ID: 679245
Sample Name: xKBLVUHoY6
Cookbook: default.jbs
Time: 13:04:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report xKBLVUHoY6 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: GuLoader 3
Yara Signatures 3
Memory Dumps 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Networking 4
Data Obfuscation 4
Malware Analysis System Evasion 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 7
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll 8
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\Modregnings.Xen 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\battery-caution-symbolic.svg 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\go-first-rtl.png 9
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 11
Rich Headers 12
Data Directories 12
Sections 12
Resources 12
Imports 13
Possible Origin 13
Network Behavior 13
Statistics 13
System Behavior 13
Analysis Process: xKBLVUHoY6.exePID: 1252, Parent PID: 5192 13
General 14
File Activities 14
File Created 14
File Deleted 16
File Written 16
File Read 18
Disassembly 18

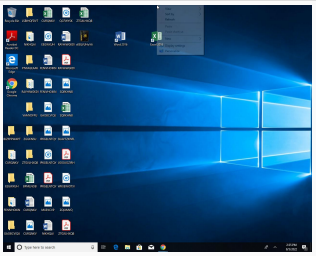
Windows Analysis Report

xKBLVUHoY6

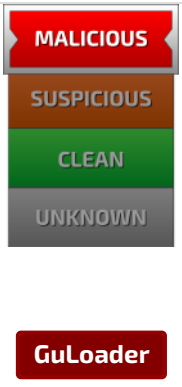
Overview

General Information

Sample Name:	xKBLVUHoY6 (renamed file extension from none to exe)
Analysis ID:	679245
MD5:	6e0bf5d5220fbe4.
SHA1:	f077644ac1eb17..
SHA256:	2914eb3edbf9da..
Tags:	exe
Infos:	



Detection



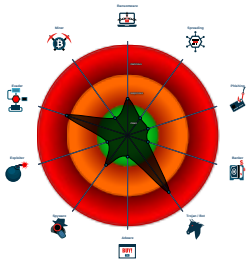
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- xKBLVUHoY6.exe (PID: 1252 cmdline: "C:\Users\user\Desktop\xKBLVUHoY6.exe" MD5: 6E0BF5D5220FBE4F7245653A259C7DAD)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://212.193.0.40/redi_oXifXcNSpB69.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.753579119.00000000031B0000.00000040.00001000.00020000.00000000.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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

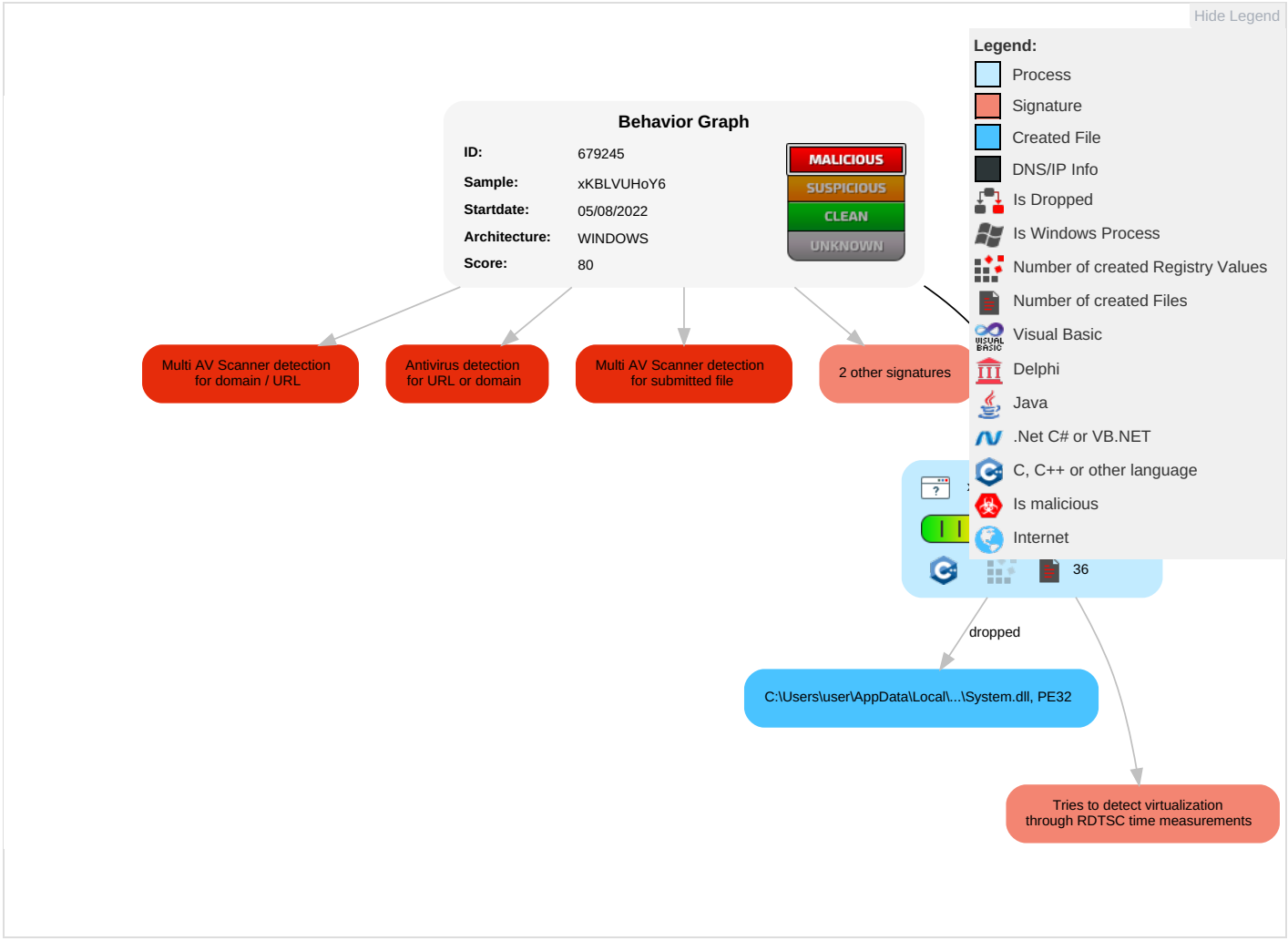
Malware Analysis System Evasion

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 1 Masquerading	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	Boot or Logon Initialization Scripts	1 Access Token Manipulation	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	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 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

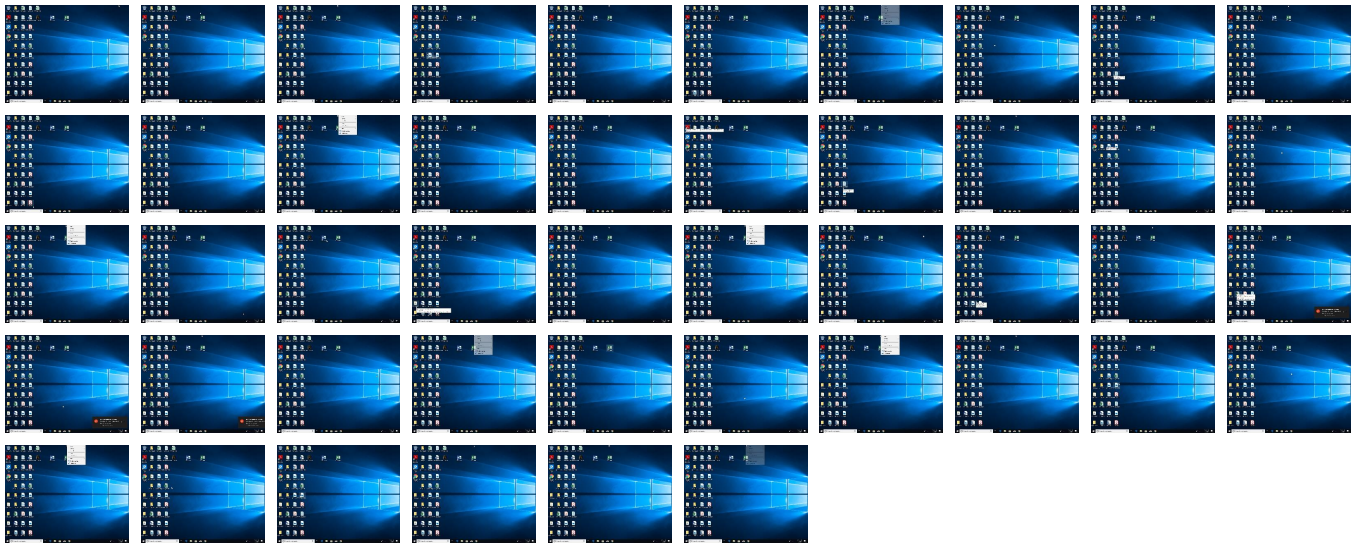
Behavior Graph



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
xKBLVUHoY6.exe	37%	Virustotal		Browse
xKBLVUHoY6.exe	6%	Metadefender		Browse
xKBLVUHoY6.exe	12%	ReversingLabs	Win32.Trojan.Gulo ader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://212.193.0.40/redi_oXifXcNSpB69.bin	16%	Virustotal		Browse
http://212.193.0.40/redi_oXifXcNSpB69.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://212.193.0.40/redi_oXifXcNSpB69.bin	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	xKBLVUHoY6.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679245
Start date and time: 05/08/202213:04:09	2022-08-05 13:04:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xKBLVUHoY6 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.6%) • Quality average: 87.5% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • 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, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, time.windows.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
13:05:12	API Interceptor	1x Sleep call for process: xKBLVUHoY6.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\Temp\nskE115.tmp\System.dll

Process:	C:\Users\user\Desktop\xKBLVUHoY6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false

Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, 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....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\Modregnings.Xen

Process:	C:\Users\user\Desktop\xKBLVUHoY6.exe
File Type:	data
Category:	dropped
Size (bytes):	89687
Entropy (8bit):	6.837509507259706
Encrypted:	false
SSDEEP:	1536:QmQLTEOmUbhvyoO0x5tFqfDDsVXK9cUcqU0C6Xi0PzBXbV8Km:NXUbhax0x5t8bDf9Mm3HJb7m
MD5:	D990EEF58440CBD9320E831F2634DA1A
SHA1:	A11659D9AF5DBA78D8255EDE08CF395EA15DDA17
SHA-256:	AB9CAE0313C6B603854407089A2680A956EBD8DDA95841FDAE71DB984FF665ED
SHA-512:	0D98927E56B9EF0C16EBB1BD075E3B3489CBD7AB3D9074B798D18969AEC044DE91663F607D4EB24F9B9789F04BA683BC779ECD6F94D75E09A354801AF4E30E D
Malicious:	false
Reputation:	low
Preview:	1...%.y....Je.UP.....(.H..O..6o..j)..*p.....8..F..C..2.U.\.S...[ju6...u..h<...o.B.91....;....a..w...q(.o0.y"x...&.....(...Y.$.Dp~....x..L.<.w..4..e.hae.....R...e..xW.2m<.....A(..Ddtm. ...j.]"%.wy...."A.U.I.`...w..Gu..^=q:.....m..t ...z.-e.P..._clf..W... v.?..#...C. .vMy...../\?.U...z.r.,B6 ...~.....i...@u..T..[...n2zA...)'S..3..P..4..A.n.$...`.>.....1...)5... -'xo..o^.c(.. .....Z....50M.3\...`....`.-...q!.....?.H.'..E.....q..?p{.!.P.....kH,.k.j...!A....X7.^.@.X.....sb.6...^.gv.(a..T..rl....Y....M.....RP.a..F.3...._....Q...=.....R...M6.8....r...f.<+..).....wV....1O.L .7iink..u$8....X.e.+..2.%...:.'...@..0....5].~.!...?..>o....~q.B.$..MJ.$H:..r;.....Ty.Z..?.?.E..O~Xh..p..'m..`.w....s..G...6.:...4.....F..~..1w@..M.k...?:)SS.[....s.G.>I,.....|.....m..!M .I.x[.K..p.Q..Z..]N...Qd.....4/...,%...:.`H.,T.J2...;....Jg1...3~....!._v.Pa...../.....r.4k.i....vJ!.....Q56..4RU...z.j.x.....b..gDL9.n....o... .H.;F.y!V>..X...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\battery-caution-symbolic.svg

Process:	C:\Users\user\Desktop\xKBLVUHoY6.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1219
Entropy (8bit):	5.18916336052597
Encrypted:	false
SSDEEP:	24:t4CYMqjwbC4KyKbRAecFhBrNxrGDT/alXuprPQ5VIblrGDRt:ojWCRNtAecFZwDT/AJsD7
MD5:	DE8960A1E15CF658A3FE4A2CAFDAA0D1
SHA1:	7EC7A95E4BC7BA19B3EC19366E87038C3902B430
SHA-256:	DF5925D3EC8C8EDD53FCEC6D7249888D9909B3D245E056028FD668DB4E23CB9B
SHA-512:	91D29A34227DD0DD672519999D32A68F8EB61A2A731495F1A5BCCCF18468BABE9FEA48F1A371A4C6C67D411C29B5ACBDA6430419924F2990DD004FF9564346A 9
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path class="error" d="M5 12v1h2v-1z" fill="#c00"/><path d="M5.469.012c-.49 0-.796.215-1.032.455C 4.202.707 4 1.023 4 1.497V2H2v14h5v-2H4V4h2V2.012h4V4h2v3h2V2h-2v-.395l-.002-.027a1.622 1.622 0 00-.416-1.014c-.236-.278-.62-.584-1.2-.552z" style="line- height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature- settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mi xed;white-space:normal;shape-padding:0;isolation:auto;mix-blend-mode:normal;solid-color:#000;solid-opacity:1;marker:none" color="#bebebe" font-weight="400" font- family="sans-serif" overflow="visible" fill="#2e3436"/><path class="warning" d="M8.875 8A.863.863 0 008 8.875v6.25c0 .492.383.875.875.875h6.25a.863.863 0 00.875- .875v-6.25A.863.863 0 0015.1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\go-first-rtl.png

Process:	C:\Users\user\Desktop\xKBLVUHoY6.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	489
Entropy (8bit):	7.398446007013356
Encrypted:	false
SSDEEP:	12:6v/7Crv9JvDU9+7g+9reUl62vs3FsMjNwAAb88CGFwleELoyrIZLU4:JhY9r+9yr73FsMjqJw8/FwlP04IZLR
MD5:	4A3BBCDA1BE7D1AFEBECAD7904875C44
SHA1:	99273960EF8EFF8CCD701EC42963CAAFB7F87E4D

SHA-256:	B152B10AA3CA6BA1927C946E91FFF1A2FDFD9212D999EC93544F202089A67B48
SHA-512:	7D63ACC041656E77C263FA69D244E9B0DDD499192A3F7CD64F0BE3A8CE0F8A17C1703FA94F0B3D415058893AE9A5DAABA5D9664D3DFE15165FD50A2CB186D 66
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx...E..P.E{#.H/ 8l.6333.....#..,.C..?f.A.k?....X..fU..{..^....f.F....UD.q.....{.RQ...p...(r.....~T.....Z.....&IP._.~.dW .GN.9QS*.&K..ppy.d.`f. ...E.....A.+..?)...}Gr.....6.8....I.X._..Y.....P...{..dj.I...3T..y..Ll...._.h..w..Z*..W....9..b..z.)..OZ~..-.J....h<L..>A .]..3...7..j...$..Q..#.x....x....k.'.5..5....N*@v.6...gO@U....!....v.P..K... h..r.2<~..|.o.h.,.v..~....@c.^..w.j..o4..#....n.E..2..`....B.,\.Qo....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.819560838319919
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:	xKBLVUHoY6.exe
File size:	314680
MD5:	6e0bf5d5220fbe4f7245653a259c7dad
SHA1:	f077644ac1eb17aa811f4805e1f5f546b4f6166f
SHA256:	2914eb3edbf9dadb98429173fb1c1b5954742b10e49b1f804024e6448028f73e
SHA512:	23c7a8aac36721080945d99eba09e0eeb29f20ac154ddbeb5b7584c9cb009189a51a7fe1b4effcb2f5dec5ee14faea9a429ca52c4f77d02add3e58871b252ad8
SSDEEP:	6144:nNeZ93O+c5v/vFGdRAiH+uZANZ8dZ4oacNtULM:nN37tyRApQ3dZ4DQZ
TLSH:	B7647D6226A6DC13E38457749165E73D8AA6FE861871C2332BF1ED9BB508F317C1C3A1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	e2aab6e6b696a6d2

Static PE Info

General

Entrypoint:	0x4034f7
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:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Inexcitable Spawners ", O=Tingibility, L=Hatzenport, S=Rheinland-Pfalz, 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	• 10/24/2021 11:57:56 PM 10/23/2024 11:57:56 PM
Subject Chain	• CN="Inexcitable Spawners ", O=Tingibility, L=Hatzenport, S=Rheinland-Pfalz, C=DE
Version:	3
Thumbprint MD5:	D2B602699036F0C874A4C03B936AC7EF
Thumbprint SHA-1:	6EE012522EF3D0CADB102A8C014FDEE562F62E70
Thumbprint SHA-256:	ADCEA7C19DB10BA76E9CA9342B4AFB6B541167D4F98E6A1795B068A01F32138A
Serial:	56DD4BCCB18528A2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FE5D913703Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FE5D913700Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx

Instruction
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	0x50000	0x31a50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x4af68	0x1dd0	.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	0x2b0	.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	0x6515	0x6600	False	0.6615349264705882	data	6.439707948554623	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.145774564074664	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.4993489583333333	data	4.013698650446401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x25000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x50000	0x31a50	0x31c00	False	0.47981607255025127	data	6.055190439227351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x50340	0x10a00	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x60d40	0x9600	data	English	United States
RT_ICON	0x6a340	0x8e00	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x73140	0x5600	data	English	United States
RT_ICON	0x78740	0x4400	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 252, next used block 1056964608	English	United States
RT_ICON	0x7cb40	0x2600	data	English	United States
RT_ICON	0x7f140	0x1200	data	English	United States
RT_ICON	0x80340	0xa00	data	English	United States
RT_ICON	0x80d40	0x600	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x81340	0x100	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x81440	0x11c	data	English	United States
RT_DIALOG	0x81560	0xc4	data	English	United States
RT_DIALOG	0x81628	0x60	data	English	United States
RT_GROUP_ICON	0x81688	0x84	data	English	United States
RT_MANIFEST	0x81710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

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: xKBLVUHoY6.exe PID: **1252**, Parent PID: **5192**

General

Target ID:	0
Start time:	13:05:10
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\xKBLVUHoY6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xKBLVUHoY6.exe"
Imagebase:	0x400000
File size:	314680 bytes
MD5 hash:	6E0BF5D5220FBE4F7245653A259C7DAD
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: 00000000.00000002.753579119.00000000031B0000.00000040.00001000.00020000.00000000.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	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nswD9D0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	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	405AC1	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	405AC1	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	405AC1	CreateDirectoryW
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	405AC1	CreateDirectoryW
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	1	405AC1	CreateDirectoryW
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	1	405AC1	CreateDirectoryW
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	1	405AC1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Lansat	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Lansat\Carinas	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Lansat\Carinas\Motorbaneanlgs144	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	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	2	405AC1	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	2	405AC1	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	2	405AC1	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	2	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\Modregnings.Xen	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\battery-caution-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\go-first-rtl.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nskE115.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	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	405AC1	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	405AC1	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	405AC1	CreateDirectoryW
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	405AC1	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	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nskE115.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	405A81	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nskE115.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nswD9D0.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nskE115.tmp	success or wait	1	405C42	DeleteFileW

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\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\Modregnings.Xen	0	22343	31 67 fd fd 25 fd 79 7f fd fd fd 4a 65 fd 55 50 fd da fd fd fd fd fd 28 fd 48 11 fd 4f fd fd 36 6f fd fd 6a 29 fd fd 2a 70 04 fd fd 18 fd 85 38 fd 05 46 09 fd 43 fd fd 32 fd 55 fd 5c fd 53 fd fd fd 5b 6a 75 36 0d 03 1e 75 fd fd 68 3c fd fd fd 6f fd 42 fd 39 31 fd fd fd fd 3b fd fd fd 08 61 35 fd 77 10 fd fd 71 28 fd 6f 30 1c 79 22 78 fd fd 02 26 1f fd fd fd 07 fd fd 28 fd fd fd 59 1c 24 0b 44 70 7e 9a fd fd fd 78 fd fd 4c fd 3c fd 77 1a fd 34 1a fd 65 fd 68 61 65 fd 0b fd fd fd 52 fd 7f fd 65 fd 5b 78 57 fd 32 6d 3c fd 1c fd fd fd 02 fd 41 28 fd fd 44 64 74 6d fd fd fd fd 6a 0c 5d 22 25 fd 77 79 fd fd fd 01 22 41 fd 55 fd 49 1d 60 2e 10 03 77 ab fd 47 75 fd fd 5e 3d 71 3a fd fd fd 09 fd 14 fd 6d fd fd 74 20 fd 10 fd 7a	1%yJeUP(HO6oj)*p8FC2U\S[ju6uh<oB91;awq(o0y"x&(Y$Dp~xL<w4ehaeRexW2m<A(Ddtmj]"%wy"AUI`.wGu^=q:mt z	success or wait	4	4060C3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\battery-caution-symbolic.svg	0	1219	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 20 64 3d 22 4d 35 20 31 32 76 31 68 32 76 2d 31 7a 22 20 66 69 6c 6c 3d 22 23 63 30 30 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 35 2e 34 36 39 2e 30 31 32 63 2d 2e 34 39 20 30 2d 2e 37 39 36 2e 32 31 35 2d 31 2e 30 33 32 2e 34 35 35 43 34 2e 32 30 32 2e 37 30 37 20 34 20 31 2e 30 32 33 20 34 20 31 2e 34 39 37 56 32 48 32 76 31 34 68 35 76 2d 32 48 34 56 34 68 32 56 32 2e 30 31 32 68 34 56 34 68 32 76 33 68 32 56 32 68 2d 32 76 2d 2e 33 39 35 6c 2d 2e 30 30 32 2d 2e 30 32 37 61 31 2e 36 32 32 20 31 2e 36 32 32 20 30	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path class="error" d="M5 12v1h2v-1z" fill="#c00"/><path d="M5.469.012c-.49 0-.796.215-1.032.455C4.202.707 4 1.023 4 1.497V2H2v14h5v-2H4V4h2V2.012h4V4h2v3h2V2h-2v-.395l-.002-.027a1.622 1.622 0	success or wait	1	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Lagerhals\Territorially\Tygnings\systemless\go-first-rtl.png	0	489	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 01 fd 49 44 41 54 78 01 fd fd 45 fd fd 50 10 45 7b 23 fd 48 2f 20 38 6c fd 36 33 33 33 fd 15 fd 44 fd fd 23 fd fd 2c 1f 43 fd fd 3f 66 fd 41 fd 6b 3f 7b fd 15 00 58 11 04 66 55 fd fd 7b fd fd 5e 11 04 fd 00 66 fd 46 fd 19 1f fd 55 44 fd 71 fd 7f 1a fd 12 7b fd 52 51 fd cf fd 70 fd 29 fd 28 72 fd fd 04 fd fd 7e 54 fd 03 fd fd fd fd fd 5b fd fd fd 5a fd fd fd ff 26 49 50 00 5f fd 7e 06 64 57 20 fd 47 4e fd 39 51 53 2a 1f 26 4b fd 09 70 70 79 fd 64 fd 60 66 50 fd fd 63 45 fd fd fd 1b fd 41 fd 2b fd 1f 3f 29 fd 14 fd 7d 47 72 fd fd fd 1a d6 36 fd 38 fd 15 fd 00 49 05 58 fd 5f fd fd 59 0a fd fd fd 0b 17 fd 50 01 fd fd 7b fd fd	PNGIHDRaIDATxEPE{#H/ 8l6333#,C?fAk?XfU{^fFUDq{RQp(r~TZ&IP_~dW GN9QS*&Kppyd`fEA+?)}Gr68IX_YP{	success or wait	1	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\nskE115.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 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 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 19 fd 4f 61 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 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\xKBLVUHoY6.exe	unknown	512	success or wait	469	406094	ReadFile
C:\Users\user\Desktop\xKBLVUHoY6.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\xKBLVUHoY6.exe	unknown	4	success or wait	9	406094	ReadFile
C:\Users\user\Desktop\xKBLVUHoY6.exe	unknown	4	success or wait	2	406094	ReadFile

Disassembly

No disassembly