ID: 694559
Sample Name: Order_002376662-579588_Date 24082022.exe
Cookbook: default.jbs
Time: 23:50:13
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

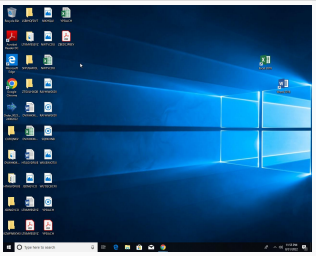
Windows Analysis Report

Order_002376662-579588_Date 24082022.exe

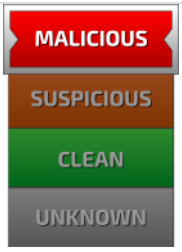
Overview

General Information

Sample Name:	Order_002376662-579588_Date 24082022.exe
Analysis ID:	694559
MD5:	8c2a59bd88b7e2..
SHA1:	7efb014d57608ff..
SHA256:	0d4b100e641aad.
Tags:	exe signed
Infos:	



Detection



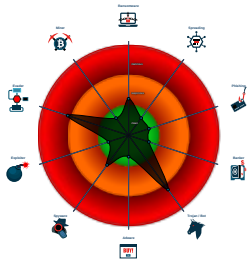
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect virtualization through…
- 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 (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- Order_002376662-579588_Date 24082022.exe (PID: 6508 cmdline: "C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe" MD5: 8C2A59BD88B7E2C26045A604ED544288)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.829249266.00000000030C0000.00000040.00001000.00020000.00000000.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

Multi AV Scanner detection for submitted file

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

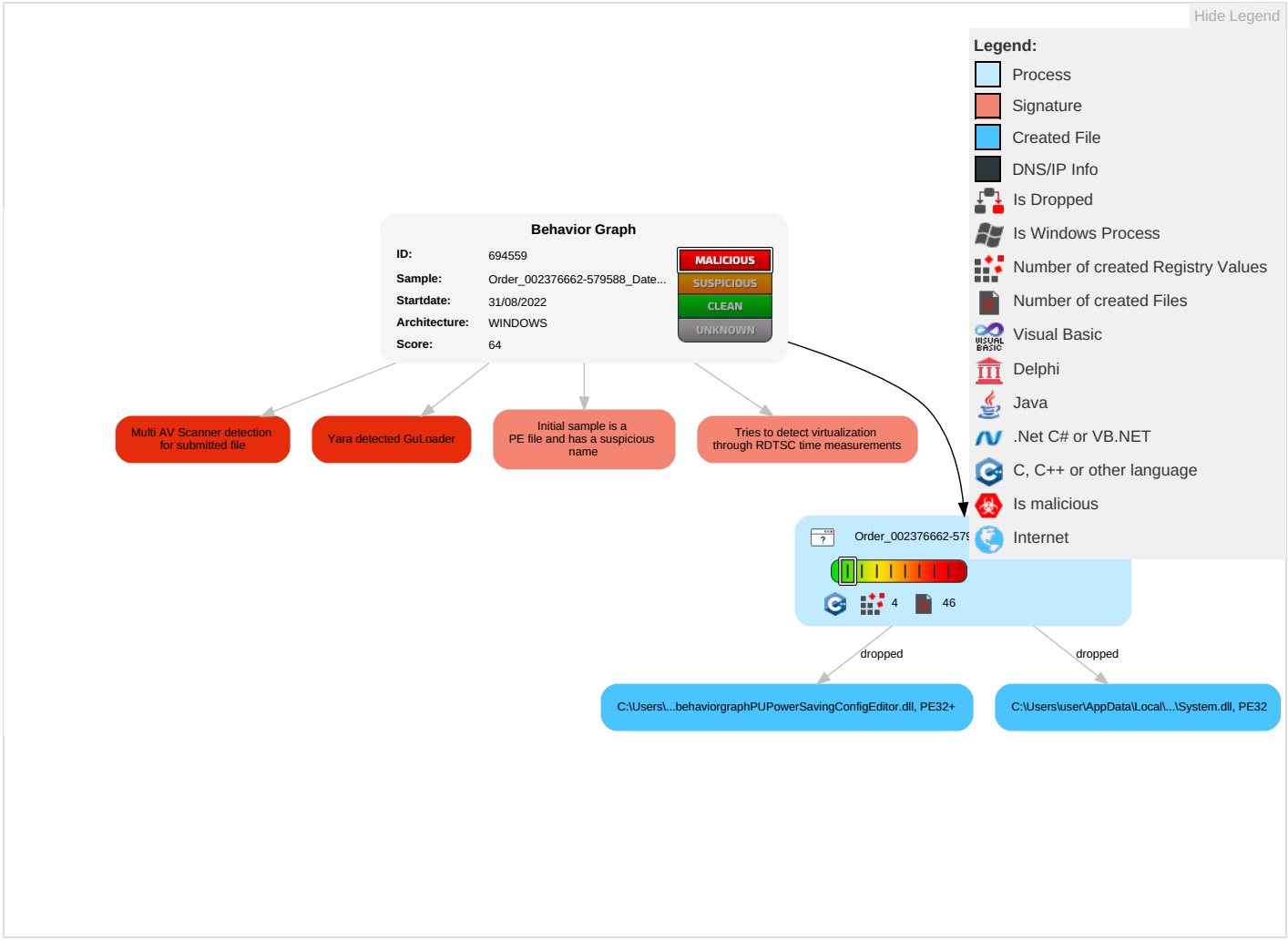
Malware Analysis System Evasion

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 1 Masquerading	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 Registry Run Keys / Startup Folder	1 Windows Service	1 Access Token Manipulation	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	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

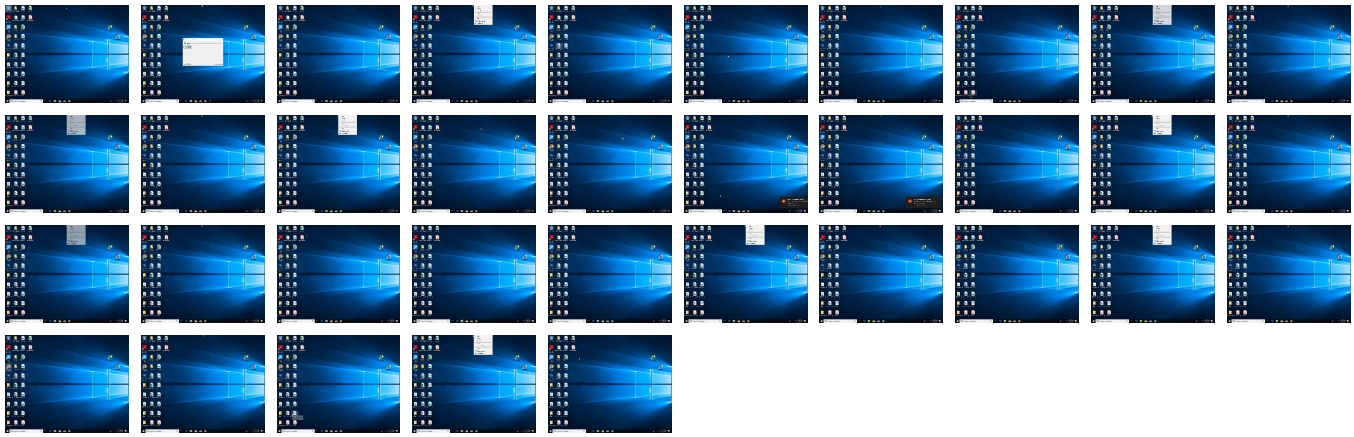
Behavior Graph



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
Order_002376662-579588_Date 24082022.exe	28%	Metadefender		Browse
Order_002376662-579588_Date 24082022.exe	65%	ReversingLabs	Win32.Trojan.Guloader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Hologr aph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Hologr aph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.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://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctnca2.crl0l	Order_002376662-579588_Date 24082022.exe	false		high
http://repository.certum.pl/ctnca2.cer09	Order_002376662-579588_Date 24082022.exe	false		high
http://crl.certum.pl/ctsca2021.crl0o	Order_002376662-579588_Date 24082022.exe	false		high
http://nsis.sf.net/NSIS_Error	Order_002376662-579588_Date 24082022.exe	false		high
http://repository.certum.pl/ctnca.cer09	Order_002376662-579588_Date 24082022.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Order_002376662-579588_Date 24082022.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	Order_002376662-579588_Date 24082022.exe	false		high
http://crl.certum.pl/ctnca.crl0k	Order_002376662-579588_Date 24082022.exe	false		high
http://subca.ocsp-certum.com05	Order_002376662-579588_Date 24082022.exe	false	• URL Reputation: safe	unknown
http://www.certum.pl/CPS0	Order_002376662-579588_Date 24082022.exe	false		high
http://subca.ocsp-certum.com02	Order_002376662-579588_Date 24082022.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	Order_002376662-579588_Date 24082022.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694559
Start date and time:	2022-08-31 23:50:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order_002376662-579588_Date 24082022.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	mal64.troj.evad.winEXE@1/7@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.6% (good quality ratio 61.3%) • Quality average: 89% • Quality standard deviation: 21.6%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.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
- VT rate limit hit for: Order_002376662-579588_Date 24082022.exe

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\nsb3C99.tmp\System.dll

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11264
Entropy (8bit):	5.767999234165119

Encrypted:	false
SSDEEP:	192:cPtkumJX7zBE2kGwfy9S9VkPsFQ1MZ1c:N7O2k5q9wA1MZa
MD5:	C9473CB90D79A374B2BA6040CA16E45C
SHA1:	AB95B54F12796DCE57210D65F05124A6ED81234A
SHA-256:	B80A5CBA69D1853ED5979B0CA0352437BF368A5CFB86CB4528EDADD410E11352
SHA-512:	EAFE7D5894622BC21F663BCA4DD594392EE0F5B29270B6B56B0187093D6A3A103545464FF6398AD32D2CF15DAB79B1F133218BA9BA337DDC01330B5ADA804D7 B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......)...m.m.m...k.m.~....j.9..i....l....l.Richm........................PE..L.....uY.. ....!................'.......0..............................`......................................2.......0..P...........................P......................................................0..X...........................text...O....... ................... ..`.rdata..S....0......."..............@..@.data...h....@.......&..............@....reloc..^....P.......(..............@..B... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Forhaanet.Nab

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	29564
Entropy (8bit):	3.9994965063204706
Encrypted:	false
SSDEEP:	768:K3xU0sST74YF3ZeaYDqKjmgtajzKmFGMiElvFoe2:2Tsusm3ODqK/Imlh
MD5:	61F8A1615921DA63C2609B90984F1D32
SHA1:	D188A91A6745481BB830704854FE61E2A41E0B9A
SHA-256:	DF023F32CE51FF8BA14F1147B1D7644D734AC9EF0FB5CF024A88A495E153EFF0
SHA-512:	9855CCCA3CF01993F04ECC48824FF8AD7084176F8A9411CF8E737FDAB5BB093B3FE19B8098D8206A1DFF546DA59D227D783470A2D1DCE1083C1FBC9661FBB3 C
Malicious:	false
Reputation:	low
Preview:	79F5033C9D5E8CB0E34E74DBA3F160A8A116FFBE99FFC4E7AB4189ABA94B8F01DD34E5CC3D75871F5B27143BFD1FAEF87C50308056EFCBC142ABE1F8 C638BE972D7DE340583A9C76BD7ED307EFB159E8EE7844BBA73F5DD7B1DF60CD378221F6BCB008205C718C5C3D2C9978871B0F9B8B02370F79F12DAB 84A9C7D793A5181FC249ED6136A6EF71E962E295EF440D9D4B0017F75253D1433B5E2E2BE721069D97AE1E0B31F4FC9F0CD109B46C79BA1D3F88D3DF 73715581039E00D83F9F0EC2B48A52CBC4A37AD6779E4997433AB97D75FF78AE1C1AA7755E884D821FD65138A7930C0213E6FE7694ABAF56071B3AF0 5D5FBC7401A6D776E5FD88DA61BCC05675FF42FCC1CBBE2894A439183B853B6C170C338105B38468CFF07EFEED9A85C335E2F04F08F2DC0F9C3243C5 319F3E4256A41FCB22BE16E71B4354F38E090AE14F8E7852031272A2063B58E48D78244C510AE6EE9C5387CFC359D0EE90882CDB81704DD368E0E963 E9E0F81DFF503D71BC346492203B0E95A7E6AF23DE1289F222F7DA779BD9B0921560969C5F3FA94C0B3E7C9E627C5ABA4EEEC74E5259BBB5F80C1393 C789B98CC7FEE06CB3AC2839022F745C4B8F402C5C24781278401E69ED99F56F08FD67C73117A09362CDAB03ED93295816298F51FBA17DEC31054D3E 4A8ACB306B2682E11BDB133A1C1E14017EC7D3BB

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\GPUPowerSavingConfig Editor.dll

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	31456
Entropy (8bit):	6.0996914820635295
Encrypted:	false
SSDEEP:	384:sQ1QmY/8eFuAYNAx4klQvhI0tUA9wZmjML9S/3oche5ZP2TFn0E0C04Haqk6Olkm:s0YvT4ZbzRj1foHGpzkkF2X9Dh/
MD5:	6213DFF7A0CE2E52FD61EC4097DF93E7
SHA1:	4087C8D803EE9E4298AA51EC05E18D020A0A2728
SHA-256:	D12DC4BBDACDE8FC92DCFB384807D793C67B9B7E88D52EE0240E8A1901B80071
SHA-512:	85446886691BE56B027519EB2C823399031CE549AA3BF8155A0E3897AAC04E4E8D960716E40E124E0E4980027CB3EB13241A9CF32D9227470F8E0EA45FFBC79D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..d..._p.a.........." ..0..T............... ....&.. ..`...@......@............... .................................`............\..............q... ..H............text....S... ...T.................. ..`.rsrc...`............V..............@. .@.......................................H.......x?...0..........Hp...(....*.~....-.r...p.....(....o....s.........~....*.~....*.......*V(....re..p~....o....*V(....rs..p~....o....*V(... .r...p~....o....*V(....r...p~....o....*.~....*..(....*Vs....(....t.........*.0...........{....o.....{.....3......{.....(....&(.....o .....5...o!...r...p....+A.......~"...(#...,....($....+..r...po%...-..{.....o&...r...p...X....i2.. .&...{....*....................0...........{....o.....{.....3.......{.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\face-cool.png

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	845
Entropy (8bit):	7.722985666159481
Encrypted:	false
SSDEEP:	24:47y7zZd6D14lz6mML1mc2TvTl4P5VwbxjoUWBx9:57mD14lz61gTv+P5Vwtj0
MD5:	EFB6B9E41A0DAAB0088A365317A4F635
SHA1:	5D5B2C92BB5870B15BFB383A4C749EE1B71E21AB
SHA-256:	40A5B74A33F7372AC62EC82CA65097B2BF411E6CAF2667C87DA374A06834AD05
SHA-512:	98BACE38224A53CCDA2039CD6089F704762A5D09D67CE924486800205596671A0BFC9A2BE26D36F77BAB7ECAF57E82C3D16739DBDA9FC1027A8E2B784D784C4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....IDATx.u..x.[..g]....m.f...m...=..y3...}.....V)..&.v.S.}.KYr..<.....n.%.....q..n.Q.W.j....2....(...N5.....1{.....&r/.....dE.1Tg^.!..T..F.C.:T.Ed..<.>.<.r..\.=..OIR.7Q..Ge.|P..`0....*X.....*.>.m.E.p....>...>..M.~.....*..*.H4k.7.Z=.d....D.S3..]....f.....E.....G.R.....'ND.}.eK...E.....V..... .....p.g..)&0$...N%dc..n.x:.i..C:...l.Vg^_....r._..9..(....G...$M.....}...u-.....}..o..Y.vLA.....-Z.K;<.....)...GW.ph..E..c]+.....c.p..#.p[...Q....G.#.....G.....Vu...q....).yl.2.....v.\.0Mz.P/.;B....F.....{.!..T..G.}.._....".2w.m../l.JHs.x..h.....t.....a!.M.....qk. ....IX/@...w.\...2U.....u^.&N3.G..t.....8...Z6].6~..`...+.....&.5&.*....ZO...$..Y..%...XF...^s[4...&.nw....?-./..T&.IS.H&.cX"...7..$c.....T.9....IEND.B`.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kalligraferendes\Quantisers\Aqua_20.bmp

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	8419
Entropy (8bit):	7.8975477212121925
Encrypted:	false
SSDEEP:	192:oXRnOJl+MmnEjHXjbDkd914gmMJrq03QVWpen7d:KRHMmn2XjXQ1VqaQVWs7d
MD5:	EF9954E2C8A46E6F0BB6AAF1E0A7F499
SHA1:	F1639B6632F6B4B472A4A0AD653B82A48B008F6B
SHA-256:	6550954EBF87A006EDA7C80EA5EB26CD51753540C159DEA36E506C811D5261DD
SHA-512:	F00EAD97959335F95B4846A7DA20A51C2B31E255F2C013DB69CF6F595E3C0BCE299C640001E2B265864528B576F161C9105AC237F09A906E74B9AF406D211D6D
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(..'...no./.....j..Z?...7..c....Z.....K.+.d....3....I.#..m@X|S...T.....g.]..eo...#XI...|D6.....D.....T.*....da<..i5..!.M...I.mC.W.<O.x._...x.....Q..3..<.....4..."...@..p..y..SX.L...v..[....].+_m.k.Y..b.*X.v:..z....A.A.....>.....f?..GG....s."..^.....=:e@.X.{.- T.....).....g...O....._[.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Noneffervescently.Cre

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
File Type:	data
Category:	dropped
Size (bytes):	105498
Entropy (8bit):	6.8469376549161245
Encrypted:	false
SSDEEP:	1536:cYUYKcQR5Y+GAjmU8R20KnRFr/ASso1gQa0CozxqDkHHB+Q/vGmHi:cYvuY+1J8R2bFbAYGQa09zxqDk++GmHi
MD5:	34957562BCFF2DAE97F8009F22642EA5
SHA1:	F22431D76E12B5E4AC240E96F6856165C70A01EE
SHA-256:	69823BE330A7C9B93750E25AFB3BC29DC33F7DE4CA7935D787BE29DD80E711D1
SHA-512:	015BE4CE81774A334761017AA7C0E397B2DE9F91904D87CDBA163CBD4C584FCBFF25A6C787595F31ABD0C24970101671C9444139088161F7C3A4E5B1634808A4
Malicious:	false
Preview:	2.1.].F..Q....H.....[.Geo.A,S.....n...+.|.....]..r.uh.%.Zng.#.;...2.a.>.....b@....f.m.....@u}.e.-..9...\P.2.(.!.z...#@..u.,.k..A9..q)}.....T...D.{.)f@z.,.....[{o.....)..S.p.&.....#SEu.L..F...mc}.....<..}lV.y.:.Z..N...8.....>.W..O...c9Q1@.~./.....6..... [8-..8EB...C.....X"x..`2[.f..P1..c.?.#.{..EvD....<6.D.,..1;p.b.....W#.4....N.G.).u.u...[JL.i.D.....@...W}).".3m...%.<..[....3.3...-7.z...{..$.ll.....7~...lV.....)y.....S.....@:.%2;]u.D..z.3..wv..6[.....*!..O..zEeT...:.8.../..C.P....H...).&n7-.t.....S...=.8].+..OsD.....v(...K..Ea5.+b.'...?..?.<....'..o.3.`.Zx.....3.<..7*...~....*..6.. >z..Z....d.6<..4).+.<...y..A...5..._..M!.$l]9.y.:...7Z.dD....}...C.M!1.Zt.1....0.)q.....=..HR....4..Z.&..s.W.....q..pRc.Q{.....S.X.....@.....+..OA.....oyw...b..*.G..d.|..b.)..... ..]YE.$.....$7U..7..P.Zh.2e.f...g...(..u...i..KB....j.. <Lts..)1...O^.X]\|[s...!.....\_5..$..-t.`#...T

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegnelserne\Suppegrydernes79\iso_3166-1.json

Process:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe

File Type:	UTF-8 Unicode text
Category:	dropped
Size (bytes):	36718
Entropy (8bit):	4.260373998588477
Encrypted:	false
SSDEEP:	192:OU+NvXvwEXFo+Hco8/+8IXAMaM2LkAAVemLK9f8QayVEJUfYZqAmULr:OU+Eo8ZLMaMWlAVemOZwyyOwMAmUX
MD5:	062FC6431BF0FF5F8E7E62587FCBD686
SHA1:	06E2BF1BB06CE408EC2AAE8D9F7A8ABC0371B57D
SHA-256:	78FB090F4A54C8B5970EC04C7511F17EB767275A8D5358604A1E335440678617
SHA-512:	8EC9F46A24C2A0B0C54463EF23D14563DDA2F7D65D8B231B994C8DDA2D5212B4DC697C6DF67B477DD245A2A065023383576A6DB48A335FAB9AFB6AAE7F7641 94
Malicious:	false
Preview:	{. "3166-1": [. {. "alpha_2": "AW",. "alpha_3": "ABW",. "name": "Aruba",. "numeric": "533". },. {. "alpha_2": "AF",. "alpha_3": "AFG",. "name": " Afghanistan",. "numeric": "004",. "official_name": "Islamic Republic of Afghanistan". },. {. "alpha_2": "AO",. "alpha_3": "AGO",. "name": "Angola",. "numeric": "024",. "official_name": "Republic of Angola". },. {. "alpha_2": "AI",. "alpha_3": "AIA",. "name": "Anguilla",. "numeric": "660". },. {. "alpha_2": "AX",. "alpha_3": "ALA",. "name": ".land Islands",. "numeric": "248". },. {. "alpha_2": "AL",. "alpha_3": "ALB",. "name": "Albania",. "numeric": "008",. "official_name": "Republic of Albania". },. {. "alpha_2": "AD",. "alpha_3": "AND",. "name": "Andorra",. "numeric": "020",. " official_name": "Principality of Andorra". },. {. "alpha_2

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.509543109745029
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:	Order_002376662-579588_Date 24082022.exe
File size:	195584
MD5:	8c2a59bd88b7e2c26045a604ed544288
SHA1:	7efb014d57608ff6a2805baf4dd7c150792e6eb4
SHA256:	0d4b100e641aad426a916cb326d20f8fe44e32ca38f7a85c505135036c6b44af
SHA512:	ca6d126b62418c1c9fe6b6c0b0418a7253b6200a179af844bd80f67c055375c51d9b268242ea9ff3e15b0c3d867d84c19508229580605cbaac8460fa9a9bec17
SSDEEP:	3072:RNzPHk9MpcDj6OzDjWubsfxAjaWde+mzaOyrxmIW//z7GfvGxkTjk3kfSD:RhRupsfKW7+me6//z7GvQ
TLSH:	7014F11D2507C7BECA53423049BA6A675EF6BA04FC8156436F637A983CD3170822F5BE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...*.uY.....b.....

File Icon

Icon Hash:	90b270f0e260b050

Static PE Info

General

Entrypoint:	0x40330d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5975952A [Mon Jul 24 06:35:22 2017 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:	57e98d9a5a72c8d7ad8fb7a6a58b3daf

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN="Fights Fratrkning Unnervingly ", OU="nerver Whitebait ", E=Nekrofili@Umiaq.An, O=Stagy, L=Kendallville, S=Indiana, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 2/20/2022 5:26:15 AM 2/19/2025 5:26:15 AM
Subject Chain	• CN="Fights Fratrkning Unnervingly ", OU="nerver Whitebait ", E=Nekrofili@Umiaq.An, O=Stagy, L=Kendallville, S=Indiana, C=US
Version:	3
Thumbprint MD5:	8BFEA38B193C49A0622C53FBF7CAADE9
Thumbprint SHA-1:	CA863CD76251E5155366225CECEF5915CDC6B279
Thumbprint SHA-256:	A8B4C4809B973CA3D72051C56C958A1F73702992E831E3DED8796A5C96627D06
Serial:	2F3B028675A5223C

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042472Ch], eax
je 00007EFC0CD39783h
push ebx
call 00007EFC0CD3C852h
cmp eax, ebx
je 00007EFC0CD39779h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007EFC0CD3C7CEh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007EFC0CD3975Dh
push 0000000Ah
call 00007EFC0CD3C826h
push 00000008h
call 00007EFC0CD3C81Fh
push 00000006h
mov dword ptr [00424724h], eax
call 00007EFC0CD3C813h
cmp eax, ebx
je 00007EFC0CD39781h
push 0000001Eh

Instruction
call eax
test eax, eax
je 00007EFC0CD39779h
or byte ptr [0042472Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [004247F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FCF0h
call dword ptr [00408178h]
push 0040A1ECh

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	0x8428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c000	0x74d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2d5a0	0x2660	.ndata
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	0x298	.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	0x603c	0x6200	False	0.6572464923469388	data	6.39361655287636	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1248	0x1400	False	0.4287109375	data	5.044261339836676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a838	0x400	False	0.6455078125	data	5.223134318413766	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x17000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c000	0x74d0	0x7600	False	0.4656382415254237	data	4.073204340591157	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3c358	0x25a8	data	English	United States
RT_ICON	0x3e900	0x10a8	data	English	United States
RT_ICON	0x3f9a8	0xea8	data	English	United States
RT_ICON	0x40850	0x988	data	English	United States
RT_ICON	0x411d8	0x8a8	data	English	United States
RT_ICON	0x41a80	0x6c8	data	English	United States
RT_ICON	0x42148	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x426b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x42b18	0x100	data	English	United States
RT_DIALOG	0x42c18	0x11c	data	English	United States
RT_DIALOG	0x42d38	0xc4	data	English	United States
RT_DIALOG	0x42e00	0x60	data	English	United States
RT_GROUP_ICON	0x42e60	0x76	data	English	United States
RT_VERSION	0x42ed8	0x2b4	data	English	United States
RT_MANIFEST	0x43190	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, CreateFileA, GetFileSize, GetModuleFileNameA, ReadFile, GetCurrentProcess, CopyFileA, Sleep, GetTickCount, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, SetCurrentDirectoryA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, GlobalUnlock, GetDiskFreeSpaceA, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

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: Order_002376662-579588_Date 24082022.exe PID: 6508, Parent PID: 5336

General

Target ID:	2
Start time:	23:51:11
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe"
Imagebase:	0x400000
File size:	195584 bytes
MD5 hash:	8C2A59BD88B7E2C26045A604ED544288
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: 00000002.00000002.829249266.00000000030C0000.00000040.00001000.00020000.00000000.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	40570F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsn2719.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405C95	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405C95	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsv2E8D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405C95	GetTempFileNameA
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	6	40570F	CreateDirectoryA
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	6	40570F	CreateDirectoryA
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	5	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	40570F	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsq2EBD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405C95	GetTempFileNameA
C:\Users\user\Videos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40570F	CreateDirectoryA
C:\Users\user\Videos\Etouffe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\Videos\Etouffe\Funktionserklringers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\Videos\Etouffe\Funktionserklringers\Cloque	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\Videos\Etouffe\Funktionserklringers\Cloque\Carportens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Noneffervescently.Cre	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	40570F	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kalligraferendes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kalligraferendes\Quantisers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kallig raferendes\Quantisers\Aqua_20.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Forhaanet.Nab	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Hologr aph\Towy\Dgnrytmers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Hologr aph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Hologr aph\Towy\Dgnrytmers\face-cool.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegnelserne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegn elserne\Suppegrydernes79	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570F	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegn elserne\Suppegrydernes79\iso_3166-1.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405C95	GetTempFileNameA
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	40570F	CreateDirectoryA
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	40570F	CreateDirectoryA
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	40570F	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	40570F	CreateDirectoryA
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	40570F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsb3C99.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	4056CF	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C5E	CreateFileA
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	374	405C5E	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsn2719.tmp	success or wait	1	403586	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp	success or wait	1	405890	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	30162	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	405CF3	WriteFile
unknown	30162	24522	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	405CF3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Noneffervescently.Cre	0	16384	32 17 31 fd 5d fd 46 fd fd 51 fd fd 1d fd 48 fd fd fd 7f fd 10 fd fd 5b 2b 47 65 6f fd 41 2c 53 fd 02 fd 0f fd 04 fd 16 6e fd fd fd 2b fd 7c 05 0d fd 0e fd 0d fd 5d 31 fd 72 fd 75 68 fd 25 fd 5a 6e 67 1c 23 fd 3b fd 1e 16 32 fd 61 fd 3e fd 1d fd fd fd 62 40 ff fd fd 1c 66 fd 6d fd fd 2f 2e fd 1f fd 0f 0b 0d 40 75 7d fd 65 fd 2d fd fd 39 fd 1d fd 5c 50 fd 32 fd 28 fd 21 fd 7a fd fd fd 23 40 fd 1a 75 01 2c fd 6b 1b fd 41 39 fd fd 71 29 7d fd fd 1b 01 09 54 fd 09 fd 44 fd 7b fd 29 66 40 7a fd 2c fd 12 1f fd a4 5b 7b 6f fd fd 02 fd 05 29 2e fd 53 fd 70 7f 26 13 fd 07 06 fd 23 53 45 75 fd 4c fd 0b 46 15 fd fd 6d 63 7d fd fd fd fd fd 04 fd 3c fd 0c 7d 6c 56 fd 79 fd 3a 3d 5a fd fd 4e fd c7 fd 38 fd fd fd fd 01 11	21]FQH[GeoA,Sn+|]ruh%Zng#;2a>b@fm.@u}e-9\P2(!z#@u,kA9q)}TD{}f@z,[{o).Sp&#SEuLFmc}<}lVy:ZN8	success or wait	7	405CF3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kalligraferendes\Quantisers\Aqua_20.bmp	0	8419	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	405CF3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Forhaanet.Nab	0	16384	37 39 46 35 30 33 33 43 39 44 35 45 38 43 42 30 45 33 34 45 37 34 44 42 41 33 46 31 36 30 41 38 41 31 31 36 46 46 42 45 39 39 46 46 43 34 45 37 41 42 34 31 38 39 41 42 41 39 34 42 38 46 30 31 44 44 33 34 45 35 43 43 33 44 37 35 38 37 31 46 35 42 32 37 31 34 33 42 46 44 31 46 41 45 46 38 37 43 35 30 33 30 38 30 35 36 45 46 43 42 43 31 34 32 41 42 45 31 46 38 43 36 33 38 42 45 39 37 32 44 37 44 45 33 34 30 35 38 33 41 39 43 37 36 42 44 37 45 44 33 30 37 45 46 42 31 35 39 45 38 45 45 37 38 34 34 42 42 41 37 33 46 35 44 44 37 42 31 44 46 36 30 43 44 33 37 38 32 32 31 46 36 42 43 42 30 30 38 32 30 35 43 37 31 38 43 35 43 33 44 32 43 39 39 37 38 38 37 31 42 30 46 39 42 38 42 30 32 33 37 30 46 37 39 46 31 32 44 41 42 38 34 41 39 43 37 44 37 39 33 41 35 31 38 31	79F5033C9D5E8CB0E34E74DBA3F160A8A116FFBE99FFC4E7AB4189ABA94B8F01DD34E5CC3D75871F5B27143BFD1FAEF87C50308056EFCBC142ABE1F8C638BE972D7DE340583A9C76BD7ED307EFB159E8EE7844BBA73F5DD7B1DF60CD378221F6BCB008205C718C5C3D2C9978871B0F9B8B02370F79F12DAB84A9C7D793A5181	success or wait	2	405CF3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.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 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 02 00 5f 70 fd 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 30 00 00 54 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 fd 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 26 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_pa" 0T &` @@	success or wait	2	405CF3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\face-cool.png	0	845	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 03 14 49 44 41 54 78 01 75 fd 03 78 1c 5b 00 fd 67 5d fd fd fd 6d fd 66 fd fd 36 6d f6 1d f6 3d fd fd 79 33 fd fd fd 7d fd fd fd 03 fa fd 56 29 fd fd 26 fd 76 fd 53 11 7d fd 4b 59 72 fd a7 3c fd fd 06 fd fd fd 6e 13 25 fd fd 89 09 fd fd 71 fd fd 6e fd 51 fd 57 fd 6a 0b fd fd fd 32 fd 04 fd 13 28 0a c5 fd 4e 35 17 fd 68 fd fd 31 7b 18 fd fd fd fd fd 26 72 2f fd 1d fd fd fd fd fd 64 45 fd 31 54 67 5e fd 21 fd 1d 54 fd fd 46 03 43 fd 3a 54 fd 45 64 fd 15 3c fd 3e fd 3c fd 72 fd d5 5c 8f 3d fd fd 4f 49 52 fd 37 51 19 fd 47 65 fd 7c 50 fd fd 60 30 fd fd fd fd 2a 58 fd fd 39 fd fd fd 00 2a fd	PNGIHDRaIDATxux[g]mfm=y3}V)&vS }KYr<n%qnQWj2(N51{&r/dE1Tg^!TFC:TEd<> <r\=OIR7QGe|P`0*X*	success or wait	1	405CF3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegnelserne\Suppegrydernes79\iso_3166-1.json	0	16384	7b 0a 20 20 22 33 31 36 36 2d 31 22 3a 20 5b 0a 20 20 20 20 7b 0a 20 20 20 20 20 20 22 61 6c 70 68 61 5f 32 22 3a 20 22 41 57 22 2c 0a 20 20 20 20 20 20 22 61 6c 70 68 61 5f 33 22 3a 20 22 41 42 57 22 2c 0a 20 20 20 20 20 20 22 6e 61 6d 65 22 3a 20 22 41 72 75 62 61 22 2c 0a 20 20 20 20 20 20 22 6e 75 6d 65 72 69 63 22 3a 20 22 35 33 33 22 0a 20 20 20 20 7d 2c 0a 20 20 20 20 7b 0a 20 20 20 20 20 20 22 61 6c 70 68 61 5f 32 22 3a 20 22 41 46 22 2c 0a 20 20 20 20 20 20 22 61 6c 70 68 61 5f 33 22 3a 20 22 41 46 47 22 2c 0a 20 20 20 20 20 20 22 6e 61 6d 65 22 3a 20 22 41 66 67 68 61 6e 69 73 74 61 6e 22 2c 0a 20 20 20 20 20 20 22 6e 75 6d 65 72 69 63 22 3a 20 22 30 30 34 22 2c 0a 20 20 20 20 20 20 22 6f 66 66 69 63 69 61 6c 5f 6e 61 6d 65 22 3a 20 22 49 73 6c	{ "3166-1": [{ "alpha_2": "AW", "alpha_3": "ABW", "name": "Aruba", "numeric": "533" }, { "alpha_2": "AF", "alpha_3": "AFG", "name": "Afghanistan", "numeric": "004", "official_name": "Isl	success or wait	3	405CF3	WriteFile
C:\Users\user\AppData\Local\Temp\nsb3C99.tmp\System.dll	0	11264	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 29 fd fd fd 6d fd 6d fd 6d fd fd bd 6b fd 6d fd 7e b3 6e fd fd 6a fd 39 4c fd 69 fd 0e 16 fd 6c b3 52 b8 fd 6c fd 52 69 63 68 6d fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 07 fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$)mmmkm~j9illRichmPELuY!	success or wait	1	405CF3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe	unknown	512	success or wait	128	405CC4	ReadFile
C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe	unknown	16384	success or wait	1	405CC4	ReadFile
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	unknown	4	success or wait	1	405CC4	ReadFile
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	unknown	11490	success or wait	1	40312C	ReadFile
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	unknown	4	success or wait	6	405CC4	ReadFile
C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe	unknown	16384	success or wait	7	405CC4	ReadFile
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	unknown	16384	success or wait	16	405CC4	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Forhaanet.Nab	unknown	1	success or wait	1023	405CC4	ReadFile
C:\Users\user\AppData\Local\Temp\nsi2749.tmp	unknown	4	success or wait	1	405CC4	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Noneffervescently.Cre	unknown	1048576	success or wait	1	100028A5	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Platooned	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Platooned\Ananthropism	success or wait	1	405F7C	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Trakeotomis	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fallalishly	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Outsnores	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Outsnores\Begre	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Outsnores\Begre\Bonusernes	success or wait	1	405F7C	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Outsnores\Begre\Bonusernes\Skovdistrikts	success or wait	1	405F7C	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Platooned\Ananthropism	Swithen	dword	1	success or wait	1	40245E	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Trakeotomis	Brndboringen	unicode	Micasts	success or wait	1	40245E	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fallalishly	Navigationsskoler	dword	0	success or wait	1	40245E	RegSetValueExA
HKEY_CURRENT_USER\Software\Outsnores\Begre\Bonusernes\Skovdistrikts	Chold146	expand unicode	%WINDIR%\Afhandlingers\reseason.Unp4	success or wait	1	40245E	RegSetValueExA

Disassembly

No disassembly