ID: 736966
Sample Name:
XShSI2OXaC.exe
Cookbook: default.jbs
Time: 12:40:26
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

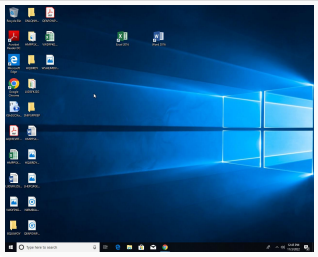
Windows Analysis Report

XShSI2OXaC.exe

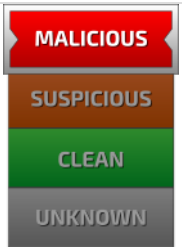
Overview

General Information

Sample Name:	XShSI2OXaC.exe
Analysis ID:	736966
MD5:	b69c9170ffab277..
SHA1:	8928e5d360edbe.
SHA256:	a8148946081866.
Tags:	exe signed
Infos:	



Detection



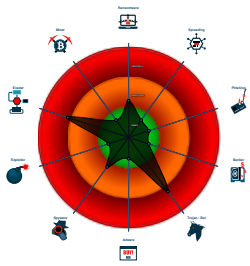
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- XShSI2OXaC.exe (PID: 5820 cmdline: C:\Users\user\Desktop\XShSI2OXaC.exe MD5: B69C9170FFAB277E1BD13FDE891A5AE5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.777436198.0000000003220000.00000040.00001000.00020000.00000000.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

Data Obfuscation

Yara detected GuLoader

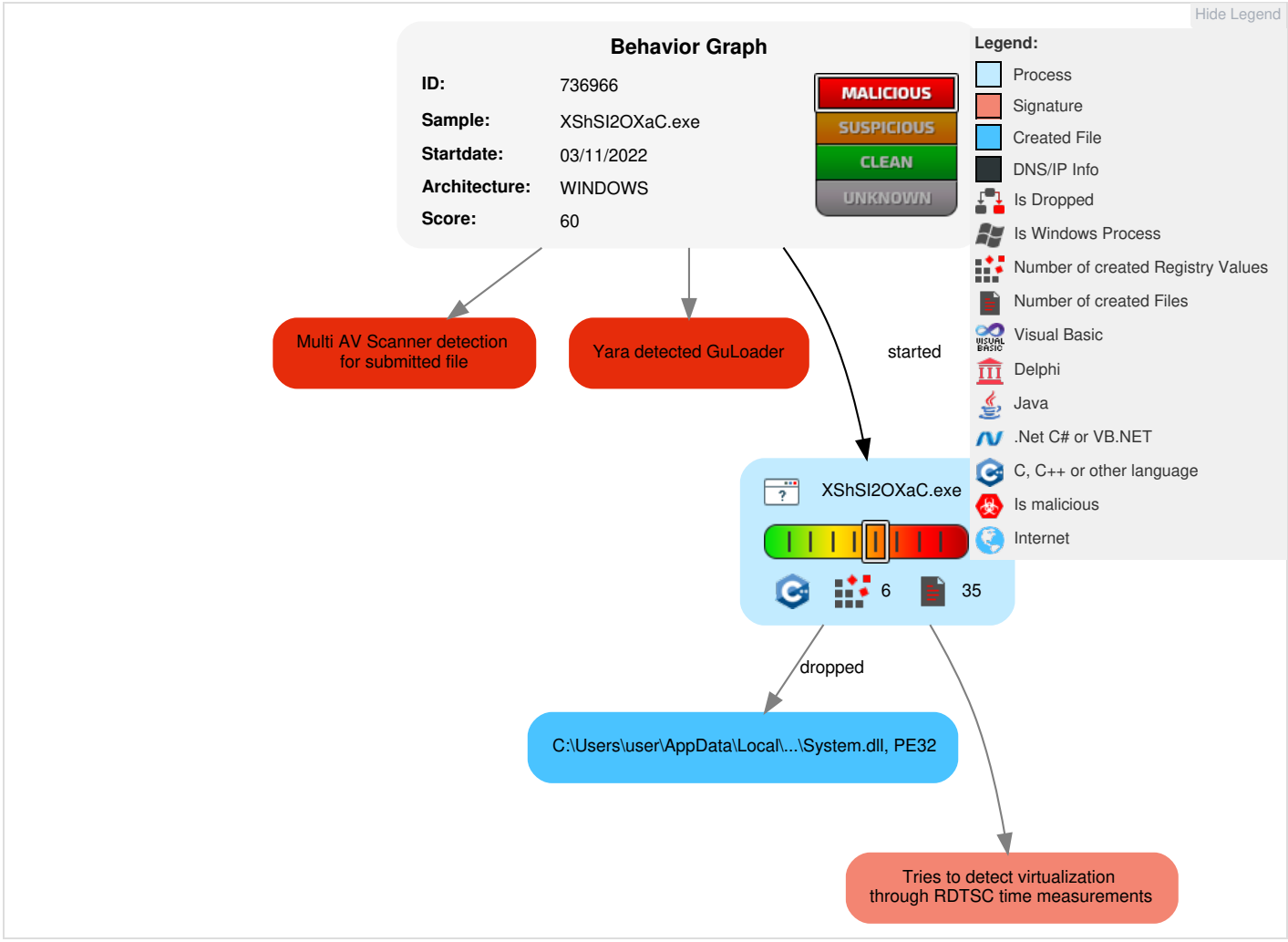
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 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 Windows Service	Rootkit	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)	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

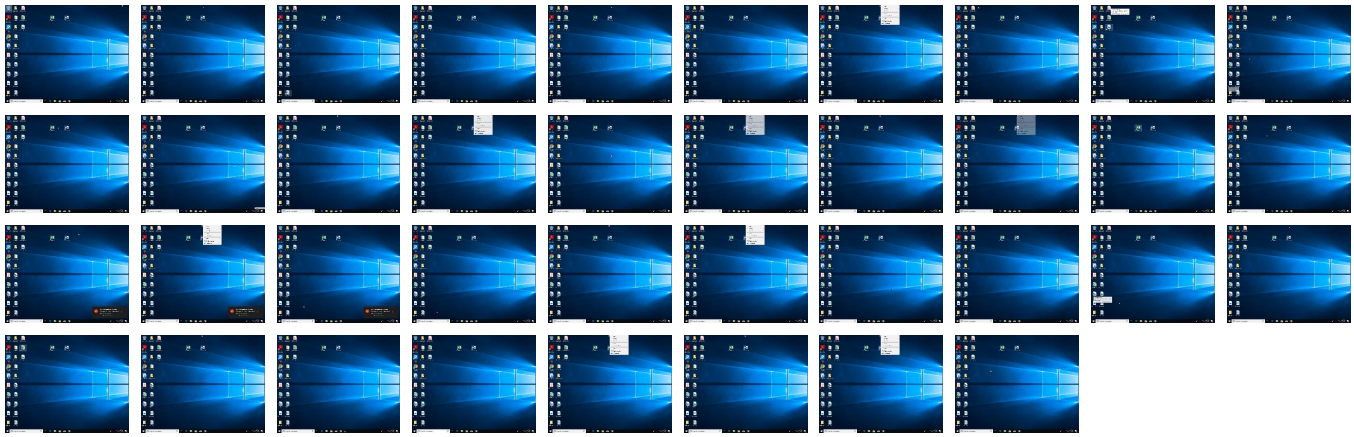
Behavior Graph



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
XShSI2OXaC.exe	40%	ReversingLabs	Win32.Trojan.InjectorX	
XShSI2OXaC.exe	8%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	4%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctnca2.crl0l	XShSI2OXaC.exe	false		high
http://repository.certum.pl/ctnca2.cer09	XShSI2OXaC.exe	false		high
http://crl.certum.pl/ctsca2021.crl0o	XShSI2OXaC.exe	false		high
http://repository.certum.pl/ctnca.cer09	XShSI2OXaC.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	XShSI2OXaC.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	XShSI2OXaC.exe	false		high
http://crl.certum.pl/ctnca.crl0k	XShSI2OXaC.exe	false		high
http://subca.ocsp-certum.com05	XShSI2OXaC.exe	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	XShSI2OXaC.exe	false		high
http://subca.ocsp-certum.com02	XShSI2OXaC.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	XShSI2OXaC.exe	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736966
Start date and time:	2022-11-03 12:40:26 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XShSI2OXaC.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:	15
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@1/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86.1% (good quality ratio 84.8%) • Quality average: 88.3% • Quality standard deviation: 20.8%
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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\hale4r.lnk

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	852
Entropy (8bit):	2.8931668942154323
Encrypted:	false

SSDEEP:	12:8gl0gsXou41w/tz+7RafgKDuKiP/3NJkKAd4t2Y+xIBjK:8/f4eaRMgKxiX9HAv7aB
MD5:	4C35348ABAD84AE5B63C7EE3148E0F95
SHA1:	6805EF5D68BFDFF71F2841255892BC1957AE40AA
SHA-256:	0D6C1CB8C1BB8471AA59E453AE72C69B894A85EB2CE3AE3EFAE789CC89D92ADF
SHA-512:	74CB2490211DC4163D2AEA5C550338806070CD90FA7A461A2DBFBBC96B49CB44E2F351BAFAD5D3B201263923A2E674209C6DEBD1C3C7F746DDBE694216EB8320
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	L.....F.....#....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<.....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....`.2.....hale4r.txt..F.....h.a.l.e.4.r...t.x.t.....\.h.a.l.e.4.r...t.x.t.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	12288
Entropy (8bit):	5.737504888129487
Encrypted:	false
SSDEEP:	192:BenY0qWTlt70IAj/lQ0sEWc/wtYbBH2aDybC7y+XB9IwL:B8+Qlt70Fj/lQRY/9VjjlL
MD5:	8CF2AC271D7679B1D68EEFC1AE0C5618
SHA1:	7CC1CAAA747EE16DC894A600A4256F64FA65A9B8
SHA-256:	6950991102462D84FDC0E3B0AE30C95AF8C192F77CE3D78E8D54E6B22F7C09BA
SHA-512:	CE828FB9ECD7655CC4C974F78F209D3326BA71CED60171A45A437FC3FFF3BD0D69A0997ADACA29265C7B5419BDEA2B17F8CC8CEAE1B8CE6B22B7ED9120BB5AD3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 4%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....].....!.....".....)....@.....p.....@.....B.....@..P.....`.....@..X.....text...O .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\Plugin_Status.ini

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	102
Entropy (8bit):	3.52328456258532
Encrypted:	false
SSDEEP:	3:Q++l3293myVfslYx5hev/LmRlfVRlVl:Q++lQWyVkixm3up
MD5:	4F9A42DF26A7D4555300076765236140
SHA1:	1F97D929B2FEC9B8171BC8433F046753E66A10A9
SHA-256:	35BFF73B98E198313A09FDC972F7E9F16014C7E96ACA96A094510D3F6462473C
SHA-512:	26C627C99A9F1BE9C311C3B185A258BC5FE2DF9DB3AB7657BB2582940C185252AB586F6F20A8086E530D4A946BD9DF495F0C43C4C9259225945E16AC61AF5C0
Malicious:	false
Reputation:	low
Preview:	..[.A.R.M.O.U.R.Y. .C.R.A.T.E. .S.T.A.T.U.S.].....A.u.r.a.P.l.u.g.l.n._.V.e.r.s.i.o.n.=.4...0...0...0.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\vfslog.c

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	22849
Entropy (8bit):	5.11077967265171

Encrypted:	false
SSDEEP:	384:mF+fT69ihYf2GM4R07AZl5dNkWb5jaxZBqOVSSZREtMOPSXCm:mf6AZlNJb5jaxDqRSZgk
MD5:	1C9F1050DD84B2B185741F28309D3B30
SHA1:	740C9AAFF5D67D3254239B5509D613E4BE9B5B85
SHA-256:	669D3FF0B8649789381CDBB5897462488 98AFB4EBC2053952E57EB9475F5064A
SHA-512:	4A568558B4EF9ED4CA579E8DFBB0FDFFFFE6A442AE11E1FF48E1DB93267469BF66BC3B10DA3397A30C362E4F4CE0A1367E6266D0A78BC61060C103BB4625A1CF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	/*.** 2013-10-09.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** **********.**.** This file contains the implementation of an SQLite vfs wrapper for.** unix that generates per-database log files of all disk activity..*/../*.** This module contains code for a wrapper VFS that causes a log of.** most VFS calls to be written into a file on disk..**.** Each database connection creates a separate log file in the same.** directory as the original database and named after the original.** database. A unique suffix is added to avoid name collisions. .** Separate log files are used so that concurrent processes do not.** try to write log operations to the same file at the same instant, .** resulting in

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Coronoid.Ano

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	data
Category:	dropped
Size (bytes):	169398
Entropy (8bit):	6.943066252449536
Encrypted:	false
SSDEEP:	1536:kYNzSfaJrHw2kpeuoo3koyTLZbsBnqxlkTfIYsZYR0JY6nue2HSPKb4aBSBXPVso:OaRSpXo/DLZe9rlsU0JDnUAKb4USV2M
MD5:	41A2DEFADC6A543205116432277F62D5
SHA1:	FEBF4BE1B62529495501EAECE3E4691342F021C7
SHA-256:	13DC3B2288380DB05CF9DDFA1EEBB66DB7C01035D3B895242824BC7CE2E6DC55
SHA-512:	3C548C50A93B730B903A1EBEB65DC73C07238E56F2EFBCFFA986B8A63C4628FA677A157A0C3AE52123B2FA21FEFBF2966EEB7E0646EB43A4EEC9A25D035D86CC
Malicious:	false
Preview:	.../.{....kD..>...I^{..h.}:).v}..e....D(.|Y).....j.....?.nA..0..m..>.r...V..']1.=.....*.d...../s*.+8..@.0.j...?6g,^v..:....mF...P4.O....BM.s..,mq.u....!2L..h..p..h.%:wm..GH.K.....S..}....hB.N.=.E0)....S.@2..Q5.T...m.].}...cYqL....._....s.....S....4..hs...T..R...R?%.=.s.@N...Q..F...!.a.....".M....[3..-.....h....xe.M.....5$..d|.c.;...T.S..SE.V.]...?a...0.I...!"..Rc..y.-1....[.Ou...c./UOEf.}T]..?r.[A...F..F@:..|-x".....k....II"4.pY.....0.j..3.I....J6.P..2.(.Js..U:...N..Qp..e.....Q.uLF...Xg..*.4..x.....j>W.m.t.X..\.w.H:)y.....}....v.<..y..q1.{..&f/...h.....vh..d.(..vi...._.....E.q..'N.uHKt9Y.R.#:m.|.S..FLU9`.,N...S{.6l....frgH.Q..r..1...;Y.->..e7:2)k@-S.P....\...6.(m.xm.C.H..&R.<3An.n..B....N.z}...\mX`...^!..(@.Y.I..QKk...Ik..A@Z....>T.Pp.~./...F.(..q.<b"%.....;XO...W.....".4..UA._.=.|..|.....at_....^..%!...K..\.b..S.,..R...[..2i..!.c.hs9]1za.X.F-o\...q..L...a..6.q....l.I..Y...V.T.J.7..{..@&.%v....T]..R..b..B...D...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts\Newcomers\Igennen\view-more-horizontal-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\XShSI2OXaC.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	136
Entropy (8bit):	5.506031499655005
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll8xn9gR5XfixtIS2kj7QJ/lsg1p:6v/lhPys6aorIStC2up
MD5:	1E05E353B63930E92518EC5136819E9E
SHA1:	82E22F6A10959DDF998F17799BC8257528DF9C8E
SHA-256:	8E686112200E526D3928BF2F717A00B2E6EC74826AB3DC3AB63F7B5D6F760348
SHA-512:	E2896BB1D9C1514C7F6E6A60F4E1614FEF8DCBE774AEE4FA977C7DE91BBF37DDE6D45ECA73730082182226B8D3F755A06528FF57C4294F7F1AAD50910FB7A3E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....?IDAT8.c`....x200<b``x....A..c....P..I!Q.L...7...S...'P.+>....._Di>.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.775192199206559

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:	XShSI2OXaC.exe
File size:	192936
MD5:	b69c9170ffab277e1bd13fde891a5ae5
SHA1:	8928e5d360edbecd1547cf61831d4f055bed92af
SHA256:	a8148946081866414 6f756543f081b702bcb69244ebf8f6a240b02b2357c577c
SHA512:	0bf095bdc0bd8c0898952e83249930fd02f68415915681a11cfed7276f7949384ed8cea8ee2339dfd567ca298402768e86a6e795086629c642c11a9d932d0196
SSDEEP:	3072:PSrFD0QAGq6muqIpb5Hp15W0Om6GHAPulczSd8/Zjx5lY8pV+DdhLeWxSbTEZfSu:7QA4WaniPVSd8xfIY8Ygmjd
TLSH:	8214F1513AB0E507ED275A3118796F273FF1791A19918B0B6350BBAA7D23380866F31F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....18..PV..PV..PV.*_...PV..PW.MPV.*_...PV..sf..PV..VP..PV.Rich.PV.....PE..L.....]..... f...*.....5.....@

File Icon

Icon Hash:	f4f0d0dc4cccdcd4

Static PE Info

General

Entrypoint:	0x40350d
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:	0x5DF6D4ED [Mon Dec 16 00:50:53 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:	24f4223e271413c25abad52fd456a9bc

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	OU="Mesterlig Efterbehandlingen Buggy ", E=rykninger@Vasks.Ud, O=Professionalisere, L=Paris 14, S=\xcele-de-France, 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	• 11/2/2022 4:13:09 PM 11/1/2025 4:13:09 PM
Subject Chain	• OU="Mesterlig Efterbehandlingen Buggy ", E=rykninger@Vasks.Ud, O=Professionalisere, L=Paris 14, S=\xcele-de-France, C=FR
Version:	3
Thumbprint MD5:	C6482E31BD649A8F80BC03910D4D9041
Thumbprint SHA-1:	D014D5D190B882F8D11FE7402087EB970E60A7DB
Thumbprint SHA-256:	44451256F3DBCD4B695F950230470C038611B2648483EF95256B6744B7A32134
Serial:	08753235BB3B561B

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi

Instruction
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 [004080ACh]
call dword ptr [004080A8h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042A24Ch], eax
je 00007F6E64BD9BC3h
push ebx
call 00007F6E64BDCE97h
cmp eax, ebx
je 00007F6E64BD9BB9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F6E64BDCE11h
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F6E64BD9B9Ch
push 0000000Ah
call 00007F6E64BDCE6Ah
push 00000008h
call 00007F6E64BDCE63h
push 00000006h
mov dword ptr [0042A244h], eax
call 00007F6E64BDCE57h
cmp eax, ebx
je 00007F6E64BD9BC1h
push 0000001Eh
call eax
test eax, eax
je 00007F6E64BD9BB9h
or byte ptr [0042A24Fh], 00000040h
push ebp
call dword ptr [00408040h]
push ebx
call dword ptr [0040829Ch]
mov dword ptr [0042A318h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408184h]
push 0040A384h

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	0x65000	0x36e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2d280	0x1f28	.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	0x2ac	.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	0x647b	0x6600	False	0.6578967524509803	data	6.426522741823245	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1384	0x1400	False	0.45	data	5.136348990166042	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20358	0x600	False	0.5032552083333334	data	4.005849468822358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x3a000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x65000	0x36e0	0x3800	False	0.44998604910714285	data	5.471517583781187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x652b0	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x65618	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_DIALOG	0x67bc0	0x144	data	English	United States
RT_DIALOG	0x67d08	0x13c	data	English	United States
RT_DIALOG	0x67e48	0x100	data	English	United States
RT_DIALOG	0x67f48	0x11c	data	English	United States
RT_DIALOG	0x68068	0xc4	data	English	United States
RT_DIALOG	0x68130	0x60	data	English	United States
RT_GROUP_ICON	0x68190	0x14	data	English	United States
RT_VERSION	0x681a8	0x1f4	data	English	United States
RT_MANIFEST	0x683a0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	ExitProcess, SetFileAttributesW, Sleep, GetTickCount, CreateFileW, GetFileSize, GetModuleFileNameW, GetCurrentProcess, SetCurrentDirectoryW, GetFileAttributesW, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, CopyFileW, MoveFileW, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, lstrcmpW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalUnlock, GetDiskFreeSpaceW, GlobalAlloc, DeleteFileW, FindFirstFileW, FindNextFileW, FindClose, SetFilePointer, ReadFile, MulDiv, lstrlenA, WideCharToMultiByte, MultiByteToWideChar, WritePrivateProfileStringW, FreeLibrary, GetPrivateProfileStringW, GetModuleHandleW, LoadLibraryExW

DLL	Import
USER32.dll	GetWindowRect, GetSystemMenu, SetClassLongW, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, TrackPopupMenu, ScreenToClient, EnableMenuItem, GetDlgItem, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, SystemParametersInfoW, EndDialog, RegisterClassW, DialogBoxParamW, CreateWindowExW, GetClassInfoW, DestroyWindow, CharNextW, ExitWindowsEx, SetWindowTextW, LoadImageW, SetTimer, ShowWindow, PostQuitMessage, wsprintfW, SetWindowLongW, FindWindowExW, IsWindow, CreatePopupMenu, AppendMenuW, GetSystemMetrics, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetTextColor, SetBkMode, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, GetDeviceCaps, SetBkColor
SHELL32.dll	ShellExecuteExW, SHGetPathFromIDListW, SHGetSpecialFolderLocation, SHGetFileInfoW, SHFileOperationW, SHBrowseForFolderW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: XShSI2OXaC.exe PID: **5820**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:41:19
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\XShSI2OXaC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\XShSI2OXaC.exe
Imagebase:	0x400000
File size:	192936 bytes
MD5 hash:	B69C9170FFAB277E1BD13FDE891A5AE5
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: 00000000.00000002.777436198.0000000003220000.00000040.00001000.00020000.00000000.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	405A1A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsyA070.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405FBE	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405FBE	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	405A1A	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	405A1A	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	405A1A	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	405A1A	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	405A1A	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	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Coronoid.Ano	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F7C	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\Plugin_Status.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F7C	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\vfslog.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F7C	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts\Newcomers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts\Newcomers\Igennen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A1A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts\Newcomers\Igennen\view-more-horizontal-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F7C	CreateFileW
C:\Users\user\AppData\Local\Temp\nszA331.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405FBE	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	405A1A	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	1	405A1A	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	1	405A1A	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405A1A	CreateDirectoryW
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	405A1A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nszA331.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	4059DA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405F7C	CreateFileW
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	7	405F7C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsyA070.tmp	success or wait	1	4037BC	DeleteFileW
C:\Users\user\AppData\Local\Temp\nszA331.tmp	success or wait	1	405B9B	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	40601C	WriteFile
unknown	46893	22546	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	40601C	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Coronoid.Ano	0	16384	02 1b fd 2f fd 7b 18 fd 06 fd 6b 44 fd fd 3e fd fd fd 49 5e 7b fd fd 68 fd 7d 3a 29 fd 76 7d fd fd 65 fd 01 10 fd 44 28 fd 7c 59 29 fd 0d fd fd fd 6a fd fd fd fd fd 3f fd 6e 41 0a fd 30 fd fd 6d fd 02 3e 1a 72 06 fd fd 56 fd fd 27 6a 31 fd 3d fd fd fd d6 fd 1e 2a fd 64 fd fd fd fd fd 2f 73 2a fd 2b 38 fd fd 40 fd 30 fd 6a 0c fd 09 3f 36 67 2c 5e 76 fd fd 3a fd fd fd fd 6d 46 fd fd 1c 50 34 fd 4f fd fd fd fd 42 4d fd 73 fd fd 2c 6d 71 08 75 fd fd 17 fd 21 32 4c 2e fd 68 fd 19 70 0e 00 68 fd 25 3a 77 6d fd fd 47 48 0e 4b fd fd 68 fd fd 53 fd 05 7d fd fd fd 13 68 42 fd 4e fd 3d fd 45 30 29 fd fd fd fd 53 fd 40 32 fd 97 51 35 fd 54 fd fd fd 6d fd 5d 00 7d 08 fd fd 63 59 71 4c fd fd fd 0c fd fd 5f fd 1f fd fd 73 fd 1a fd 1a 0f 53 fd fd 30	/{kD>I^{h}:)v}eD(|Y)j?nA0m>rV'j1="d/s*+8@0j?6g,^v:mFP4OBMs,mqu!2L.hph%:wmGHKS}hBN=E0)S@2Q5Tm]}cYqL_sS	success or wait	11	40601C	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\Plugin_Status.ini	0	102	fd fd 5b 00 41 00 52 00 4d 00 4f 00 55 00 52 00 59 00 20 00 43 00 52 00 41 00 54 00 45 00 20 00 53 00 54 00 41 00 54 00 55 00 53 00 5d 00 0d 00 0a 00 41 00 75 00 72 00 61 00 50 00 6c 00 75 00 67 00 49 00 6e 00 5f 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 34 00 2e 00 30 00 2e 00 30 00 2e 00 30 00	[ARMOURY CRATE STATUS]AuraPlugIn_Version=4.0.0.0	success or wait	1	40601C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Contentness\Filialbestyrerens\Talkability\Platybrachycephalous\vfslog.c	0	16384	2f 2a 0a 2a 2a 20 32 30 31 33 2d 31 30 2d 30 39 0a 2a 2a 0a 2a 2a 20 54 68 65 20 61 75 74 68 6f 72 20 64 69 73 63 6c 61 69 6d 73 20 63 6f 70 79 72 69 67 68 74 20 74 6f 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65 2e 20 20 49 6e 20 70 6c 61 63 65 20 6f 66 0a 2a 2a 20 61 20 6c 65 67 61 6c 20 6e 6f 74 69 63 65 2c 20 68 65 72 65 20 69 73 20 61 20 62 6c 65 73 73 69 6e 67 3a 0a 2a 2a 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 64 6f 20 67 6f 6f 64 20 61 6e 64 20 6e 6f 74 20 65 76 69 6c 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 66 69 6e 64 20 66 6f 72 67 69 76 65 6e 65 73 73 20 66 6f 72 20 79 6f 75 72 73 65 6c 66 20 61 6e 64 20 66 6f 72 67 69 76 65 20 6f 74 68 65 72 73 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 73 68 61 72 65 20 66 72 65 65 6c	/*** 2013-10-09**** The author disclaims copyright to this source code. In place of** a legal notice, here is a blessing:**** May you do good and not evil.** May you find forgiveness for yourself and forgive others.** May you share freel	success or wait	2	40601C	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Parfaits\Produktoversigts\Newcomers\Igennen\view-more-horizontal-symbolic.symbolic.png	0	136	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 3f 49 44 41 54 38 fd 63 60 18 05 fd 03 78 32 30 30 3c 62 60 60 78 fd fd fd 41 fd fd 63 06 06 fd fd 50 fd 08 49 21 51 fd 4c fd fd fd 37 03 03 fd 53 06 06 fd 27 50 fd 2b 3e 0a 06 0c 00 00 fd fd 19 5f 44 69 3e fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d?IDAT8c`x200<b``xAcPI!QL7S'P+>_Di>IENDB`	success or wait	1	40601C	WriteFile
C:\Users\user\AppData\Local\Temp\nszA331.tmp\System.dll	0	12288	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 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 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 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 22 00 00 00 0a 00 00 00 00 00 00 fd 29 00 00 00 10 00 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPEL].!")	success or wait	1	40601C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\XShSI2OXaC.exe	unknown	512	success or wait	98	405FED	ReadFile
C:\Users\user\Desktop\XShSI2OXaC.exe	unknown	16384	success or wait	1	405FED	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	4	success or wait	1	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	28524	success or wait	1	40332C	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	4	success or wait	1	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	4	success or wait	4	405FED	ReadFile
C:\Users\user\Desktop\XShSI2OXaC.exe	unknown	16384	success or wait	8	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	16384	success or wait	15	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	4	success or wait	215	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	4	success or wait	1	405FED	ReadFile
C:\Users\user\AppData\Local\Temp\nsyA071.tmp	unknown	12288	success or wait	1	405FED	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Tonefilmsgengiveren\Coronoid.Ano	unknown	1052672	success or wait	1	73792BB9	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Undeprecative	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\One	success or wait	1	406324	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Limulus	success or wait	1	406324	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Limulus\tidliges	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Tg	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Tg\Cocinero	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Tg\Cocinero\Kejserdoemme	success or wait	1	406324	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\jerkies	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\forlagsboghandlerne	success or wait	1	406324	RegCreateKeyExW
HKEY_CURRENT_USER\Software\forlagsboghandlerne\refugium	success or wait	1	406324	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Undeprecative	Reinfestation	binary	FF 7F 9C B6	success or wait	1	4024E2	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\One	Guli	dword	145	success or wait	1	4024E2	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Limulus\tidliges	Arteriolith123	unicode	Holdvis	success or wait	1	4024E2	RegSetValueExW
HKEY_CURRENT_USER\Software\Tg\Cocinero\Kejserdoemme	Ordentlig	binary	92 B2 CE	success or wait	1	4024E2	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\jerkies	idiotiskes	unicode	Antitoksinet	success or wait	1	4024E2	RegSetValueExW
HKEY_CURRENT_USER\Software\forlagsboghandlerne\refugium	Summerendes	expand unicode	%Brutter227%\Echeveria.Mes	success or wait	1	4024E2	RegSetValueExW

Disassembly

No disassembly