ID: 830630
Sample Name:
QUOTATION.exe
Cookbook: default.jbs
Time: 14:56:35
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

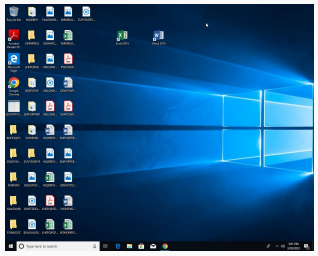
Windows Analysis Report

QUOTATION.exe

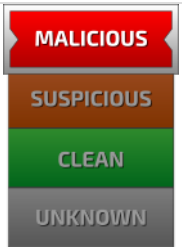
Overview

General Information

Sample Name:	QUOTATION.exe
Analysis ID:	830630
MD5:	9f23ccacd9553..
SHA1:	d7c9c869add7…
SHA256:	7b8d50ac67b2…
Tags:	exe guloader
Infos:	



Detection



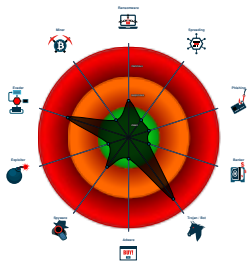
GuLoader

Score:	76
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: 1668 cmdline: C:\Users\user\Desktop\QUOTATION.exe MD5: 9F23CCACD955392C62B1B5D4BE4ED690)
- **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-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-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\INetCache\Ghetto\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\System.dll	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.257915542.0000000002888000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000000.00000002.779007942.00000000052F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000000.00000002.779007942.00000000053F7000.00000040.00001000.00020000.00000000.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

Networking

Yara detected Generic Downloader

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

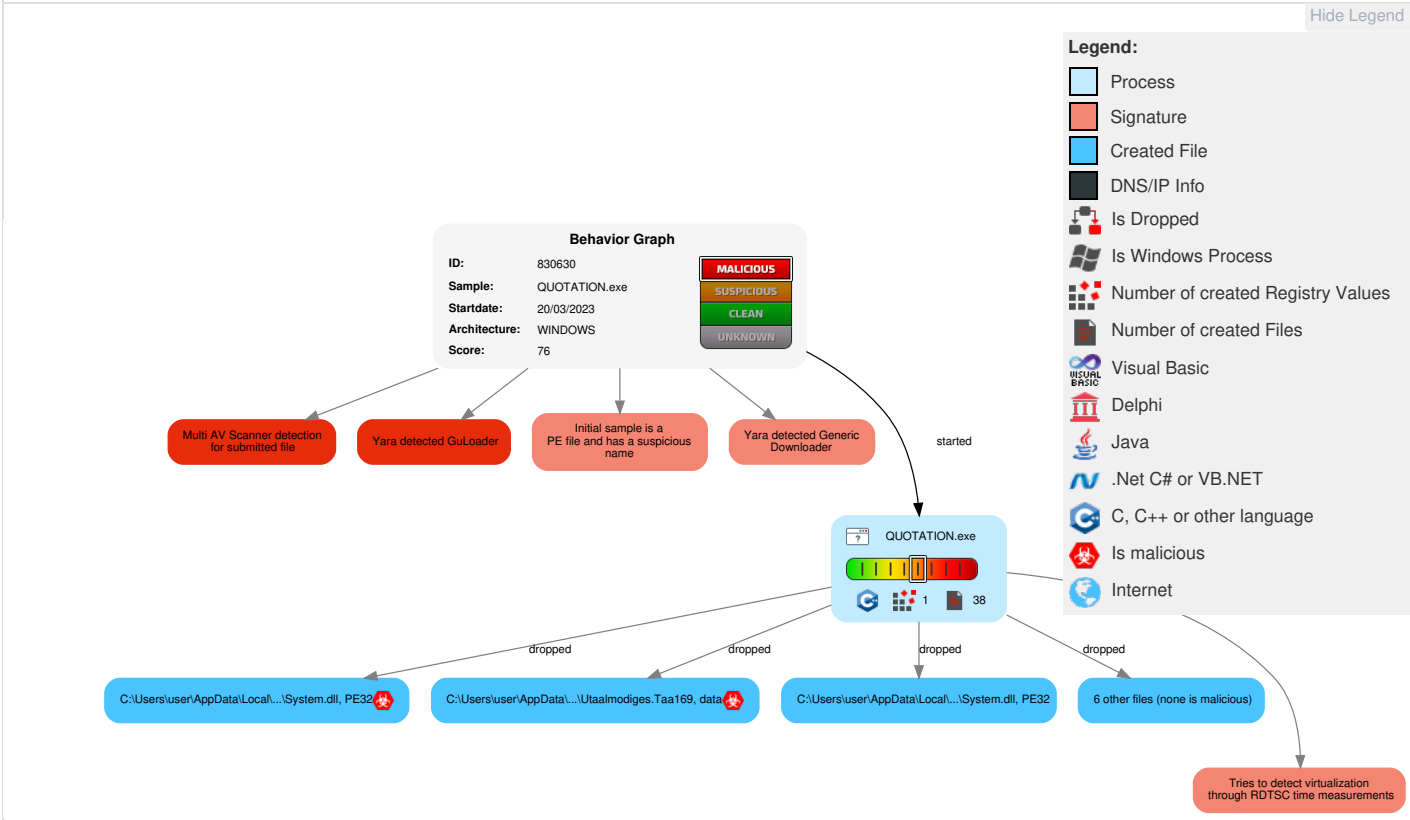
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 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	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Access Token Manipulation	LSASS Memory	3 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)	Logon Script (Windows)	1 Timestomp	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

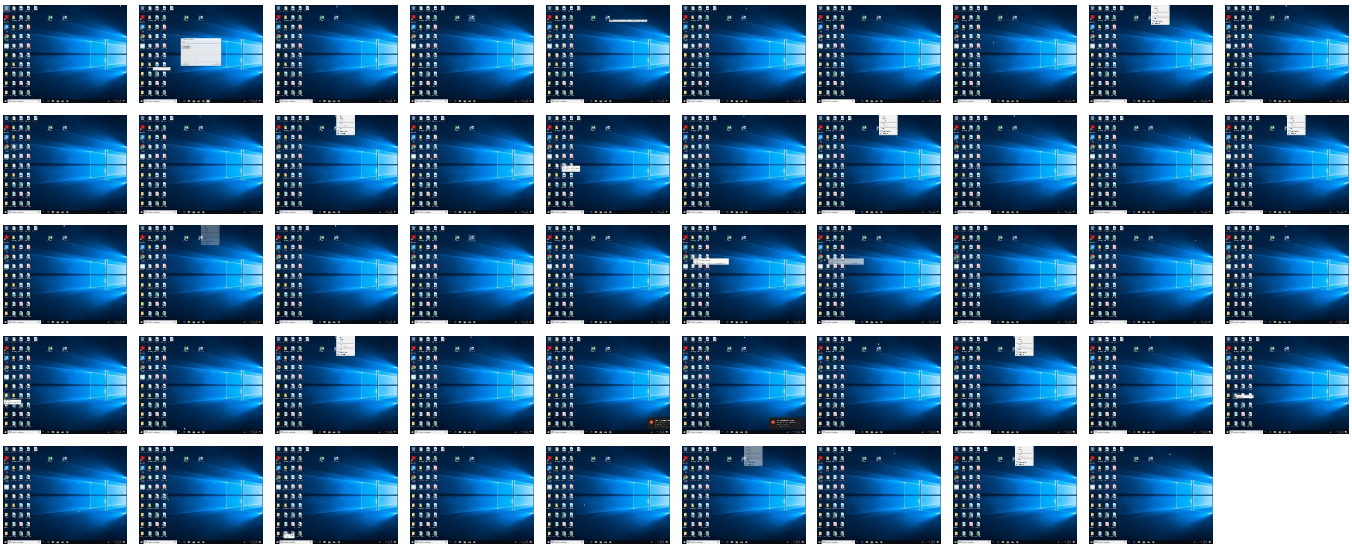
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QUOTATION.exe	33%	ReversingLabs	Win32.Trojan.Leoncem	
QUOTATION.exe	13%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87\SolutionExplorerCLI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87\SolutionExplorerCLI.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\libpkcs11-helper-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\libpkcs11-helper-1.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\maintenanceservice2.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\maintenanceservice2.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\percentile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\percentile.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\System.Security.Cryptography.X509Certificates.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\libdatrie-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsc344B.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	

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, 00000000.00000003.258854903.000000000288A000.00000004.00000020.00020000.00000000.sdmp, System.Security.Cryptography.X509Certificates.dll.0.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	QUOTATION.exe, 00000000.00000003.258243906.0000000002885000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://www.symauth.com/cps0(	QUOTATION.exe, 00000000.00000003.258243906.0000000002885000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.symauth.com/rpa00	QUOTATION.exe, 00000000.00000003.258243906.0000000002885000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://https://mozilla.org0	QUOTATION.exe, 00000000.00000003.262585876.0000000004AEF000.00000004.00000020.00020000.00000000.sdmp, maintenanceservice2.exe.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	QUOTATION.exe, 00000000.00000003.258243906.0000000002885000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.nero.com	QUOTATION.exe, 00000000.00000003.258243906.0000000002885000.00000004.00000020.00020000.00000000.sdmp, SolutionExplorerCLI.dll.0.dr	false		high
http://https://github.com/dotnet/runtime	QUOTATION.exe, 00000000.00000003.259097589.0000000002881000.00000004.00000020.00020000.00000000.sdmp, QUOTATION.exe, 00000000.00000003.258854903.000000000288A000.00000004.00000020.00020000.00000000.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:	830630
Start date and time:	2023-03-20 14:56:35 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
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:	22
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:	mal76.troj.evad.winEXE@1/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.3% (good quality ratio 62%) • Quality average: 89.3% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, ar c.msn.com

- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
14:57:34	API Interceptor	1x Sleep call for process: QUOTATION.exe modified

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\Microsoft\Windows\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87\SolutionExplorerCLI.dll

Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	75248
Entropy (8bit):	6.149004775364808
Encrypted:	false
SSDEEP:	1536:GmY7dQU8l75gS4SqQR27YZW1cwvbTxUd6Rw:GmacliS49QR27YZW1vn2dWw
MD5:	3A03B61FA01DCDFF3E595D279F159D6E
SHA1:	94900C28C23AD01D311C389A0813277CFB30345C
SHA-256:	4F4D6511BEC955B4E8A30371ED743EA5EBC87CEB0BF93FE21F0A378AA2C05A01
SHA-512:	0D04D3486911DFE0439449554E90FB68B4D85EEE025A9B89910C306DE33CBFDBBEF1ABCAC5D4CD3B3CC1B1F445B7C67DC341C9363C9B127810ABD0498EC94AC4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T..:.:.:....:....:.:.:.]..:..]...:..]..:..]...:..u...:..u..:....:..u...:.Rich.:..... ....PE..L...w..U.....!.....:.....dG.....P.....@.....p...@.....<...P.... .....0.....P..8.....R..@.....P.....(Q.. H.....text...!8.....:..... ..`.rdata.....P.....>.....@..@.data.....@....rsrc..... .....@..@.reloc.. ....0.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169

Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	data
Category:	dropped
Size (bytes):	254328
Entropy (8bit):	7.284609523209945
Encrypted:	false
SSDEEP:	3072:PRs7IL/hhpwtoHPCrwXE/Y5aBMCYDjTQXB3EZ+FhS2LYga8KB9JIopauAxqOp2xP:eh4tsCrJxMvDj8X8+FYxP3pnUqLdN
MD5:	F4CC23ED0D3896E2B178E6A55C40AA4E
SHA1:	370ACD45CAAE23C832BD48E3CC3D56C1107E3A51
SHA-256:	F70AA179CC5D44B7605AC33C35BA47DC32A5DA0EFE494AB7C5CF132AEF6ACA0C
SHA-512:	F920BB342EF61E0EC18B4C9A698821606E41B8D31A423A3B196C7ED5E804BCAE4825C0E142DB6AF1611D01C75F8B7D0D780C7A2FAC4FB4533C70FD9395E1B810
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169, Author: Joe Security
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\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:tKInqqVjbm+1Vi5R6QQU7k1TAH1OobTrWHEE+jFpCOx:tVzjvi5R6QQU7k1TAH1OobTrWHExFpdx
MD5:	2455841538BA8A502398C18781CC3CEB
SHA1:	86CFD513FEE46EBC2C35225B27372679BE6ADA91
SHA-256:	F37BE7BD8C46D58CA931810536C8A2BEC36D06FF3281740FE0AD177F022AC781
SHA-512:	BC1DCDDE074150616DED7EAACC3FC44BDD2487EB5E550172F5EA46432AA76F19443A9FD6CEF61577B7803C1B083FFCBCEAF9ADC3114A97B547A78C2654F757E3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
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\Wept\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/rKQgYva3o4vj272BNvlJuQlf2qIHL2:uYrK4a3PvKw7ufg2
MD5:	49A2E97304EF8E044EEBD7ACCAD37E11
SHA1:	7D0F26591C8BD4CAB1718E323B65706CBEA5DE7A
SHA-256:	83EAFBF165642C563CD468D12BC85E3A9BAEDE084E5B18F99466E071149FD15F
SHA-512:	AC206C5EF6F373A0005902D09110A95A7F5FB4F524653D30C3A65182717272FE244694A6698D40884BEA243B2CA00D7741CED796DF7AE8C633F513B8C6FCD6C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file

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....!...0.....@....pdata..h....`.....*.....@..@.00cfg.....D.....@..@.tls.....F.....@....rsrc.....H.....@..@.reloc..... .....P.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\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:t9H5uXFjJeEoPsznZgkZNhFdS2E0fVnSdNPfZ5+uKIu7aQzTgp37CtHRMX6NX0:tJ5wJeEoU9g0Nhav09nahfYxDRx0
MD5:	3144FDFEC817D0AC6FE3F4642B70328B
SHA1:	756C3513DC10CF00B517C72B2D3AB3E20895A46C
SHA-256:	BF17F5B38DCF35B55B1E0FAD462D4095ABAAA4CD8F1EDBDC8657C0249EF5D4D3
SHA-512:	012D9A3B88BA5D5090E8B47B49FE50E518489AB05FAAC6A1A0743F29A369B7D67F39B8E113B34740607137F2D67D75116DBE2A76E8E1DBE699BA4973F8037684
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
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.....*.....@.0@.xdata..l...`.....@.0@.bss.....p.....`..edata..Y.....0.....@.0@.idata.. .....2.....@.0..CRT....X.....6.....@.@..tls.....8.....@.@..reloc..`.....:.....@.0B/4.....<.....@.PB/19.....C.....@..... .....@..B/31.....`.....@..B/45..... .....@..B/57.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\Dampning.Dub

Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	74176
Entropy (8bit):	2.6722266832319854
Encrypted:	false
SSDEEP:	1536:NKBIx/TbxyxbZ3K4FBS/PqiqRqxmyFJcEXxedrfEf6v3Zm2:YrEXgd6u
MD5:	992929F1D7A90F5CE4FCCD117E1A7DBE
SHA1:	44CCBD5EBFE22ACECEFBF0CF381F99CD6015943B
SHA-256:	BBA853900D50A7D6952063FAD68F534B5CB97B336B1B129F2F0717669BCF309A
SHA-512:	15062430326D4964BFD07129146BADC839D253D20401F7D872BFB39A5D903C31BCF0ACEFCF3F960ADF228084CB3EC8415D5375FC8CF8B7DEB0678FCF9E44A9 C
Malicious:	false
Preview:	0000EFEF002E00000000C5C500D0D0005300A50063005F5F5F5F5F0000A800B2B200F4F400002A2A2A2A2A00282828000000A2A2009B00005B5B5B5B 5B007E0002000029000060606000000004C002E2E00BDBDBDBD0000A500D8000000D400009797008C8C8C8C8C0000BBBBBB00505000000000000006E 0043000000DFDF0000000000004C00740000B1005656565656560000600AAAA002E2E0000E5E50000005700000000D80000000007070000F00000000000D800EE 00000000000000029290000000008E8E0000BDBD00BEBEBE003400008B00000000001F000000000000003535002828007D7D7D7D009A9A9A9A9A000000 DD000000CE0000F3F30043009D9D9D9D00AF0000001E001A000000000000008A8A00D6000000001600D700DB000000000007979790073737373000D80000F200 6C007373000006B6B6B6B00FC003B0000D2D2000015001818001C1C1C0000000000002000D4D400004200002B2B2B000000000000FDFDFDFDFDFD0071 000000E000006969000000C3C3008E000000C400292929000000A000F3F3000008080000000900E1E1E1008C8C009494940000000000000000005E000037370000 1414140000000000000000000DB00A200A5A50000FC000091000000636363630000C8C8000000F9F900323200006900 5F00F0F00000A50039390066660000000

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\System.Security.Cryptography.X509Certificates.dll

Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	485488
Entropy (8bit):	6.710350474742332
Encrypted:	false
SSDEEP:	6144:1E5AW+0VyAaOKxFf8r6S2rGjF0KAmdHCKsCZcufvh7OzxQxQ5JVIRVrk:KGWlaOKC2a0tmFChCOFeqLIRpk
MD5:	84D7B1FB924AEEFCF4A2C7A687FE2EF1
SHA1:	A2C2C7DE9096328A3FEF0C7FCEA262A294C0807B
SHA-256:	32A54C24B18B3C087E06F4F19885FB410304AB4AF2263154020D3F5CDCE36D99
SHA-512:	E75F91DA415B15CA0B19519179021FD88C0FC68FE4EF2A68B899B121BD511C04AECCB58101318C86CB0458D7310208C358DBB9155A02D62DE73C04128ECC593
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....fW....." .....` ..`...@.....@..... .....1...D..p$...P.....0..T.....H.....text..... ..`.data...wy.....z..... .....@....reloc.....P.....:.....@..B.....0.....T.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i .l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....d...C.o.m.m.e.n.t.s...I.n.t.e.r.n.a.l. .i.m.p.l.e.m.e.n.t.a.t.i.o.n. .p.a.c.k.a.g.e. .n.o.t. .m .e.a.n.t. .f.o.r. .d.i.r.e.c.t. .c.o.n.s.u.m.p.t.i.o.n... .P.l.e.a.s.e. .d.o. .n.o.t. .r.e.f.e.r.e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\System.dll

Process:	C:\Users\user\Desktop\QUOTATION.exe
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:	768:4vuoy1c6A2ZX8TRNH5JVbOd502zq1TntV5fljM: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\hamotzi\System.dll, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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..;..I..;..Q..;..Y..;..a..;..i..;..q..;..y..;....; ...;....;..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\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/LHlM6GnPGUvMrsztd/sLLhF3VI:a53y6Gy6GuU5d/OhF3G
MD5:	8A54723090530190EB11AFCD5B702B1B
SHA1:	DFA923EC796A754BD21C4F9E504305848A4CB1B2
SHA-256:	738F67F45FAA07CC387BAF390604EE4CE709CBE7C223D9A043EE06F7CB360D5B
SHA-512:	E0D310458C8259112E07B153EDC86FDFF29E1B09648FED8D163D44DEB3BEE1545E7AD37BB00E9255DF6514844B21A829750848DA42F85FA77BEF376CE09750CF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....<.....&".....R.....0.....h.....^.. ....`.....(.....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\Temp\nsc344B.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:	71CBBCAEB345E09306E368717EA0503FE8DF485BE2E95200FEBC61BCD8BA74FB4211CD263C232F148C0123F6C6F2E3FD4EA20BDECC4070F5208C35C6920240F0
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....]..... .....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.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):	7.973819019229736
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:	690832
MD5:	9f23ccacd955392c62b1b5d4be4ed690
SHA1:	d7c9c869add707b5b41a1f11f5c82bba94eabbd7
SHA256:	7b8d50ac67b2f0de5e35909025cc1a8d15f5edd18675878c7aaa31e3fe83a9fd
SHA512:	6ece2c0aa30e9967a673ccd1b0aa248f0fce1bb5745458e641107962552dffeb8ea0c87d89d6e5487559db76e1c76b8f98718125afd5f7a70fa91af8c3b59c1c
SSDEEP:	12288:2V5hWKql4jLy5cdg3ExKcZnY4UKwp7hVOZCbgjvwP:2V5hC4icdg1cUNEZCbgj8
TLSH:	A1E42317758392D6F67B45FB5E6EA72603B32F670862828FB3E937B18874910446630F
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=Radiov@Charley.Po, OU="Polyparasitic semisagittate ", O=Syndoc, L=Fervaches, S=Normandie, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 4/21/2022 5:46:17 PM 4/20/2025 5:46:17 PM

Subject Chain	• E=Radiov@Charley.Po, OU="Polyparasitic semisagittate ", O=Syndoc, L=Fervaches, S=Normandie, C=FR
Version:	3
Thumbprint MD5:	F54BEA37D1ADC4BAD2F60927632A2EC9
Thumbprint SHA-1:	BF5EB77E7A91F7976F23F102B3C078DB9DAAF954
Thumbprint SHA-256:	A4139CD92C018C5E22E64C59A153598DB90CDE89114105F7C95C552D2C985DB3
Serial:	122A79BA407440E874A3850AF2969681469C2B80

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, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042370Ch], eax
je 00007F06486A4313h
push ebx
call 00007F06486A73FBh
cmp eax, ebx
je 00007F06486A4309h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007F06486A7377h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F06486A42EDh
push 0000000Ah
call 00007F06486A73CFh
push 00000008h
call 00007F06486A73C8h
push 00000006h
mov dword ptr [00423704h], eax
call 00007F06486A73BCh
cmp eax, ebx
je 00007F06486A4311h
push 0000001Eh
call eax
test eax, eax
je 00007F06486A4309h
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]

Instruction
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407178h]
push 00409188h

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	0x7430	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0x4568	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa68a8	0x21e8	
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

Name	RVA	Size	Type	Language	Country
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
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetFileAttributesA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileTime, GetFileAttributesA, SetCurrentDirectoryA, MoveFileA, GetFullPathNameA, GetShortPathNameA, SearchPathA, CloseHandle, lstrcmpiA, CreateThread, GlobalLock, lstrcmpA, 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: 1668, Parent PID: 3452

General

Target ID:	0
Start time:	14:57:32
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:	690832 bytes
MD5 hash:	9F23CCACD955392C62B1B5D4BE4ED690
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000003.257915542.0000000002888000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000002.779007942.00000000052F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.779007942.00000000053F7000.00000040.00001000.00020000.00000000.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\nssF5CA.tmp	read attributes | synchronize | 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\INetCache	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\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\INetCache\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
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Industrialization	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\INetCache\Ghetto\Industrialization\Snoldets	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\INetCache\Ghetto\Industrialization\Snoldets\Embrocates	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\INetCache\Ghetto\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169	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\INetCache\Ghetto\Alswith	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\INetCache\Ghetto\Alswith\Peroxidisement	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\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87	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\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87\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\INetCache\Ghetto\hamotzi	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\INetCache\Ghetto\hamotzi\Dampning.Dub	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\INetCache\Ghetto\hamotzi\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\INetCache\Ghetto\hamotzi\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\INetCache\Ghetto\hamotzi\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\INetCache\Ghetto\Wept	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\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\INetCache\Ghetto\Wept\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\INetCache\Ghetto\Wept\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\nsc344B.tmp	read attributes | synchronize | 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	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\nsc344B.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\nsc344B.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\nsc344B.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\nssF5CA.tmp	success or wait	1	4034AC	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsc344B.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\INetCache\Ghetto\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169	0	32768	0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c		success or wait	13	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Alswith\Peroxidisement\Foresprges87\SolutionExplorerCLI.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 54 fd fd 3a fd fd 3a fd fd 3a fd fd 4b fd 3a fd fd 69 fd fd 3a fd fd 3b fd 5b 3a fd 1c 5d fd fd 3a fd 1c 5d fd fd fd 3a fd 1c 5d fd fd 3a fd 1c 5d fd fd fd 3a fd fd 75 fd fd fd 3a fd fd 75 fd fd 3a fd ed fd fd 3a fd fd 75 fd fd fd 3a fd 52 69 63 68 fd 3a fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$T:::::;:]:]:]:]:u:u::u:Rich:PEL	success or wait	3	405C34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\Dampning.Dub	0	32768	30 30 30 30 45 46 45 46 30 30 32 45 30 30 30 30 30 30 30 30 43 35 43 35 30 30 44 30 44 30 30 30 35 33 30 30 41 35 30 30 36 33 30 30 35 46 35 46 35 46 35 46 35 46 30 30 30 30 41 38 30 30 42 32 42 32 30 30 46 34 46 34 30 30 30 30 32 41 32 41 32 41 32 41 32 41 30 30 32 38 32 38 32 38 30 30 30 30 30 30 41 32 41 32 30 30 39 42 30 30 30 30 35 42 35 42 35 42 35 42 35 42 30 30 37 45 30 30 30 32 30 30 30 30 32 39 30 30 30 30 36 30 36 30 36 30 30 30 30 30 30 30 34 43 30 30 32 45 32 45 30 30 42 44 42 44 42 44 42 44 30 30 30 30 41 35 30 30 44 38 30 30 30 30 30 30 44 34 30 30 30 30 39 37 39 37 30 30 38 43 38 43 38 43 38 43 38 43 30 30 30 30 42 42 42 42 42 42 30 30 35 30 35 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 36 45 30 30 34 33 30 30 30 30 30 30 44 46 44 46 30	0000EFEF002E00000000 C5C500D0D0 005300A50063005F5F5F 5F5F0000A8 00B2B200F4F400002A2 A2A2A2A0028 2828000000A2A2009B00 005B5B5B5B 5B007E00020000290000 6060600000 004C002E2E00BDBDBD BD0000A500D8 000000D400009797008C 8C8C8C8C00 00BBBBBB00505000000 0000000006E 0043000000DFDF0	success or wait	4	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 03 00 fd 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.$PEdfW" ``@@	success or wait	20	405C34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\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 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 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.$PEL" 0 `	success or wait	2	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\hamotzi\libdatrie-1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 fd 00 00 3c 00 00 00 fd 00 26 22 0b 02 02 1f 00 52 00 00 00 fd 00 00 00 0a 00 00 30 13 00 00 00 10 00 00 00 00 fd 68 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 10 01 00 00 04 00 00 fd 5e 01 00 03 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$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\INetCache\Ghetto\Wept\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 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 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.$PEd&""\dPz`	success or wait	6	405C34	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Wept\maintenanceservice2.exe	0	32768	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 08 00 4a 0e 2e 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 3a 02 00 00 1a 01 00 00 00 00 00 fd fd 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 03 00 00 04 00 00 59 fd 03 00 02 00 60 fd 00 00 fd 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$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\INetCache\Ghet to\Wept\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 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 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`<& $6PU`	success or wait	4	405C34	WriteFile
C:\Users\user\AppData\Local\Temp\nsc344B.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a fd 2d 13 44 fd 2d 13 44 fd 2d 13 44 fd fd 0f 4a fd 2a 13 44 fd 2d 13 45 fd 3e 13 44 fd fd 1c 19 fd 2a 13 44 fd 79 30 74 fd 29 13 44 fd 4e 31 6e fd 2c 13 44 fd fd 33 40 fd 2c 13 44 fd 52 69 63 68 2d 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 5d 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$ir*-D-D-DJ*D-E>D*Dy0t)DN1n,D3@,DRich-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	51	405C05	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghet to\hamotzi\Dampning.Dub	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\INetCache\Ghet to\Industrialization\Snoldets\Embrocates\Utaalmodiges.Taa169	unknown	28311552	success or wait	1	73512AF9	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