ID: 755084
Sample Name:
98765434567890.exe
Cookbook: default.jbs
Time: 10:12:41
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

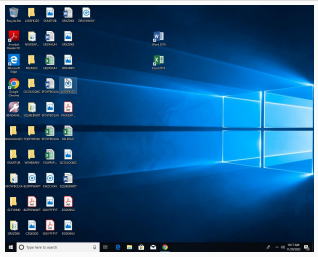
Windows Analysis Report

98765434567890.exe

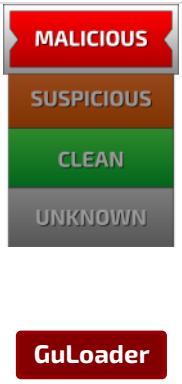
Overview

General Information

Sample Name:	98765434567890.exe
Analysis ID:	755084
MD5:	1c4e3e615e3596..
SHA1:	40365b3026ba2f..
SHA256:	622163e09e5ad5.
Tags:	exe signed
Infos:	



Detection



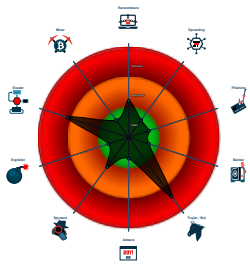
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Stores files to the Windows start me…
- PE / OLE file has an invalid certifica…
- PE file contains more sections than…
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64**
- 98765434567890.exe (PID: 5852 cmdline: C:\Users\user\Desktop\98765434567890.exe MD5: 1C4E3E615E3596572062BCA5EC498D41)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.765192426.0000000003410000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.764218177.0000000000840000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
Process Memory Space: 98765434567890.exe PID: 5852	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Yara detected GuLoader

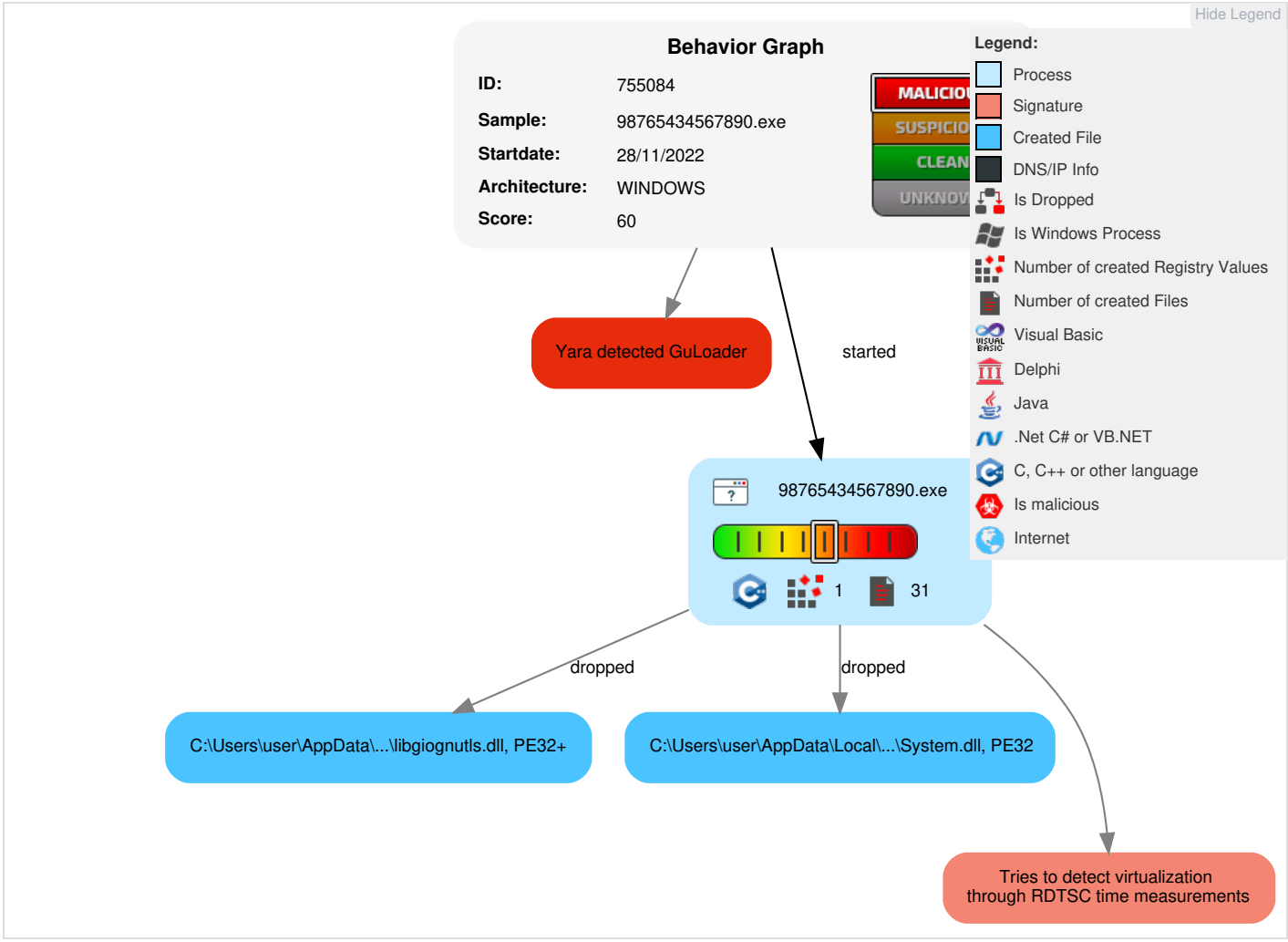
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

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

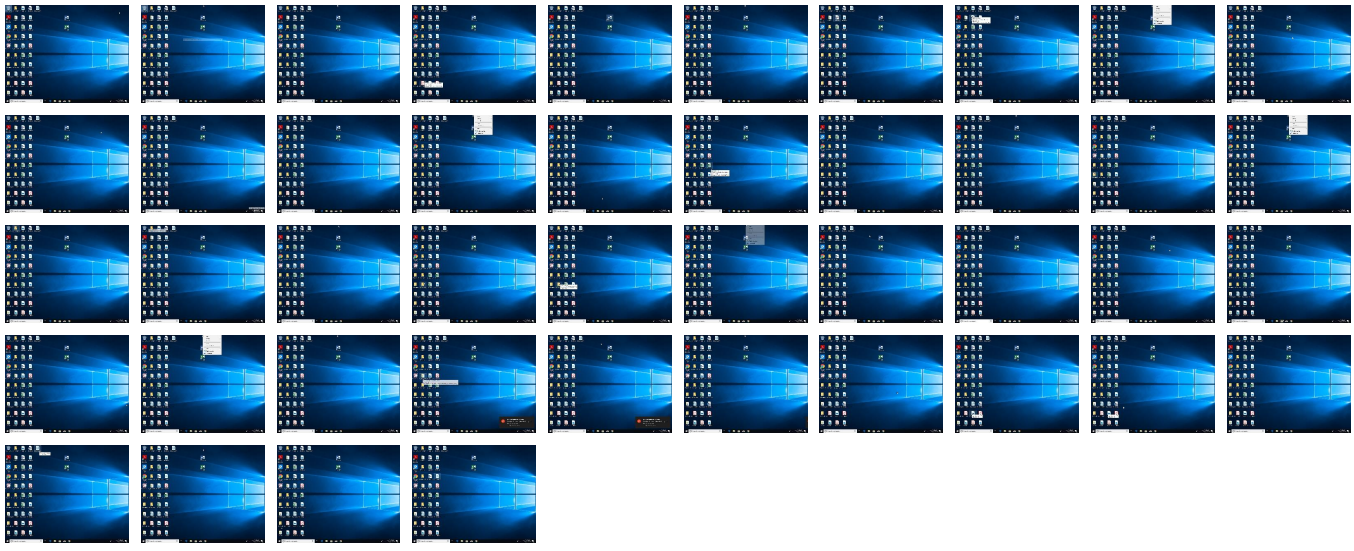
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
98765434567890.exe	5%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsa22B8.tmp\System.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsa22B8.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\libgiognutls.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\libgiognutls.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

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_ErrorError	98765434567890.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755084
Start date and time:	2022-11-28 10:12:41 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	98765434567890.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.5%) • Quality average: 87.7% • 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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsa22B8.tmp\System.dll

Process:	C:\Users\user\Desktop\98765434567890.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\Epithem.Dre

Process:	C:\Users\user\Desktop\98765434567890.exe

File Type:	data
Category:	dropped
Size (bytes):	71042
Entropy (8bit):	**7.997487610071428**
Encrypted:	**true**
SSDEEP:	1536:LoTgnjw+E7cYT8/O3qCaPdc4MgMHJB5KGSZfV:cww+8YSqnG4MNoGSD
MD5:	B11B64A276E8FEB3D09F2CBCEE1DA91D
SHA1:	AC7191608193A7479C7BE2AD72754D60BB22801B
SHA-256:	5F2966EE48ACB731DCE5B8977D6A61C891059058B76F03F670A75C3B2BDB83EA
SHA-512:	CA023A0D961F3E4886F5345EE9A877B632D017AC2028DEAB0AFD6BBDB86F19AD9E018CD16F1A692764076FD556FB8AD3BA01366B013EC35153C1BC88B9D9B3B4
Malicious:	false
Reputation:	low
Preview:	.M...V.).....q.7Q....8P.@d.E..ls....f..u*..d.]${1##.B*g...I..sf...(.....f..J..7....Q....&..._py.O.?.v...@q..L..nD.o..!o.Y..W*...q.(9.....f..F...>Bl.6....E?..'....{v..5.o>c..r1.....P.......?...,..4.....%....C;.`..g9..U.^....b.v.dXC..*.g...^....a..}V"..a..'...&..w....6...,^...z.#g....d..,..M@..{_...Aiu....y~..*#..bW.x...R.Z.....YN..?H....t....>.Im'.Kl...EDT.....&...7L..^...A.....k|....f1.....U.R.y/...X.a...I....g.....+.F..=a...{.C....n..[A....w^.R.d9.]+.......O..{V..e.....&...hl..G...ZF..,[.....4...&5J(}gH...b......CL.H;z0.._}.....q..*..My=.`.7>.F....../|1..}.B_.C..LV.[...o...W....Q#&.....1hkq.1u...'O<.........6U...h....m....}F]D....T..S.B....X.bs..#%...9c.s.k;....o.KL..M,s.l.{.\....eu._Es.+.G.Q..y.p...Bi...^.....?.....>...%....!U..N...*.').tZ[&...s...R.^....%Z..H..3.....TBq'.T:s1..d...]... ...H.46K*....(.^...@.U.7.;.....Q....w.....F..}'...L...f}.....,o...WJ...(.. ....|!.....B...MZ...^@j.....H.R.]'.v%P.w.e..KBVQ.(.<.g

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\libgiognutls.dll

Process:	C:\Users\user\Desktop\98765434567890.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	131991
Entropy (8bit):	5.8780987492725405
Encrypted:	false
SSDEEP:	1536:v6J1cdTEl2OzvUtevCuoCW9fPr+vo9F5J7YWv3vbRnBycYWOGWSeaGymtYWOGWSS:VdW2OLgNCwXKSH8WPvVBjA+KE8S5
MD5:	10D998CF80B4437C2979B25EBCBE16D1
SHA1:	79C99DD2ABB99253E41C5E40DAB29522F93345BB
SHA-256:	A0A87BC30F4B39D7B642841A10208CE5286C6CA712B28B9D921E1EA6F547AEE6
SHA-512:	44863645B48815C3C248111F86440E3A0C515AF61B5A17D15B5A6C7304277F76056BCEB6C579E7824E11ADCA4DB3E385FA8019D602C40FA527E725C09B6AA523
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.....&"...%.....P.....@.....g}.. ..`... .....IE.....0..... i..(.....text...X.....`..`.data..... .....@. ...rdata...A...0...B.....@..@.pdata.....R.....@..@.xdata..X.....`.....@..@.bss....p.....edata.....n.....@..@.idata.. IE.....F...p.....@....CRT....X.....@....tls..... .....@....reloc.....0.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing\Trespassage\Importprisernes.Qui

Process:	C:\Users\user\Desktop\98765434567890.exe
File Type:	data
Category:	dropped
Size (bytes):	178390
Entropy (8bit):	6.530973591237936
Encrypted:	false
SSDEEP:	1536:D2+s6BE+9e6acEoJlwBCIQBMvbN+r9dt0ppPn4t2vcCTAgP+48IhsckBtg6:DVur6aRwssypZ4t2kCMgP8cWtg6
MD5:	EE4440124C925FE4F95735EA4568FAE6
SHA1:	C7428FDB29B43C77589FF0C160AEE0C063DD20A1
SHA-256:	08705B17B6DAE5798AD5AE935FC23CFFE929B3EA490C0D0F09EBD6F1CE19E4A2
SHA-512:	C8927169A8395684C24C680498A152D53FCCFD3C5D05E0CB83926565C77BDAE6F9468744FC2A010E45FD6E6860877AA05F6067C3A2484BD1E26BBE780A01E82
Malicious:	false
Reputation:	low
Preview:	*....[?E..+ .;..."x.2k...1..`._.i...{.H.?.....+,O.....,.D6#...1^I..&.{&-P#.`.....Q.c....o....Fw-..Ts[....U.w_F....c..?....i...Hk.....>*.mr...Oj...Vz..(..0.RO.I../...t4.(.X.....XD..^.&...9g.D'.> \..8=0T!.....B'!.R....d.>\...Ho.....E..m...94..)..s...h.....HI.....T.g5.....L(i.Vz.YM.....Z.D../....`....Q$9....c.GDk".....;..<.....(..?.....Y.7.....[.]O.....S36.....&D.....9u. ^.a`....5T.I?.I..Ha.ks....[]=..h...2....:....P.'..^.p..@+.s.....l4p<...2.-.q.7q...O..w..],.....x(k....v.!Ih3n..il....sa.....Z...5..=.Z1y.P..c7..R.^....B..+..I.NA!x.+Z...:...U.(...E@cqQ... ..+..@....]/.A..4.....<L8h..gbW...G,.qN<`.17t.P...$#.Y....Y.t.....z."...\..u.q...-..w.....B....].v..."cZ]\..P...f...Iy....2.m../..{.0.B.w....C.&J_..AA.....Y(....R...-....f.B....R...d..w...|..nR ..X.2.2..>9%`..f/#OT`W.C.0....=9.g..uBTb..0..2...Q.ir.Aq...LT..IU.c.$xk....??g.{.....V.....w.....K...\5..b.....[%...`..\....ga.. .Xq.PTS..;<....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.422995711933732
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:	98765434567890.exe
File size:	428864
MD5:	1c4e3e615e3596572062bca5ec498d41
SHA1:	40365b3026ba2fca699462877fc106d58d2406c2
SHA256:	622163e09e5ad5324887c02d7834628d7213015fc48d286d69b4a90fa17a772d
SHA512:	2e87606c186203ee5018d737721e6de9e5ccfbc3c541f71dc7e836c705d8afa7a41e13b8e70f85223b41117323b9c15cc3301b3438eee5cf26200e48c01ba033
SSDEEP:	6144:0wq3NpnsvZK26XgmwnTi512noHCAibaH+Z23pSzpQl2sCbtORgNbTg:0z772qgvq2njDme2pSzZhtE
TLSH:	D894DF95F78106D9DC75577149BB9D370277BD3E18B10B9F62AD32312F332828A07A2A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	b8eee6a4c0c8c6c2

Static PE Info

General

Entrypoint:	0x40344a
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:	0x584DCA38 [Sun Dec 11 21:50:48 2016 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:	4ea4df5d94204fc550be1874e1b77ea7

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Derobe, OU="Papirspose Dokumentfilens ", E=Drikkelagets@Unaadigt.Sh, O=Derobe, L=Neu Duvenstedt, S=Schleswig-Holstein, C=DE
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	• 12/3/2021 7:47:31 AM 12/2/2024 7:47:31 AM
Subject Chain	• CN=Derobe, OU="Papirspose Dokumentfilens ", E=Drikkelagets@Unaadigt.Sh, O=Derobe, L=Neu Duvenstedt, S=Schleswig-Holstein, C=DE
Version:	3
Thumbprint MD5:	13BD13A74F5989BBBF4626613B253C7F
Thumbprint SHA-1:	3FF1D875731FD030D811E21481EF38D2C90E217A
Thumbprint SHA-256:	919DEF4FB98F825B484FBCC82721EDA3F9094E0BAFFBEF15B4BC145160DD6350
Serial:	1254C7D01C8577B0

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007FB478C09843h
push ebx
call 00007FB478C0C99Ch
cmp eax, ebx
je 00007FB478C09839h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FB478C0C916h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FB478C0981Ch
push ebp
push 00000009h
call 00007FB478C0C96Eh
push 00000007h
call 00007FB478C0C967h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007FB478C0C550h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FB478C0C53Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x28868	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x675d8	0x1568	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.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	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x43000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6e000	0x28868	0x28a00	False	0.4693269230769231	data	6.072692072533226	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6e3b8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x6e720	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x7ef48	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x883f0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x8d878	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x91aa0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x94048	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x950f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x95a78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x95ee0	0x144	data	English	United States
RT_DIALOG	0x96028	0x13c	data	English	United States
RT_DIALOG	0x96168	0x100	data	English	United States
RT_DIALOG	0x96268	0x11c	data	English	United States
RT_DIALOG	0x96388	0xc4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x96450	0x60	data	English	United States
RT_GROUP_ICON	0x964b0	0x76	data	English	United States
RT_MANIFEST	0x96528	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, WaitForSingleObject, GetCurrentProcess, CompareFileTime, GlobalUnlock, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, lstrcpyW, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GlobalFree, GlobalAlloc, GetShortPathNameW, SearchPathW, lstrcmpiW, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, lstrcmpW, GetDiskFreeSpaceW, lstrlenW, lstrcpynW, GetExitCodeProcess, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, MulDiv, MultiByteToWideChar, lstrlenA, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, IsWindowEnabled, EnableMenuItem, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, wsprintfW, ScreenToClient, GetWindowRect, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, LoadImageW, SetTimer, SetWindowTextW, PostQuitMessage, ShowWindow, GetDlgItem, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegDeleteKeyW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges, RegOpenKeyExW, RegEnumValueW, RegDeleteValueW, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: 98765434567890.exe PID: **5852**, Parent PID: **3320**

General

Target ID:	0

Start time:	10:13:38
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\98765434567890.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\98765434567890.exe
Imagebase:	0x400000
File size:	428864 bytes
MD5 hash:	1C4E3E615E3596572062BCA5EC498D41
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: 00000000.00000002.765192426.0000000003410000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000000.00000002.764218177.0000000000840000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	4058C9	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\nsf214F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\nsf2150.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
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	3	4058C9	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing\Trespassage	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing\Trespassage\Importprisernes.Qui	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\libgiognutls.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\Epithem.Dre	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user~1\AppData\Local\Temp\nsa22B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
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	4058C9	CreateDirectoryW
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C9	CreateDirectoryW
C:\Users\user~1\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	4058C9	CreateDirectoryW
C:\Users\user~1\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	4058C9	CreateDirectoryW
C:\Users\user~1\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	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\nsa22B8.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	405889	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\nsa22B8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user~1\AppData\Local\Temp\nsa22B8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	2	405E13	CreateFileW
C:\Users\user~1\AppData\Local\Temp\nsa22B8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	19381	405E13	CreateFileW
C:\Users\user~1\AppData\Local\Temp\nsa22B8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	6	405E13	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf214F.tmp	success or wait	1	4036D7	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsa22B8.tmp	success or wait	1	405A32	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	405EB3	WriteFile
unknown	43505	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing\Trespassage\Importprisernes.Qui	0	16384	2a 0a 1c 7f fd 5b 3f 45 fd fd 2b 20 fd 3b 03 fd fd 22 78 fd 32 6b fd fd 16 31 fd 08 60 fd 5f fd 69 fd fd fd 7b fd 48 fd 3f fd fd 0e fd fd 2b 2c 4f fd fd fd e1 fd fd fd 2c 9c 44 36 23 fd fd fd 31 5e 49 fd fd 26 08 7b 26 2d 50 23 fd 60 fd fd fd fd 05 fd 0a fd fd 1b 51 fd 63 fd fd fd fd 6f fd 01 fd 01 46 77 2d fd 88 54 73 5b 1d 10 05 fd 55 6d 77 5f 46 fa fd 90 fd 63 a9 fd 3f fd fd fd fd 69 fd fd fd 48 6b 00 fd fd fd fd 3e 2a 00 6d 72 fd fd 1e 4f 6a fd 92 11 56 7a fd fd 28 fd 11 30 fd 52 4f 13 49 fd fd 2f fd 03 fd 74 34 fd 28 1c 58 02 2e fd fd fd 58 44 fd fd 5e fd 26 fd fd fd 39 67 a0 44 27 1a 3e 5c 0c fd 38 3d 30 54 21 fd fd fd fd fd fd 42 27 21 fd 52 01 fd fd fd 64 fd 3e 5c fd fd fd 48 6f 07 0e fd 06 fd 45 fd fd	*[?E+ ;"x2k1`_i{H? +,O,D6#1^l&{&- P#`QcoFw-Ts[Uw_Fc? iHk>*mrOjV z(0ROl/t4(X.XD^&9gD'>\ 8=0T!B'!Rd>\HoE	success or wait	11	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\libgiognutls.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 01 00 fd 01 00 00 fd 00 26 22 0b 02 02 25 00 0a 01 00 00 fd 01 00 00 04 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 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 40 02 00 00 04 00 00 67 7d 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.$PEd&"%P@g}`	success or wait	9	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\Epithem.Dre	0	16384	fd 4d fd fd fd 56 fd 29 4e 05 fd fd fd fd fd fd 71 02 37 51 fd fd fd 2e 38 50 fd 40 64 fd 45 fd fd 6c 73 fd fd fd fd 66 fd fd 75 2a e1 fd 64 fd 5d 24 7b 31 23 23 0f 42 2a 67 fd fd fd 49 fd 1a 73 66 fd fd fd 28 fd fd fd fd 1b 66 fd fd 4a fd fd 37 0f 05 fd fd 51 1f fd fd fd 26 fd 0b fd 5f 70 79 fd 4f 0a 3f fd 76 1b 04 1a 40 71 96 fd 4c fd fd 6e 44 0a 6f fd fd 21 6f 7f 59 fd fd 57 2a fd fd fd 71 fd 28 39 fd fd 12 fd fd 66 fd fd 46 fd fd fd 3e 42 6c fd 36 fd fd 2e fd 45 3f fd fd 27 fd 0a fd 19 7b 76 fd fd 35 fd 6f 3e 63 fd fd 72 31 fd 07 01 fd fd 50 fd fd 65 fd fd 0e fd 3f fd fd 00 2c fd fd 34 fd 13 fd 14 fd 06 fd fd 25 fd 80 fd fd 43 3b 0d 60 14 fd 67 39 fd fd 55 08 5e 07 fd fd fd 62 fd 76 12 64 58 43 fd fd 2a fd 67 fd fd	MV)q7Q.8P@dElsfu*d]${1##B*gIsf(fJ7Q&_pyO?v@qLnDo!oYW*q(9fF>Bl6.E?'{v5o>cr1P?,4%C;`g9U^bvdXC*g	success or wait	5	405EB3	WriteFile
C:\Users\user\AppData\Local\Temp\nsa22B8.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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 1a fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELMX!	success or wait	1	405EB3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\98765434567890.exe	unknown	512	success or wait	337	405E84	ReadFile
C:\Users\user\Desktop\98765434567890.exe	unknown	16384	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	26356	success or wait	1	403269	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	4	success or wait	3	405E84	ReadFile
C:\Users\user\Desktop\98765434567890.exe	unknown	16384	success or wait	13	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	16384	success or wait	25	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	4	success or wait	2	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsf2150.tmp	unknown	4	success or wait	19381	405E84	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\X\Unsalty\Epithem.Dre	unknown	2	success or wait	318	4026D2	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\antagonizing\Trespassage\Importprisernes.Qui	unknown	1052672	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Spaan\Pushfully	success or wait	1	40242E	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan\Pushfully	Trials101	binary	FF C0 52 EF	success or wait	1	40248E	RegSetValueExW

Disassembly

No disassembly