

JoeSandbox Cloud BASIC



ID: 830618

Sample Name: Quotation.exe

Cookbook: default.jbs

Time: 14:46:25

Date: 20/03/2023

Version: 37.0.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report Quotation.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Threat Intel	4
Malware Configuration	4
Yara Signatures	5
Dropped Files	5
Memory Dumps	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
System Summary	5
Data Obfuscation	5
Malware Analysis System 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	8
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	9
General Information	9
Warnings	9
Simulations	9
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\Microsoft\Windows\INetCache\Ghetto\Blegnbetheden\Telegrammers.Non	10
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Cohesion\Quakily\Privileger.Fla	10
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Cohesion\Quakily\SolutionExplorerCLI.dll	11
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Cohesion\Quakily\System.Security.Cryptography.X509Certificates.dll	11
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\System.dll	11
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\libdatr1e-1.dll	12
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\libpkcs11-helper-1.dll	12
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\maintenanceservice2.exe	13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\percentile.dll	13
C:\Users\user\AppData\Local\Temp\inst891E.tmp\System.dll	13
Static File Info	14
General	14
File Icon	14
Static PE Info	14
General	14
Authenticode Signature	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	16
Sections	16
Resources	16
Imports	16
Possible Origin	17
Network Behavior	17
Statistics	17

System Behavior

Analysis Process: Quotation.exePID: 2684, Parent PID: 3452

General

File Activities

File Created

File Deleted

File Written

File Read

Registry Activities

Key Created

Key Value Created

Disassembly

17

17

17

18

18

20

20

25

25

25

26

26

Windows Analysis Report

Quotation.exe

Overview

General Information

Sample Name:

Quotation.exe

Analysis ID:

830618

MD5:

8a81948116d2...

SHA1:

5cf4113debe6d..

SHA256:

5a64a3fd65f71...

Tags:

exe

guloader

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Yara detected GuLoader

Yara detected Generic Downloader

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 ...

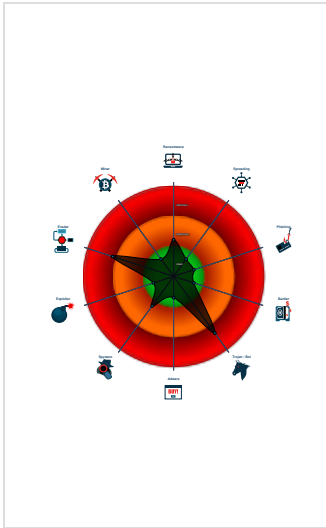
Drops PE files

Contains functionality to shutdown /...

Uses code obfuscation techniques (...)

PE file contains sections with non-s...

Classification



Process Tree

System is w10x64

Quotation.exe (PID: 2684 cmdline: C:\Users\user\Desktop\Quotation.exe MD5: 8A81948116D2EA79BEE1D261733DBA89)

cleanup

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-useringhttps://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecnica-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\System.dll	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.773629937.0000000005789000.0000040.00001000.00020000.00000000.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

Networking



Yara detected Generic Downloader

System Summary



Initial sample is a PE file and has a suspicious name

Data Obfuscation



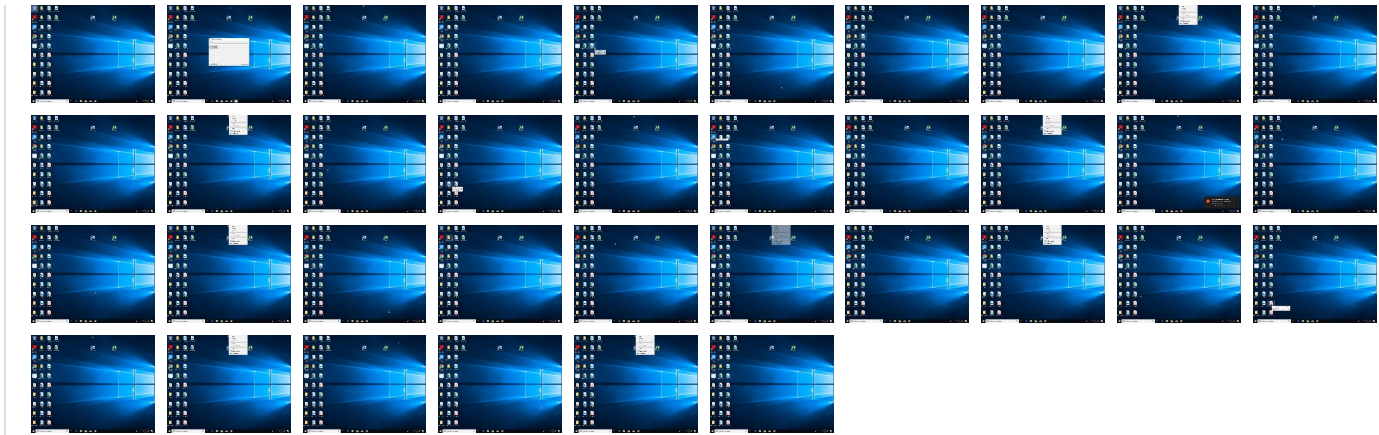
Yara detected GuLoader

Malware Analysis System Evasion



Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix



Antivirus, Machine Learning and Genetic Malware Detection				
Initial Sample				
Source	Detection	Scanner	Label	Link
Quotation.exe	19%	Virustotal		Browse
Quotation.exe	26%	ReversingLabs	Win32.Trojan.Genetic	

Dropped Files				
Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Cohesion\Quakily\SolutionExplorerCLI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Cohesion\Quakily\System.Security.Cryptography.X509Certificates.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\libdatrie-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Forureningsforebygget\Pegboard\libpkcs11-helper-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Forureningsforebygget\Pegboard\maintenanceservice2.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\iNetCache\Ghetto\Forureningsforebygget\Pegboard\percentile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\inst891E.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files					
Source	Detection	Scanner	Label	Link	Download
0.0.Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.2.Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains	
 No Antivirus matches	

URLs				
Source	Detection	Scanner	Label	Link
http://https://mozilla.org0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	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://nsis.sf.net/NSIS_Error	Quotation.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Quotation.exe	false		high
http://https://aka.ms/dotnet-warnings/	Quotation.exe, 00000000.00000003.252894237.00000000027AA000.00000004.00000020.00020000.00000000.sdmp, System.Security.Cryptography.X509Certificates.dll.0.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	Quotation.exe, 00000000.00000003.252069193.00000000027A3000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://www.symauth.com/cps0(	Quotation.exe, 00000000.00000003.252069193.00000000027A3000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://www.symauth.com/rpa00	Quotation.exe, 00000000.00000003.252069193.00000000027A3000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://https://mozilla.org0	Quotation.exe, 00000000.00000003.253899222.00000000027A4000.00000004.00000020.00020000.00000000.sdmp, maintenanceservice2.exe.0.dr	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.thawte.com0	Quotation.exe, 00000000.00000003.252069193.000000000027A3000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://www.nero.com	Quotation.exe, 00000000.00000003.252069193.000000000027A3000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://https://github.com/dotnet/runtime	Quotation.exe, 00000000.00000003.253157391.000000000027A3000.00000004.00000020.00020000.00000000.sdmp, Quotation.exe, 00000000.00000003.252894237.000000000027AA000.00000004.00000020.00020000.00000000.sdmp, System.Security.Cryptography.X509Certificates.dll.0.dr, System.dll.0.dr	false		high

World Map of Contacted IPs

 No contacted IP infos

General Information	
Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830618
Start date and time:	2023-03-20 14:46:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	13
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
Sample file name:	Quotation.exe
Detection:	MAL
Classification:	mal68.troj.evad.winEXE@1/10@0/0
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 63.5% (good quality ratio 62.2%) - Quality average: 89% - Quality standard deviation: 21.4%
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Found application associated with file extension: .exe - Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs		
Time	Type	Description
14:47:24	API Interceptor	1x Sleep call for process: Quotation.exe modified

Time	Type	Description
14:47:24	API Interceptor	1x Sleep call for process: Quotation.exe modified

Joe Sandbox View / Context

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Blegnbetheden\Telegrammers.Non

[illegible]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Cohesion\Quakily\Privileger.Fla

Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	ASCII text, with very long lines (55032), with no line terminators
Category:	dropped

File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	49768
Entropy (8bit):	5.650496280667822
Encrypted:	false
SSDEEP:	768:4vuoy1c6A2ZX8TRNH5JVbOd502zq1TntV5fjM:4vuoO3ZX8Q5jzC35NjM
MD5:	BCC32F5B608C99F89508921B6333B329
SHA1:	5F70BB4A3A812C399D8D2A2954C9A715574CFF61
SHA-256:	5D4FF9A8E3B3CA26F53CD2CC4C557C5F2074A431B9CD029AE7F7A7B8902FA3C1
SHA-512:	99C7623BCA873C75A3B804C815DF178ACC88E043A36473C785216CD26DC73F0525FE336F17F0F2C8CA6473FBD407A953D4650D093C52440D93ECF07C1440FAE
Malicious:	true
Yara Hits:	Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\System.dll, Author: Joe Security
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....PE..L....." ..0..... ..`.....O.....h\$.....T.....H.....text.....`..rsrc.....@ ..@.reloc.....@..B.....H.....P.....BSJB.....v4.0.30319.....l..\$;..#~...R.#Strings...4.....#US.8.....#GUID...H..... #Blob.....T.....3...../.....=.....J=...=.....V...}.....h.....J.....1.. .j.. , AF..a.AF....R..e..=.....;.....;.....;.....1..;9..; ..A...l...Q...Y...a...l...q...y...;.....;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\libdatrie-1.dll 	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	36029
Entropy (8bit):	5.699900454607003
Encrypted:	false
SSDEEP:	768:Hm5z53y6m/LHIM6GnPGUvMrsztd/sLLhF3VI:a53y6Gy6GuU5d/OhF3G
MD5:	8A54723090530190EB11AFCD5B702B1B
SHA1:	DFA923EC796A754BD21C4F9E504305848A4CB1B2
SHA-256:	738F67F45FAA07CC387BAF390604EE4CE709CBE7C223D9A043EE06F7CB360D5B
SHA-512:	E0D310458C8259112E07B153EDC86FDF729E1B09648FED8D163D44DEB3BEE1545E7AD37BB00E9255DF6514844B21A829750848DA42F85FA77BEF376CE09750CF
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....PE..d.....&"R.....0.....h.....^.. ..`.....X.....0.....X.....@.....(.....P.....text...HP.....R.....P`.data.....p.....V.....@.. P..rdata.....X.....@.. @.pdata.....b.....@.0@.xdata.....j.....@.0@.bss.....`..edata.....r.....@.0@.idata..... ..v.....@.0..CRT...X.....~.....@..@..tls.....@..@..reloc..`.....@.0B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\libpkcs11-helper-1.dll 	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	130344
Entropy (8bit):	6.2622011397185
Encrypted:	false
SSDEEP:	3072:tKInqVjbm+1Vi5R6QUU7k1TAH1OobTrWHEE-hjFpCOx:tVzjvi5R6QUU7k1TAH1OobTrWHExFpdx
MD5:	2455841538BA8A502398C18781CC3CEB
SHA1:	86CFD513FEE46EBC2C35225B27372679BE6ADA91
SHA-256:	F37BE7BD8C46D58CA931810536C8A2BEC36D06FF3281740FE0AD177F022AC781
SHA-512:	BC1DCDDE074150616DED7EAACC3FC44BDD2487EB5E550172F5EA46432AA76F19443A9FD6CEf61577B7803C1B083FFCBCEAF9ADC3114A97B547A78C2654F757E3
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....PE..d.....&"`d.....P.....z.. ..`.....X.....0.....X.....@.....(.....P.....text...8!....."P`.data.....@.....&..... .....@..`rdata...^P...`.....@.. @.pdata.....@.0@.xdata.....@.0@.bss.....`..edata.....@.0@.idata.. X.....@.0..CRT...X.....@..@..tls...h.....@..`rsrc.....0.....@.0..reloc.....@.....@.0B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\maintenanceservice2.exe 	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	227256
Entropy (8bit):	6.388677533277947
Encrypted:	false
SSDEEP:	6144:ue/rKQgYva3o4vj272BNvJJuQlf2qIHL2:uYrK4a3PvKw7ufg2
MD5:	49A2E97304EF8E044EEBD7ACCAD37E11
SHA1:	7D0F26591C8BD4CAB1718E323B65706CBEA5DE7A
SHA-256:	83EAFBF165642C563CD468D12BC85E3A9BAEDE084E5B18F99466E071149FD15F
SHA-512:	AC206C5EF6F373A0005902D09110A95A7F5FB4F524653D30C3A65182717272FE244694A6698D40884BEA243B2CA00D7741CED796DF7AE8C633F513B8C6FCD6C
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L!This program cannot be run in DOS mode.\$..PE..d...J..b....."......@.....Y.....`..... .....h..X.....(....P.....(..h.....text...9.....`..rdata.....P.....>..... @...@.data...l...0.....@...pdata..h...`.....*.....@...@.00cfg.....D.....@...@.tls.....F.....@...rsrc.....H.....@...@.reloc..... ...P.....@...B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Foreureningsforebygget\Pegboard\percentile.dll 	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	102577
Entropy (8bit):	5.075179901575448
Encrypted:	false
SSDEEP:	768:t9H5uXFjJeEoPsznZgkZNFdS2E0fVnSdNPfZ5+uKlu7aQzTgp37CtHRMX6NX0:tJ5wJeEoU9g0Nhav09nahfYxDRx0
MD5:	3144DFDEC817D0AC6FE3F4642B70328B
SHA1:	756C3513DC10CF00B517C72B2D3AB3E20895A46C
SHA-256:	BF17F5B38DCF35B55B1E0FAD462D4095ABAAA4CD8F1EDBDC8657C0249EF5D4D3
SHA-512:	012D9A3B88BA5D5090E8B47B49FE50E518489AB05FAAC6A1A0743F29A369B7D67F39B8E113B34740607137F2D67D75116DBE2A76E8E1DBE699BA4973F8037684
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..d...rL`<.....&...\$.....6.....P.....U.. .....Y.....P.....A.....(.....text.....`..P..data...p...0.....@.. P..rdata..p...@....."......@...@.pdata..P.....*.....@...@.xdata..l...`.....@...@.bss.....p.....`..edata..Y.....0.....@...@.idata..2.....@...@.CRT...X.....6.....@...@.tls.....8.....@...@.reloc..`.....@...@.B/4.....<.....@.PB/19...C.....@..... .....@...B/31.....`.....@...B/45.....@...B/57.....

C:\Users\user\AppData\Local\Temp\nst891E.tmp\System.dll 	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.854901984552606
Encrypted:	false
SSDEEP:	192:qPtKiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4U:F7VpNo8gmOyRsVc4
MD5:	0063D48AFE5A0CDC02833145667B6641
SHA1:	E7EB614805D183ECB1127C62DECB1A6BE1B4F7A8
SHA-256:	AC9DFE3B35EA4B8932536ED7406C29A432976B685CC5322F94EF93DF920FEDE7
SHA-512:	71CBBCAEB345E09306E368717EA0503FE8DF485BE2E95200FEB61BCD8BA74FB4211CD263C232F148C0123F6C6F2E3FD4EA20BDECC4070F5208C35C6920240F0
Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....ir*..-D..-D...J*.D..-E..>D.....*.D.y0t.).D.N1n.,D..3@.,.D.Rich-.D..PE..L.....].....!.....0.....@.....2.....0..P.....P.....0.X.....text.....`..rdata..c...0.....\$.....@...@.data..h....@.....(.....@...reloc.. ...P.....*.....@...B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.974128626441633
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:	Quotation.exe
File size:	693360
MD5:	8a81948116d2ea79bee1d261733dba89
SHA1:	5cf4113debe6d37bd770d8d3870647b8bac082a3
SHA256:	5a64a3fd65f7176b7ad623893e3cb573af13eb51850f8243a1951884eee757a9
SHA512:	bc5707d66c79d3f01e29227514bc1fa938e0165b000b94efefdb3c8d2849e2ede859c037b103b9f85365cd178c179171e8e7dec071c71ba61b6e919d1eba8841
SSDEEP:	12288:QV5CSEuHKGQYpovMKcZnY4UKwp7hVOZCbgjvwf:QV51qFMccUNEZCbgjY
TLSH:	7BE42317B19382C3D5E749F53E698B3683B33F570D22878FF2AA37B19974914812A427
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$..... (...F...F...F.*.....F...G.w.F.*.....F...v...F...@...F.Rich..F.....PE..L.....].....52.....p....@

File Icon



Icon Hash:	84c8c888cac88800
------------	------------------

Static PE Info

General

Entrypoint:	0x403235
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:	0x5DF6D4E3 [Mon Dec 16 00:50:43 2019 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:	e9c0657252137ac61c1eeeba4c021000

Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Hjertecenteret@Brahminee.Sta, OU="Slewingselews Styrborde Nadines ", O=Demystify, L=Parlier, S=California, 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	8/14/2022 6:11:02 PM 8/13/2025 6:11:02 PM
Subject Chain	E=Hjertecenteret@Brahminee.Sta, OU="Slewingselews Styrborde Nadines ", O=Demystify, L=Parlier, S=California, C=US
Version:	3
Thumbprint MD5:	62DE8C7E9FEEF9C1BE32A539EE8C3042
Thumbprint SHA-1:	3D54D8A3F7094698631D99D96688154B999E2C8B
Thumbprint SHA-256:	A645406AC892515D81FC329AB84ADDF8C558F2770665B05F23CFC9F4C322D1DC
Serial:	3F5567173D0043C048AB0658FB8124DCFF6DDE12

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], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A0h]
call dword ptr [0040709Ch]
and eax, BFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042370Ch], eax
je 00007FD5E8C59E63h
push ebx
call 00007FD5E8C5CF4Bh
cmp eax, ebx
je 00007FD5E8C59E59h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007FD5E8C5CEC7h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FD5E8C59E3Dh
push 0000000Ah
call 00007FD5E8C5CF1Fh
push 00000008h
call 00007FD5E8C5CF18h
push 00000006h
mov dword ptr [00423704h], eax
call 00007FD5E8C5CF0Ch
cmp eax, ebx
je 00007FD5E8C59E61h
push 0000001Eh
call eax
test eax, eax
je 00007FD5E8C59E59h
or byte ptr [0042370Fh], 00000040h
push ebp
call dword ptr [00407040h]
push ebx
call dword ptr [00407284h]
mov dword ptr [004237D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407178h]
push 00409188h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7430	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0x4568	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa7228	0x2248	
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	0x7000	0x294	.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	0x5f7d	0x6000	False	0.6680094401041666	data	6.466064816043304	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x123e	0x1400	False	0.4275390625	data	4.989734782278587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a818	0x400	False	0.638671875	data	5.130817636118804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x12000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x36000	0x4568	0x4600	False	0.42265625	data	5.512282206254712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x36268	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x38810	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x398b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x39d20	0x100	data	English	United States
RT_DIALOG	0x39e20	0x11c	data	English	United States
RT_DIALOG	0x39f40	0xc4	data	English	United States
RT_DIALOG	0x3a008	0x60	data	English	United States
RT_GROUP_ICON	0x3a068	0x30	data	English	United States
RT_VERSION	0x3a098	0x190	data	English	United States
RT_MANIFEST	0x3a228	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
-----	--------

DLL	Import
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, IsStrlenA, GetVersion, SetErrorMode, IstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetFileAttributesA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, IstrcpyA, MoveFileExA, IstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileTime, GetFileAttributesA, SetCurrentDirectoryA, MoveFileA, GetFullPathNameA, GetShortPathNameA, SearchPathA, CloseHandle, IstrcmpiA, CreateThread, GlobalLock, IstrcmpA, DeleteFileA, FindFirstFileA, FindNextFileA, FindClose, SetFilePointer, GetPrivateProfileStringA, WritePrivateProfileStringA, MulDiv, MultiByteToWideChar, FreeLibrary, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	GetSystemMenu, SetClassLongA, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, LoadImageA, CreateDialogParamA, SetTimer, SetWindowTextA, SetForegroundWindow, ShowWindow, SetWindowLongA, SendMessageTimeoutA, FindWindowExA, IsWindow, AppendMenuA, TrackPopupMenu, CreatePopupMenu, DrawTextA, EndPaint, DestroyWindow, wsprintfA, PostQuitMessage
GDI32.dll	SelectObject, SetTextColor, SetBkMode, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, GetDeviceCaps, 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

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

 No statistics

System Behavior

Analysis Process: Quotation.exe PID: 2684, Parent PID: 3452

General	
Target ID:	0
Start time:	14:47:23
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation.exe
Imagebase:	0x400000
File size:	693360 bytes

MD5 hash:	8A81948116D2EA79BEE1D261733DBA89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.773629937.0000000005789000.00000040.00001000.00020000.00000000.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	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\Temp\nsr50D7.tmp	read attributes generic read	device	synchronous io non alert non directory file	success or wait	1	405BD6	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	5	405650	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	5	405650	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	405650	CreateDirectoryA	
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	5	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\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	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\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	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	5	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	4	405650	CreateDirectoryA	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Blegnbetheden	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Blegnbetheden\Telegrammers.Non	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\SolutionExplorerCLI.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\Privileger.Fla	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\System.Security.Cryptography.X509Certificates.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget\Melotragedy	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget\Melotragedy\Lindhardt	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\System.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Delforliget\Melotragedy\Lindhardt\libdatrie-1.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Foreureningsforebygget	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Foreureningsforebygget\Pegboard	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Foreureningsforebygget\Pegboard\libpkcs11-helper-1.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Foreureningsforebygget\Pegboard\maintenanceservice2.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Foreureningsforebygget\Pegboard\percentile.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Temp\nst891E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	405BD6	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405650	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	405650	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	405650	CreateDirectoryA
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	405650	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	405650	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nst891E.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	405610	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nst891E.tmp\System.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405B9F	CreateFileA
C:\Users\user\AppData\Local\Temp\nst891E.tmp\System.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	object name collision	4	405B9F	CreateFileA

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr50D7.tmp	success or wait	1	4034AC	DeleteFileA
C:\Users\user\AppData\Local\Temp\nst891E.tmp	success or wait	1	4057D1	DeleteFileA

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\Privileger.Fla	0	32768	30 30 30 30 30 30 30 30 30 30 30 30 30 30 42 39 30 30 44 32 30 30 35 38 35 38 30 30 30 30 43 42 30 30 32 42 30 30 30 30 42 43 30 30 30 30 30 38 30 38 30 30 35 41 30 37 31 30 30 30 30 35 37 30 30 30 30 30 30 30 30 30 35 30 30 42 43 42 43 42 43 30 30 30 30 30 30 30 30 30 30 30 30 31 32 30 30 30 33 30 30 43 30 43 30 30 30 30 30 30 30 42 31 30 30 30 30 30 30 41 33 41 33 41 33 30 30 44 42 44 42 30 30 30 30 30 30 30 30 30 36 30 30 34 34 30 30 30 30 30 30 30 30 30 30 33 31 30 30 30 30 46 46 46 46 30 30 31 35 30 30 45 42 30 30 30 30 30 30 30 30 37 31 30 30 30 30 45 42 45 42 30 30 30 30 44 34 30 30 30 30 30 30 39 37 39 37 30 30 30 30 30 30 30 30 45 33 30 30 30 30 30 30 30 30 30 30 30 30 30 30 45 38 30 30 30	00000000000000B900D2 0058580000 CB002B0000BC0000080 8005A000000 00000000000007100005 700000000 0500BCBCBC000000000 00012000300 C0C0000000B1000000A3 A3A300DBDB 000000000600440000000 000310000 FFFF001500EB00000000 710000EBEB 0000D400000097970000 0000E30000 0000000000E8000	success or wait	2	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\System.Security.Cryptography.X509Certificates.dll	0	24802	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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 03 00 fd 66 57 fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 fd 06 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 07 00 00 02 00 00 fd 04 08 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.\$PEdW" ``@@	success or wait	20	405C34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Gheto\Delforliget\Melotragedy\Linhardt\System.dll	0	32768	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 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 4c 01 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 00 00 00 08 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 02 00 00 fd fd 00 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEL" 0 `	success or wait	2	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Gheto\Delforliget\Melotragedy\Linhardt\libdatrie-1.dll	0	32768	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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 fd 00 00 3c 00 00 00 fd 00 26 22 0b 02 02 1f 00 52 00 00 00 fd 00 00 00 0a 00 00 30 13 00 00 00 10 00 00 00 00 fd 68 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 10 01 00 00 04 00 00 fd 5e 01 00 03 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEd<&"R0h^	success or wait	2	405C34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Gheto\Forureningsforebygget\Pegboard\libpkcs11-helper-1.dll	0	32768	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 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 0c 00 00 00 00 00 00 fd 01 00 fd 00 00 00 fd 00 26 22 0b 02 02 1e 00 22 01 00 00 fd 01 00 00 0c 00 00 fd 13 00 00 00 10 00 00 00 00 5c 64 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 50 02 00 00 04 00 00 7a fd 02 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEd&""dPz`	success or wait	6	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Gheto\Forureningsforebygget\Pegboard\maintenanceservice2.exe	0	32768	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 78 00 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 24 00 00 50 45 00 00 64 fd 08 00 4a 0e 2e 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 3a 02 00 00 1a 01 00 00 00 00 00 fd fd 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 03 00 00 04 00 00 59 fd 03 00 02 00 60 fd 00 00 fd 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.\$PEdJ.b":@Y`	success or wait	11	405C34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Forureningsforebygget\Pegboard\percentile.dll	0	32768	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 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 13 00 72 4c fd 60 00 3c 01 00 fd 03 00 00 fd 00 26 20 0b 02 02 24 00 1a 00 00 00 36 00 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 fd 05 03 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 00 02 00 00 06 00 00 fd 55 02 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEdrL`-& \$6PU`	success or wait	4	405C34	WriteFile
C:\Users\user\AppData\Local\Temp\nst891E.tmp\System.dll	0	11776	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 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 69 72 2a fd 2d 13 44 fd 2d 13 44 fd 2d 13 44 fd fd 0f 4a fd 2a 13 44 fd 2d 13 45 fd 3e 13 44 fd fd 1c 19 fd 2a 13 44 fd 79 30 74 fd 29 13 44 fd 4e 31 6e fd 2c 13 44 fd fd 33 40 fd 2c 13 44 fd 52 69 63 68 2d 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 5d 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.\$ir*-D-D-DJ*D-E >D*Dy0t)DN1n,D3@,DRi ch-DPEL].! !)	success or wait	1	405C34	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\Desktop\Quotation.exe	unknown	512	success or wait	119	405C05	ReadFile	
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	2	405C05	ReadFile	
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	50	405C05	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Cohesion\Quakily\Privileger.Fla	unknown	1	success or wait	1023	405C05	ReadFile	
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	5050	405C05	ReadFile	
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	2	405C05	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Ghetto\Blegnbbetheden\Telegrammers.Non	unknown	26271744	success or wait	1	6D012AF9	ReadFile	

Registry Activities
Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\anarkisterne	success or wait	1	405EBD	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\anarkisterne\Thanages	success or wait	1	405EBD	RegCreateKeyExA

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\anarkisterne\Thanages	Festival	binary	2A 58 C6	success or wait	1	4024CB	RegSetValueExA

Disassembly

 No disassembly