

JOeSandbox Cloud BASIC



ID: 694559

Sample Name:

Order_002376662-579588_Date
24082022.exe

Cookbook: default.jbs

Time: 23:59:12

Date: 31/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report Order_002376662-579588_Date 24082022.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Memory Dumps	4
Sigma Signatures	4
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
System Summary	5
Data Obfuscation	5
Malware Analysis System Evasion	5
HIPS / PFW / Operating System Protection Evasion	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
World Map of Contacted IPs	8
Public IPs	9
General Information	9
Warnings	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
C:\Users\user\AppData\Local\Temp\nsa7CF6.tmp\System.dll	10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Forhaanet.Nab	11
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.dll	11
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\face-cool.png	11
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Kalligraferendes\Quantisers\Aqua_20.bmp	12
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Noneffervescently.Cre	12
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Tilegnelserne\Suppegrydernes79\iso_3166-1.json	12
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Authenticode Signature	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	15
Sections	15
Resources	15
Imports	16
Possible Origin	16
Network Behavior	16
Snort IDS Alerts	16
Network Port Distribution	16
TCP Packets	17
UDP Packets	19
DNS Queries	19
DNS Answers	19

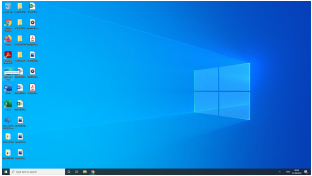
Statistics	19
Behavior	19
System Behavior	19
Analysis Process: Order_002376662-579588_Date 24082022.exePID: 2812, Parent PID: 5772	19
General	19
File Activities	20
Registry Activities	20
Analysis Process: CasPol.exePID: 3112, Parent PID: 2812	20
General	20
File Activities	20
Analysis Process: conhost.exePID: 4392, Parent PID: 3112	20
General	20
File Activities	20
Disassembly	21

Windows Analysis Report

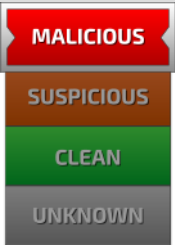
Order_002376662-579588_Date 24082022.exe

Overview

General Information

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

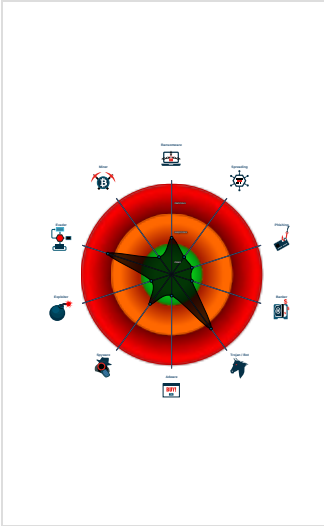
Detection

	
	
Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Yara detected GuLoader
Snort IDS alert for network traffic
Initial sample is a PE file and has a...
Writes to foreign memory regions
Tries to detect Any.run
Tries to detect sandboxes and other...
Uses 32bit PE files
May sleep (evasive loops) to hinder...
Contains functionality to shutdown /...
Uses code obfuscation techniques (...)
Tries to connect to HTTP servers, b...

Classification



Process Tree

- System is w10x64native
-  Order_002376662-579588_Date 24082022.exe (PID: 2812 cmdline: "C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe" MD5: 8C2A59BD88B7E2C26045A604ED544288)
 -  CasPol.exe (PID: 3112 cmdline: "C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 -  conhost.exe (PID: 4392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.22683438457.0000000000F70000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000002.27549390202.0000000000F70000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.23342945270.0000000003500000.0000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures	
ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.11.20 - Destination IP: 1.1.1.1	
Timestamp:	192.168.11.201.1.1.150882532012811 09/01/22-00:01:35.227375
SID:	2012811
Source Port:	50882
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

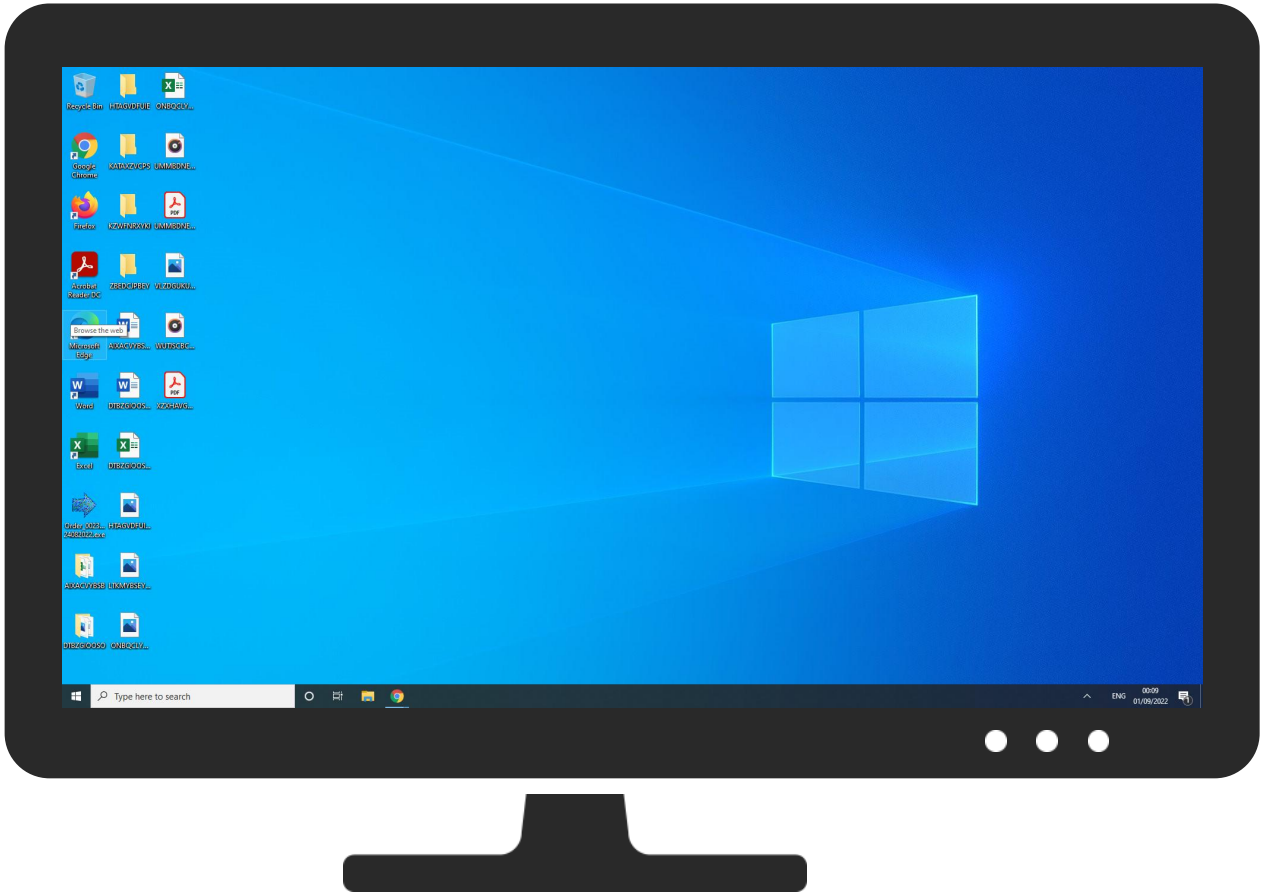
Tries to detect Any.run

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

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	1Native API	1Windows Service	1Access Token Manipulation	11Masquerading	OS Credential Dumping	221Security Software Discovery	Remote Services	1Archive Collected Data	Exfiltration Over Other Network Medium	1Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1Registry Run Keys / Startup Folder	1Windows Service	12Virtualization/Sandbox Evasion	LSASS Memory	12Virtualization/Sandbox Evasion	Remote Desktop Protocol	1Clipboard Data	Exfiltration Over Bluetooth	1Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout



Antivirus, Machine Learning and Genetic Malware Detection				
Initial Sample				
Source	Detection	Scanner	Label	Link
Order_002376662-579588_Date 24082022.exe	49%	Virustotal		Browse
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\lnsa7CF6.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lnsa7CF6.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\Towy\Dgnrytmers\GPUPowerSavingConfigEditor.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Sigtelinjens\Tvtningerne\Holograph\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%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mnhckm.tk	45.8.132.92	true	false		unknown

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	Avira URL Cloud: 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	Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	Order_002376662-579588_Date 24082022.exe	false	Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.132.92	mnhckm.tk	Germany		61317	ASDETUKhttpwwwheficedcomGB	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694559
Start date and time:	2022-08-31 23:59:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
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 20H2 Native physical Machine for testing VM-aware malware (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301)
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	24
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:	mal80.troj.evad.winEXE@4/7@1/1
EGA Information:	Successful, ratio: 50%

HDC Information:	- Successful, ratio: 24.4% (good quality ratio 24.1%) - Quality average: 88.7% - Quality standard deviation: 20.8%
HCA Information:	- Successful, ratio: 92% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Found application associated with file extension: .exe - Adjust boot time - Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, wdcplalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcpl.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target CasPol.exe, PID 3112 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

-  No simulations

Joe Sandbox View / Context

IPs

-  No context

Domains

-  No context

ASNs

-  No context

JA3 Fingerprints

-  No context

Dropped Files

-  No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsa7CF6.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:	EAFE7D5894622BC21F663BCA4DD594392EE0F5B29270B6B56B0187093D6A3A103545464FF6398AD32D2CF15DAB79B1F133218BA9BA337DDC01330B5ADA804D 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.. !.....O.....2.....O..P.....P.....0..X......text...O.....`rdata..S...O.....".....@..@..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:K3xU0sST74YF3ZeaYDqKjmgtajzKmFGMiElvFoe2:2Tsum3ODqK/lmlh
MD5:	61F8A1615921DA63C2609B90984F1D32
SHA1:	D188A91A6745481BB830704854FE61E2A41E0B9A
SHA-256:	DF023F32CE51FF8BA14F1147B1D7644D734AC9EF0FB5CF024A88A495E153EFF0
SHA-512:	9855CCCA3CF01993F04ECC48824FF8AD7084176F8A9411CF8E737FDAB5BB093B3FE19B8098D8206A1DFF546DA59D227D783470A2D1DCE1083C1FBC9661FBB3 C
Malicious:	false
Reputation:	low
Preview:	79F5033C9D5E8CB0E34E74DBA3F160A8A116FFB8E99FFC4E7AB4189ABA94B8F01DD34E5CC3D75871F5B27143BFD1FAEF87C50308056EFCBC142ABE1F8 C638BE972D7DE340583A9C76BD7ED307EFB159E8EE7844BBA73F5DD7B1DF60CD378221F6BCB008205C718C5C3D2C9978871B0F9B8B02370F79F12DAB 84A9C7D793A5181FC249ED6136A6EF71E962E295EF440D9D4B0017F75253D1433B5E2E2BE721069D97AE1E0B31F4FC9F0CD109B46C79BA1D3F88D3DF 73715581039E00D83F9F0EC2B48A52CBC4A37AD6779E4997433AB97D75FF78AE1C1AA7755E884D821FD65138A7930C0213E6FE7694ABAF56071B3AF0 5D5FBC7401A6D776E5FD88DA61BCC05675FF42FCC1CBBE2894A439183B853B6C170C338105B38468CFF07EFEE9A85C335E2F04F08F2DC0F9C3243C5 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/8eFuAYNAX4kiQvhl0tUA9wZmjML9S/3oche5ZP2TFn0E0C04Haqk6Olkm:s0YvT4ZbzRj1foHGpzkkf2X9Dh/
MD5:	6213DFFF7A0CE2E52FD61EC4097DF93E7
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....." ..O..T..... ..&.. ...@.....@.....\.....q......H......text...S... ..T..... ..rsrc... ..V.....@.. ..@.....H.....x?...0.....Hp.....(*~-.f..p....(....o.s.....~...*~...*V(....re..p~...o....*V(.. ...p~...o....*V(....f..p~...o....*~...*(....*Vs...(....t.....*0.....{....o....{....3....{....(....&(....oS...o!...f...p....+A.....~*...(#.....(\$...+..f...po%...~..{....o&...f...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
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.X/@...w.l..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:	F1639B6632F6B4B72A4A0AD653B82A48B008F6B
SHA-256:	6550954EBF87A006EDA7C80EA5EB26CD51753540C159DEA36E506C811D5261DD
SHA-512:	F00EAD97959335F95B4846A7DA20A51C2B31E255F2C013DB69CF6F595E3C0BCE299C640001E2B265864528B576F161C9105AC237F09A906E74B9AF406D211D6C
Malicious:	false
Preview:	JFIF.....d.d.....:Exif..MM.*.....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....l.#..m@X S...T....g.].eo...#Xl...[D6.....D.....T.*....da<..i5..!M...l.mC.W.<O.x_...x.....Q..3.<....4..."@...p ..y..SX.L...v..[...].+_m.k.Y..b.*X.v:...A.A.....>.....?..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].....<.)jV.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.....@...Wj})."3m...%. <.[...3.3.-7.z...-f.\$ll.....7~...lV.....)y.....S.....@.:%2;]u.D..z.3..wv..6[.....*l..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!.\$[j9.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\Suppegyrdernes79\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/+8lXAMaM2LkAAVemLK9f8QayVEJUfYZqAmULr:OU+Eo8ZLMaMWIAVemOZWyyOwMAmUX
MD5:	062FC6431BF0FF5F8E7E62587FCBD686
SHA1:	06E2BF1BB06CE408EC2AAE8D9F7A8ABC0371B57D
SHA-256:	78FB090F4A54C8B5970EC04C7511F17EB767275A8D5358604A1E335440678617
SHA-512:	8EC9F46A24C2A0B0C54463EF23D14563DDA2F7D65D8B231B994C8DDA2D5212B4DC697C6DF67B477DD245A2A065023383576A6DB48A335FAB9AFB6AAE7F764194
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:RNzPHk9MpcDj6OzDjWubsfxAjAWe+mzaOyrxmlW//z7GfvGxkJk3kfSD: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=Nekrofilii@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	20/02/2022 13:26:15 19/02/2025 13:26:15
Subject Chain	CN="Fights Fratrkning Unnervingly ", OU="nerver Whitebait ", E=Nekrofilii@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 00007FCB6CAB7F03h
push ebx
call 00007FCB6CABAFD2h
cmp eax, ebx
je 00007FCB6CAB7EF9h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007FCB6CABAF4Eh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FCB6CAB7EDDh
push 0000000Ah
call 00007FCB6CABAF6h
push 00000008h
call 00007FCB6CABAF9Fh
push 00000006h
mov dword ptr [00424724h], eax
call 00007FCB6CABAF93h
cmp eax, ebx
je 00007FCB6CAB7F01h
push 0000001Eh
call eax
test eax, eax
je 00007FCB6CAB7EF9h
or byte ptr [0042472Fh], 00000040h

Instruction
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

Name	RVA	Size	Type	Language	Country
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, IstrlenA, GetVersion, SetErrorMode, IstrcpynA, ExitProcess, SetCurrentDirectoryA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, WriteFile, IstrcpyA, MoveFileExA, Istrcata, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, IstrcmpiA, GlobalUnlock, GetDiskFreeSpaceA, IstrcmpA, 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

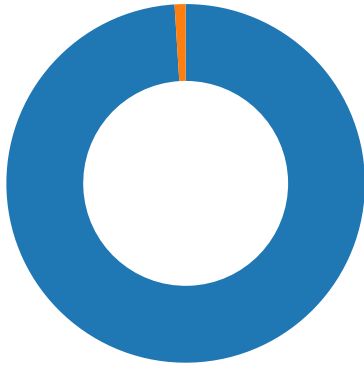
Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior							
Snort IDS Alerts							
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.201.1.1.150882532012811 09/01/22-00:01:35.227375	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	50882	53	192.168.11.20	1.1.1.1

Network Port Distribution

Total Packets: 101

- 53 (DNS)
- 80 (HTTP)



TCP Packets

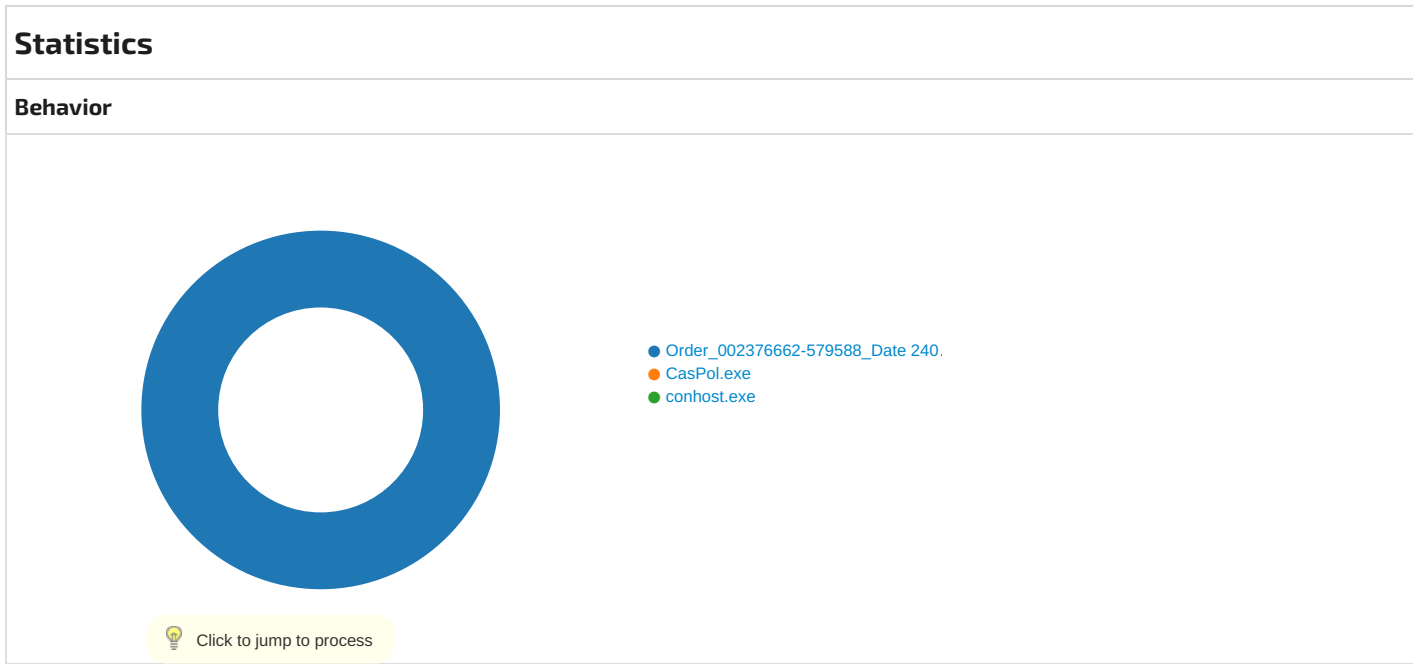
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:01:35.308299065 CEST	49785	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:36.315388918 CEST	49785	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:38.330445051 CEST	49785	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:40.369848967 CEST	49786	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:41.376629114 CEST	49786	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:43.391850948 CEST	49786	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:45.408461094 CEST	49787	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:46.422430038 CEST	49787	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:48.437733889 CEST	49787	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:50.456871033 CEST	49788	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:51.468318939 CEST	49788	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:53.483436108 CEST	49788	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:55.499950886 CEST	49792	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:56.513902903 CEST	49792	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:01:58.529259920 CEST	49792	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:00.562407970 CEST	49793	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:01.575304985 CEST	49793	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:03.590568066 CEST	49793	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:05.609458923 CEST	49796	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:06.621233940 CEST	49796	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:08.636473894 CEST	49796	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:10.652667999 CEST	49797	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:11.666898012 CEST	49797	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:13.682023048 CEST	49797	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:15.698669910 CEST	49799	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:16.712882042 CEST	49799	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:18.727937937 CEST	49799	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:20.730597019 CEST	49800	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:21.742830992 CEST	49800	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:23.758183002 CEST	49800	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:25.764751911 CEST	49801	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:26.773145914 CEST	49801	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:28.788141966 CEST	49801	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:30.804523945 CEST	49802	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:31.818802118 CEST	49802	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:33.834007978 CEST	49802	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:35.852221966 CEST	49803	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:36.864648104 CEST	49803	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:38.879693031 CEST	49803	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:40.911767960 CEST	49805	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:41.925821066 CEST	49805	80	192.168.11.20	45.8.132.92

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:02:43.941128969 CEST	49805	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:45.957909107 CEST	49806	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:46.971666098 CEST	49806	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:48.986955881 CEST	49806	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:51.005455017 CEST	49807	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:52.017404079 CEST	49807	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:54.032732010 CEST	49807	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:56.049453020 CEST	49808	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:57.063225985 CEST	49808	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:02:59.078370094 CEST	49808	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:01.079262972 CEST	49810	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:02.093373060 CEST	49810	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:04.108613014 CEST	49810	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:06.111105919 CEST	49812	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:07.123639107 CEST	49812	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:09.138787985 CEST	49812	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:11.155225992 CEST	49813	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:12.169295073 CEST	49813	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:14.184425116 CEST	49813	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:16.201354027 CEST	49814	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:17.215018988 CEST	49814	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:19.230299950 CEST	49814	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:21.264312983 CEST	49815	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:22.276478052 CEST	49815	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:24.291551113 CEST	49815	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:26.307991982 CEST	49817	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:27.322268963 CEST	49817	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:29.321742058 CEST	49817	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:31.353950977 CEST	49818	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:32.367949963 CEST	49818	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:34.383192062 CEST	49818	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:36.400821924 CEST	49819	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:37.413822889 CEST	49819	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:39.428946972 CEST	49819	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:41.429650068 CEST	49820	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:42.443809986 CEST	49820	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:44.459158897 CEST	49820	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:46.459882021 CEST	49821	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:47.474100113 CEST	49821	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:49.489119053 CEST	49821	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:51.508166075 CEST	49822	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:52.519743919 CEST	49822	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:54.535005093 CEST	49822	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:56.552083969 CEST	49823	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:57.565715075 CEST	49823	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:03:59.580818892 CEST	49823	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:01.615175009 CEST	49825	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:02.626914978 CEST	49825	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:04.642173052 CEST	49825	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:06.660598993 CEST	49826	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:07.672652006 CEST	49826	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:09.688244104 CEST	49826	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:11.704653025 CEST	49827	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:12.718499899 CEST	49827	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:14.733779907 CEST	49827	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:16.750761986 CEST	49828	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:17.764363050 CEST	49828	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:19.779428959 CEST	49828	80	192.168.11.20	45.8.132.92
Sep 1, 2022 00:04:21.781795979 CEST	49829	80	192.168.11.20	45.8.132.92

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:01:35.227375031 CEST	50882	53	192.168.11.20	1.1.1.1
Sep 1, 2022 00:01:35.296704054 CEST	53	50882	1.1.1.1	192.168.11.20

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:01:35.227375031 CEST	192.168.11.20	1.1.1.1	0x8709	Standard query (0)	mnhckm.tk	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 1, 2022 00:01:35.296704054 CEST	1.1.1.1	192.168.11.20	0x8709	No error (0)	mnhckm.tk		45.8.132.92	A (IP address)	IN (0x0001)



System Behavior	
Analysis Process: Order_002376662-579588_Date 24082022.exe PID: 2812, Parent PID: 5772	
General	
Target ID:	2
Start time:	00:01:06
Start date:	01/09/2022
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: 00000002.00000002.23342945270.0000000003500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low
-------------	-----

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: CasPol.exe PID: 3112, Parent PID: 2812

General

Target ID:	4
Start time:	00:01:25
Start date:	01/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Order_002376662-579588_Date 24082022.exe"
Imagebase:	0xb90000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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: 00000004.00000000.22683438457.0000000000F70000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.27549390202.0000000000F70000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 4392, Parent PID: 3112

General

Target ID:	5
Start time:	00:01:25
Start date:	01/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c1b30000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

 No disassembly