-04-20 15:18:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FRACCIONAMIENTO 1722403906461L.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:	17
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@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.7%) • Quality average: 87.8% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • 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 • 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, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.112.88.60
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ris-prod.trafficmanager.net, asf-ris-prod-neu.northeurope.cloudapp.azure.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\camera-hardware-disabled-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	216
Entropy (8bit):	6.561875161973391
Encrypted:	false
SSDEEP:	6:6v/lhPysbg1s0zIRU4MNfxwp/Dn4fqUz41p:6v/77gfzIm4aqprnRb
MD5:	6F86F050B74E4FC04A1F375E8E2744A9
SHA1:	3060A2BA1BE38388DC86FB43E3826B1045407551
SHA-256:	2647746C3F2852DF0693865D4EBDC22FD6AAE4E725F8EA13C263766C98AFB787
SHA-512:	10969F0A23D81064E7BBE980AA10D4D42C1713157F9EB725737FAF666326066BC75082F10D5976F803BDED998CFC5BB6EA51D373A5E1A30B3F0CE940BAD235DC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1..Q...L5Q.....`.. .E.....(44&1.g"...;.....d.%.AK...0c.?..].W..H.....;...)...D.gjlqy..8a.L.3...A.....u...k.8C..6M.I..J,:....~...0.\...P....IEND.B`.

C:\Users\user\AppData\Local\Temp\emblem-unreadable.png	
Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 8 x 8, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	347
Entropy (8bit):	6.38137890298033
Encrypted:	false
SSDEEP:	6:6v/lhPZo+aWdKcfi+2jlAVVziUdCyENoKuAkmHXkg6u2p+bp:6v/7R4aZKjCVdCyENyTg72pA
MD5:	0916297AA635A852B181B815131AFD11
SHA1:	46E2E8BAAB9D8C299833F45924CD5C58869B26E4
SHA-256:	72428164FA2F8DF4FDED0E5213A4043729929CA53AE3F7C0BED73ED1BF835AE1
SHA-512:	902C50D12BBBEE1BF0D4D938D12809BA79277BA891E51D6802590878DAFD49D8F7429671E333335AF8FE0811283CD8DFFE72C27ABCA345B729BE66E3E9C3342F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....pHYs.....o.d....tEXtSoftware.www.inkscape.org..<.....tEXtAuthor.Jakub Steiner.../....tEXtDescription.mimetypes7..d...!tEXtSource.http://jimmac.musichall.czif.^...zIDAT..}.-..@....p.=AC.a.XDe.Q.?....c ....F.,..d..dF<.b.4..* ..:h^&.4&N...t.....~h..z3^.....{..v.....u..Y...<+|.$...owq..{\h.....IEND.B`.

C:\Users\user\AppData\Local\Temp\mail-signed.png	
Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.4316463225570235
Encrypted:	false
SSDEEP:	12:6v/7e8otKtOqI81slANbOA1k9cT+83NBO7GdV095m:oaGc81sd9k9c62NBO76V0/m
MD5:	DAB703E211118D187B2FCB4FB0E43124
SHA1:	5539F00C552DC23AB09EF2797F74412D12F0D8BA
SHA-256:	D4D203344A07ECF9E755E9396C7986A84B7F8684AA94F87C64CFDAD29E3558CE
SHA-512:	41CD1A9DDF90EE76BD66FC96FA188ED56573F433B2743DF84014FE022173703029A294B12749FA21BD7F57695134FD99B92A681DD6A0934AC1AA904BB0C3220E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....IDATx.....$A.D.O.k.t....m.m..v..S]cv^...x.....z.@\..w....?~p.O.a7v...*.UB...v..yp...CA.1M...?.1...y..CR...v.....B.....oD;Rv..w...*...m.....L...u.LJ..v.@Y.C.R.J..&.&.n...<..e...q....>2.4.&.U..J.}Sk.#W^...p..G.....X.f3..g.c..X..6...5...g..!.....\..il.8w....b.]..yL.xU}$....{.Uw._..o-.....p.....=...OQ...(..(.;.k.....J."FL<.....oA.\R....f....\1w...1i.....*Jj}...*.J7.CD=..Z..W.(....w..,.b...vc.....m...v....zt3.W.....IEND.B`.

C:\Users\user\AppData\Local\Temp\media-removable.png	
Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	834
Entropy (8bit):	7.403819222634866

Encrypted:	false
SSDEEP:	12:6v/7maZB4RO4HE+swFImYYh1EBYwBREz/7AdqJuT+wZqlz9W9s24zYCK0Xwr/zN:tak15rEZGj7UqPWqlRWquCKV/J
MD5:	32148C57FEC1C44D630694C2F3EB9C79
SHA1:	7D241B5BFEFF379A96AECC6D20A2B85A40FDB460
SHA-256:	F5948768EE8A33988F530948A10EC8333BB2AE91450C4A0FFDA6C78E9E454AC2
SHA-512:	1F7F216461F1348BE09E0A57EAF75BB595E95105C3729601741E54337629C684FD620292CD6267465C1CF65BBA6E17DC0F6CB81C44182474812496520CDE65E6
Malicious:	false
Reputation:	moderate, very likely benign file
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...KH.Q.....;.k.i.R..z'.(..".2Z.J!.....M...@...(.q.E.....X.J#...6.:...w..p&...~p 6..?... .....w....e.g..#._.Z.....@....!..H:...b..c-GS..'#..X(.I...v.c.ci.....7O..O.....>.J.E...y...f.b.D"B8..:h9.h....*kmO..[..U...9W.....b.h..\e446`T.-.\..R47. .....R.}..a~....&....D-LC.....b. ..:dc...`...}.J.....-.6v.DqR...%c.....w6_/...f1..a.....Z.....F..!C8..#.A...r.&...Q.bn....X.y..D.q0>8...g..*.<$.8#..c#_.!..M.....|.C4X.....;.q...dW[.r'.`.^...x....3O?.|...K\..~...L<.'.L ".R....3.Ks..L...l.....f..{9=..z3.....>.....IEND.B`.

C:\Users\user\AppData\Local\Temp\monotocardiac.dat

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	data
Category:	dropped
Size (bytes):	114102
Entropy (8bit):	4.590163620452223
Encrypted:	false
SSDEEP:	768:t/GyI2l2XmzoEf1woV2kTCzhf0RUJswAFtnkFmhvkhmAd6P+sRkv:VhkXyjR2kTeeRUw7hshmAynev
MD5:	FE6B2641187E785DD0264A4D4A783B59
SHA1:	FDFC09D27370575972E25756DE665B82D372BD76
SHA-256:	8D6EF611ED26F02C8A5B80721628AEF8766F501F130AC25ED120E281BB2A0A24
SHA-512:	A1D6F07C4E8F7117EE77945F7AFE1D98A4BB9BED190552E075383BC1F2E6C35385A4D2429D9E45AAF3EE5980B2D0832DB7BCEC973DF829896220845C7C3E22B B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\nsa7A50.tmp\System.dll

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.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: 0%, 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\preferences-system-network-proxy-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	287
Entropy (8bit):	6.877606568262548
Encrypted:	false
SSDEEP:	6:6v/lhPyso9FwH4OWXHQNBVTEoL2NfawlZywceJCSHGq7UZ56Iqgaeup:6v/7IsHuQlTEWyy5wca/Hz7UZ5jqnec

MD5:	739EF7135750B4A34587B311374CFD3B
SHA1:	2C7BB533D0C3B0FB2E953E21C949A38CCADCB994
SHA-256:	DCF5CCF55CD3A0C22D7E1E15BA74A77E87564C53782139305319 57E837BCFFD0
SHA-512:	A123F0270240DAB31EDDE187B52534B032534A993DF5DC3C023F47DF22DD13CDD4875894180D7CA5A7D58A8341BE03B193D645DBE6C5355F0A8C813052D6C7
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...=N.1.../.....4.. w..)....\!G...S.p...:D.. %.6El.Z..2.H.7.yoms.=..d....f.s.4g.%.&.]$.uK+.l6...Z.*....8.yA?.M..9.u..j.Q..4 .L..aY.{ .o!...]&..mb..:.bQ...m.gP....N..??..?.pVK..... |7A.v...7...j..../xm.....U..}.....IEND.B`.

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

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	803
Entropy (8bit):	7.445534026139213
Encrypted:	false
SSDEEP:	12:6v/7wtZNGfN/qk9eell0BA5Q8nokd/XaaURqN7C8qDUJ01D8/MS+BFdCkAQ:XtvGV/SslL5Q68MN2jDvAKZCNQ
MD5:	B344495C567F359D8A722E788409C26B
SHA1:	B599EB3F171E4EB856BBC28E8BE4F50975ACBC32
SHA-256:	DA4223F95FA7D4A484C1CA675BB8BD4F6DDEEB0F274A4F32616655189033E5C2
SHA-512:	658E0F63022AB10538D7921FC98994200397F73A7FB63100278A955925AB5B9DE6CA2652061FD82704319613596DECC0A76C21DFD3B968947518AAD6465225E1
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtAuthor.Lapo Calamandrei..*...'tEXtDescription.Based of Jakub Stei ner work.)8_...JIDAT8....OTA.....U..\.0a..m..X.....:..1$."1.D..k...YP`C...@...A.. *....{w,`.P.....\|..w...0.j..J>.Z.S...\|.....lb.tD..lvo.....@?..0I..F).R...Q...Y).P.....A)E&..c+_<{y.@< ~.4..\|.8mm.....E...I..)%Ji66.POS.&.Oa.K.?.\|.$F.>s...P)...+P.....f...:.M..s.lll2>.....6...//..f..p3.[.X-.v...ccoy36.....C.cA.....o....J....c,..:.c.{.'.....n..... .8.%l%..`.u.B.q....R..==='Ck.. ..D..[g).....@..><..~.Wk...4..... M....PJ4.VWW.V..d.Y.(.z..y>KK..b{.....:J.& ...G'...!c.....I../."a..;B....._.V.r9|?.,(.J.j..F..^.....c.7.u.....R.....D20.....N.n?..phpp.....j.... IEND.B`.

C:\Users\user\AppData\Local\Temp\selection-end-symbolic-rtl.symbolic.png

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	142
Entropy (8bit):	5.583604569229667
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllBM9JT8J6yjjJmS/PB3eD0bdR1rrF/1p:6v/lhPysz8JYJvf/lc0bTxzp
MD5:	B361CAD290962835529009E96E49CC9F
SHA1:	2E29CB53B9B3BD6A433FB2C50950288E321AE551
SHA-256:	AB86F801B5ED71C581E2A68B6E052953C6B5B95DFBC617A117DEA9B084429618
SHA-512:	3100203CE8A3D2DE5717EDC0D67A1BC47CB2C78CE5EFFEE51327EA0AE71F4945188ABAD9AF49E5D8BD78F3B6B5807692975537B49873F601C9AA9F49DD2588 7C
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....EIDAT8.c`../....,.]!...`....TRj0...C....H.!dy.....f....D.p.j.!(=....S.....IEND.B`.

C:\Users\user\AppData\Local\Temp\value-increase-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	113
Entropy (8bit):	5.322830648467957
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllRxdh9TFaxedVjtNOh99bXDgpaGp:6v/lhPysfnTF6QROripxp
MD5:	2D78FF1482A10EA250A500C55EDB7A4D
SHA1:	02DC306A0B14673185941637E78C3E0115F3BADC
SHA-256:	EA88C0E8743471267DB4183A75E6122CE10062EF396ABEAE5C0BC4FD2D65A6F1
SHA-512:	2EB3D54E72CFF8B061676AA791D021464777FEA77E5D6424B8DE9A78C8E32D894ED164C096FC150C7B0E4D46A8B31C75B54A72C2DB02DECAECB8E555D3999 A0
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....(IDAT8.c`...?...L..0..0.....>.]@...X.....S.w....IEND.B`.

C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg

Process:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
File Type:	SVG Scalable Vector Graphics image
Category:	modified
Size (bytes):	335
Entropy (8bit):	4.737555359684875
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slZRI2rjFvRbWHFHUHFvCpifW1IUHFBLJZtSKlNK+:TMHdPnnl/nu3i2FZ484sIBLjdlj
MD5:	C05C42CB3D95BF3BC7F49CCD8DCCA510
SHA1:	20442E344E95508586B1B2A7B4C6272C3F5C86F8
SHA-256:	695554CE5F23A275D3C25C27410D0CFBF8A83156807DAA3A601635E4E5D8AED0
SHA-512:	0EC19BBA7B5032670524965A8C55D8C6401F833000880DE1C0F74A5EAA4E302B0CE3E60218F3DDB95CB3E1EA7374A197CB71682526DFF910D9A6CF35FF971BE6
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <path d="m 4 1 c -1.660156 0 -3 1.339844 -3 3 v 8 c 0 1.660156 1.339844 3 3 3 h 8 c 1.660156 0 3 -1.339844 3 -3 v -8 c 0 -1.660156 -1.339844 -3 -3 -3 z m 0 6 h 8 v 2 h -8 z m 0 0" fill="#2e3436"/>.</svg>.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.124578250940887
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:	FRACCIONAMIENTO 1722403906461L.exe
File size:	125736
MD5:	04e8c57a5df1834c590c49ccc8734d6e
SHA1:	b53b20975776cc58ed77d8bfff905303aa84391e
SHA256:	345aa66f6945c8fadee442f115591eaa694196c3ec207246814b5c90ab39df0a
SHA512:	fdd62abfed177e5d45be7ba8d185e8c955605e05674a05f899a1a7ee11eb60898dfe0cb6be9392b1b71700ca3e27e51e4c18bf55975a4a8f5acf159185b43d15
SSDEEP:	3072:dfY/TU9fE9PEtu4IEOa8jDbD2yJEmR2qMQh1pzScoTB:BYa6PaaDNms1Z4d
TLSH:	73C3B0187F64C527D85A4270096747E65EF5ED118850A39F2360ABAE3CB3242BB1F3DB
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:	f89c9e8eaeb3f162

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:	E=PRIMEVOUS@tinkturen.Non, CN=ULIGELNNEN, OU=Peritropal, O=Craggiest7, L=ANFALDENES, S=SULPHONATE, C=MR
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	• 4/19/2022 6:35:53 PM 4/19/2023 6:35:53 PM
Subject Chain	• E=PRIMEVOUS@tinkturen.Non, CN=ULIGELNNEN, OU=Peritropal, O=Craggiest7, L=ANFALDENES, S=SULPHONATE, C=MR
Version:	3
Thumbprint MD5:	E4BFB521658CD7B3034F27E18D2A5D0F
Thumbprint SHA-1:	2ECBD5255612406BEE49C9664C97CD33AD373599
Thumbprint SHA-256:	F05E501D2E2A047E9752DDB3D0CE3F55FB13505223FA83A8DB6AFCB3481C07BD
Serial:	00

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 00007F4F9CC4759Ah
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 00007F4F9CC4756Ah
and word ptr [ebp-00000132h], 0000h

Instruction
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x51000	0x8860	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1d1c0	0x1968	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x26000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x51000	0x8860	0x8a00	False	0.405712182971	data	5.18891166126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x514c0	0x368	data	English	United States
RT_ICON	0x51828	0x25a8	data	English	United States
RT_ICON	0x53dd0	0x10a8	data	English	United States
RT_ICON	0x54e78	0xea8	data	English	United States
RT_ICON	0x55d20	0x988	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x566a8	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x56f50	0x6c8	data	English	United States
RT_ICON	0x57618	0x668	data	English	United States
RT_ICON	0x57c80	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x581e8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x58650	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2289596279, next used block 2022213768	English	United States
RT_ICON	0x58938	0x1e8	data	English	United States
RT_ICON	0x58b20	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x58c48	0xb8	data	English	United States
RT_DIALOG	0x58d00	0x144	data	English	United States
RT_DIALOG	0x58e48	0x13c	data	English	United States
RT_DIALOG	0x58f88	0x100	data	English	United States
RT_DIALOG	0x59088	0x11c	data	English	United States
RT_DIALOG	0x591a8	0x60	data	English	United States
RT_GROUP_ICON	0x59208	0xae	data	English	United States
RT_VERSION	0x592b8	0x268	MS Windows COFF Motorola 68000 object file	English	United States
RT_MANIFEST	0x59520	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	Premoltbrevvek
FileVersion	9.21.27
CompanyName	Zincl
LegalTrademarks	Blepharocol
Comments	lasciv
ProductName	Akseltap182
FileDescription	Bagepulveretsu254
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: FRACCIONAMIENTO 1722403906461L.exe PID: 6260, Parent PID: 668

General

Target ID:	0
Start time:	15:19:15
Start date:	20/04/2022
Path:	C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe"
Imagebase:	0x400000
File size:	125736 bytes
MD5 hash:	04E8C57A5DF1834C590C49CCC8734D6E
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: 00000000.00000002.801228236.000000000325C000.00000040.00001000.00020000.00000000.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\nsk7954.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\nsk7955.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\nsa7A50.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa7A50.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\nsa7A50.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\nsa7A50.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	14	406184	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\monotocardiac.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\camera-hardware-disabled-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\emblem-unreadable.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-signed.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\media-removable.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\preferences-system-network-proxy-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\printer-network.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\selection-end-symbolic-rtl.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\value-increase-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\zoom-out-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsk7954.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsa7A50.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	3	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsa7A50.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 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
unknown	88278	25241	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\monotocardiac.dat	0	16384	fd fd		success or wait	7	406224	WriteFile
C:\Users\user\AppData\Local\Temp\camera-hardware-disabled-symbolic.symbolic.png	0	216	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 31 0e 01 51 14 fd fd 4c 35 51 12 e0 fd 00 fd 60 fd fd 20 fd 45 fd 06 15 fd fd 28 34 34 26 31 fd 67 22 13 fd fd 3b fd fd 13 fd ff 19 64 fd 25 fd 41 4b fd fd fd 30 63 10 3f fd fd 5d fd 57 1b fd 48 fd fd fd fd 1a 3b 1c fd fd 29 fd 18 fd 44 fd 67 6a 6c 71 79 fd 0e 38 61 15 4c fd 33 fd fd fd 41 fd fd fd 19 fd fd fd fd 75 fd fd fd 6b fd 38 43 19 fd 36 4d fd 49 fd fd 4a 2c 3a fd fd fd fd 7e fd 1b 16 30 13 5c fd fd 03 50 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT81QL5Q` E(44&1g";d%AK0c?]WH;)Dgjlqy8aL3Auk8C6MIJ,:~0\PIENDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\emblem-unreadable.png	0	347	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 08 00 00 00 08 08 06 00 00 00 fd 0f fd fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 6f fd 64 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 14 74 45 58 74 41 75 74 68 6f 72 00 4a 61 6b 75 62 20 53 74 65 69 6e 65 72 fd fd fd 2f 00 00 00 15 74 45 58 74 44 65 73 63 72 69 70 74 69 6f 6e 00 6d 69 6d 65 74 79 70 65 73 37 fd fd 64 00 00 00 21 74 45 58 74 53 6f 75 72 63 65 00 68 74 74 70 3a 2f 2f 6a 69 6d 6d 61 63 2e 6d 75 73 69 63 68 61 6c 6c 2e 63 7a 69 66 fd 5e 00 00 00 7a 49 44 41 54 18 fd 7d fd 2d 0e fd 40 18 05 fd fd 70 fd 3d 41 43 fd 61 fd 58 44 65 fd 51 0c 3f 44 fd 06 fd 63 20 11 1c fd fd 46 fd 2c 0a 0c 64 fd fd	PNGIHDRpHYsodtEXtSoftwarewww.inkscape.org<tEXtAuthorJakub Steiner/tEXtDescriptionmimetypes7d!tEXtSourcehttp://jimmac.musichall.czif^zIDAT}-@p=ACaXDeQ?c F,d	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-signed.png	0	501	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 01 fd 49 44 41 54 78 01 fd fd fd fd 24 41 00 44 fd 4f fd 6b 2e 74 fd fd 0d fd 6d f6 6d f6 fd 76 fd fd 53 5d 63 76 5e fd 0e fd 78 fd fd fd 1d fd 7f fd 7a 1c 40 5c 08 11 77 fd 1f fd 1f 3f 7e 70 fd 4f fd 61 37 76 fd fd fd 2a 00 55 42 fd 0d 0a 76 0d fd 79 70 fd 10 fd 43 41 26 31 4d fd fd df 3f fd 31 fd fd fd 79 36 fd 43 52 06 fd 1d 76 fd 1f fd fd 01 fd 42 04 7f fd fd fd fd 6f 44 3b 52 76 11 fd 77 25 00 1c 2a fd 10 fd 6d 0b fd fd fd 1f 4c fd 03 fd 75 fd 4c 4a 02 0e 76 fd 40 59 fd 43 17 52 fd 4a fd fd 26 fd 26 fd 6e 02 1d fd 3c 17 fd 65 b6 fd fd 71 1c 0b fd fd 3e 32 fd 34 fd 26 fd 55 fd 15 4a fd 7d 53 6b fd 23 57 5e fd fd 1a	PNGIHDRaIDATx$ADOk .tmmvS]cv^xz@\w? ~pOa7v*UBvypCA1M? 1yCRvBoD; Rvw*mLuLJv@YCRJ&&n <eq>24&UJ}Sk#W^	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\media-removable.png	0	834	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 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 6f fd 64 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 1b 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 49 63 6f 6e 20 54 65 6d 70 6c 61 74 65 fd fd fd 3f 00 00 00 18 74 45 58 74 41 75 74 68 6f 72 00 47 4e 4f 4d 45 20 44 65 73 69 67 6e 20 54 65 61 6d 60 fd 76 7e 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 73 65 73 2f 62 79 2d 73 61 2f 34 2e 30	PNGIHDRapHYsodtEXtSoftwarewww. inkscape.org<tEXtTitleAdwaita Icon Template? tEXtAuthorGNOME Design Team`v~RtEXtCopyright CC Attribution-ShareAlike http:/ /creativecommons.org/licenses/by-sa/4.0	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\preferences-system-network-proxy-symbolic.symbolic.png	0	287	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 3d 4e 03 31 14 04 fd 2f 10 fd fd 04 fd 34 14 1c 20 77 fd 0e 29 fd 02 fd 00 5c 21 47 fd 01 fd 53 fd 70 0a 0a 1a 3a 44 fd fd 20 25 10 36 45 6c fd 5a fd fd 32 fd 48 fd 37 fd 79 6f 6d 73 fd 3d fd fd 64 fd fd fd 0a 66 05 73 fd 34 67 fd 25 fd 26 fd 5d 24 fd 75 4b 2b fd 49 36 fd 13 fd 5a fd 2a fd fd fd fd 38 fd 79 41 3f fd 4d 10 fd 39 fd 75 0a fd 6a fd 51 fd fd 34 20 1e 4c fd 0a 61 59 0b 7b fd 6f 21 fd 07 0f 5d 26 fd fd 6d 62 fd fd 3a 0f 62 51 fd fd fd 6d fd 67 50 fd fd 2e fd 4e fd fd 3f 3f ff fd 3f fd 70 56 4b fd fd 0e fd 18 fd fd 20 7c 37 41 fd 76 fd fd fd 37 fd fd	PNGIHDRasBIT|dIDAT8 =N1/4 w)\!GSp:D %6ElZ2H7yoms=dfs4g% &]$uK+I6Z*8yA?M9ujQ4 LaY{o!]&mb:bQmg P.N???pVK |7Av7	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\printer-network.png	0	803	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 17 74 45 58 74 41 75 74 68 6f 72 00 4c 61 70 6f 20 43 61 6c 61 6d 61 6e 64 72 65 69 d1 1a 2a 00 00 00 27 74 45 58 74 44 65 73 63 72 69 70 74 69 6f 6e 00 42 61 73 65 64 20 6f 66 20 4a 61 6b 75 62 20 53 74 65 69 6e 65 72 20 77 6f 72 6b fd 29 38 5f 00 00 02 4a 49 44 41 54 38 fd fd fd fd 4f 54 41 14 fd 7f fd fd fd fd 55 fd fd 5c fd 30 61 fd fd 6d fd fd 58 fd 18 fd 17 13 3a 1f 09 31 24 fd 22 31 fd 44 0b 1b 6b fd fd fd 59 50 60 43	PNGIHDRasBIT|dpHYs+t EXtSoftwar ewww.inkscape.org<tEXt AuthorLapo Calamandrei*'tEXtDescr iptionBased of Jakub Steiner work)8_JIDAT8OTAU\0a mX:1$"1DkYP`C	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\selection-end-symbolic-rtl.symbolic.png	0	142	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 45 49 44 41 54 38 fd 63 60 18 fd fd 2f 03 03 fd 7f 2c fd 09 5d 21 fd 00 fd 60 fd 00 fd 06 54 52 6a 30 03 03 03 43 19 03 11 fd 48 fd 21 64 79 19 fd 10 fd fd 0c 66 08 fd 01 fd 44 1a 70 14 6a fd 21 28 3d fd 00 00 fd 53 15 fd fd fd 17 fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dEIDAT 8c`/,]!`TRj0CH!dyfDpj! (=SIENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\value-increase-symbolic.symbolic.png	0	113	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 28 49 44 41 54 38 fd 63 60 18 fd fd 3f 14 fd 04 4c fd fd 30 fd 06 30 fd fd fd fd 17 fd 3e fd 5d 40 08 fd fd 58 18 06 00 00 fd 05 0c fd 53 fd 77 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d(IDAT8c`?L00>]@XSwIENDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\zoom-out-symbolic.svg	0	335	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 34 20 31 20 63 20 2d 31 2e 36 36 30 31 35 36 20 30 20 2d 33 20 31 2e 33 33 39 38 34 34 20 2d 33 20 33 20 76 20 38 20 63 20 30 20 31 2e 36 36 30 31 35 36 20 31 2e 33 33 39 38 34 34 20 33 20 33 20 33 20 68 20 38 20 63 20 31 2e 36 36 30 31 35 36 20 30 20 33 20 2d 31 2e 33 33 39 38 34 34 20 33 20 2d 33 20 76 20 2d 38 20 63 20 30 20 2d 31 2e	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <path d="m 4 1 c -1.660156 0 -3 1.339844 -3 3 v 8 c 0 1.660156 1.339844 3 3 3 h 8 c 1.660156 0 3 -1.339844 3 -3 v -8 c 0 -1.	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe	unknown	512	success or wait	115	4061F5	ReadFile
C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsk7955.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsk7955.tmp	unknown	12354	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsk7955.tmp	unknown	4	success or wait	11	4061F5	ReadFile
C:\Users\user\Desktop\FRACCIONAMIENTO 1722403906461L.exe	unknown	16384	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\monotocardiac.dat	unknown	1048576	success or wait	1	72E62C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Finlandsrejserne	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Finlandsrejserne	SPRANGLING	dword	1	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly