ID: 679245
Sample Name:
xKBLVUHoY6.exe
Cookbook: default.jbs
Time: 14:04:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

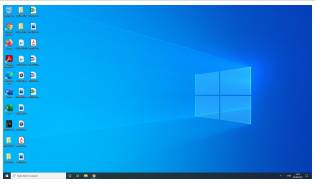
Windows Analysis Report

xKBLVUHoY6.exe

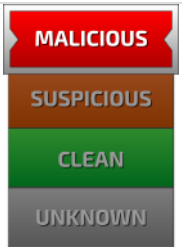
Overview

General Information

Sample Name:	xKBLVUHoY6.exe
Analysis ID:	679245
MD5:	6e0bf5d5220fbe4.
SHA1:	f077644ac1eb17..
SHA256:	2914eb3edbf9da..
Infos:	



Detection



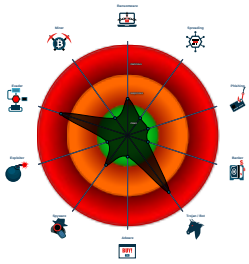
GuLoader

Score:	88
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
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Tries to connect to HTTP servers, b…

Classification



Process Tree

- **System is w10x64native**
- xKBLVUHoY6.exe (PID: 8532 cmdline: "C:\Users\user\Desktop\xKBLVUHoY6.exe" MD5: 6E0BF5D5220FBE4F7245653A259C7DAD)
  - CasPol.exe (PID: 8740 cmdline: "C:\Users\user\Desktop\xKBLVUHoY6.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 8764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1475620205.0000000003360000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000003.00000000.817511706.0000000001230000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000003.00000002.5715131175.0000000001230000.00000040.00000400.00020000.00000000.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 Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging

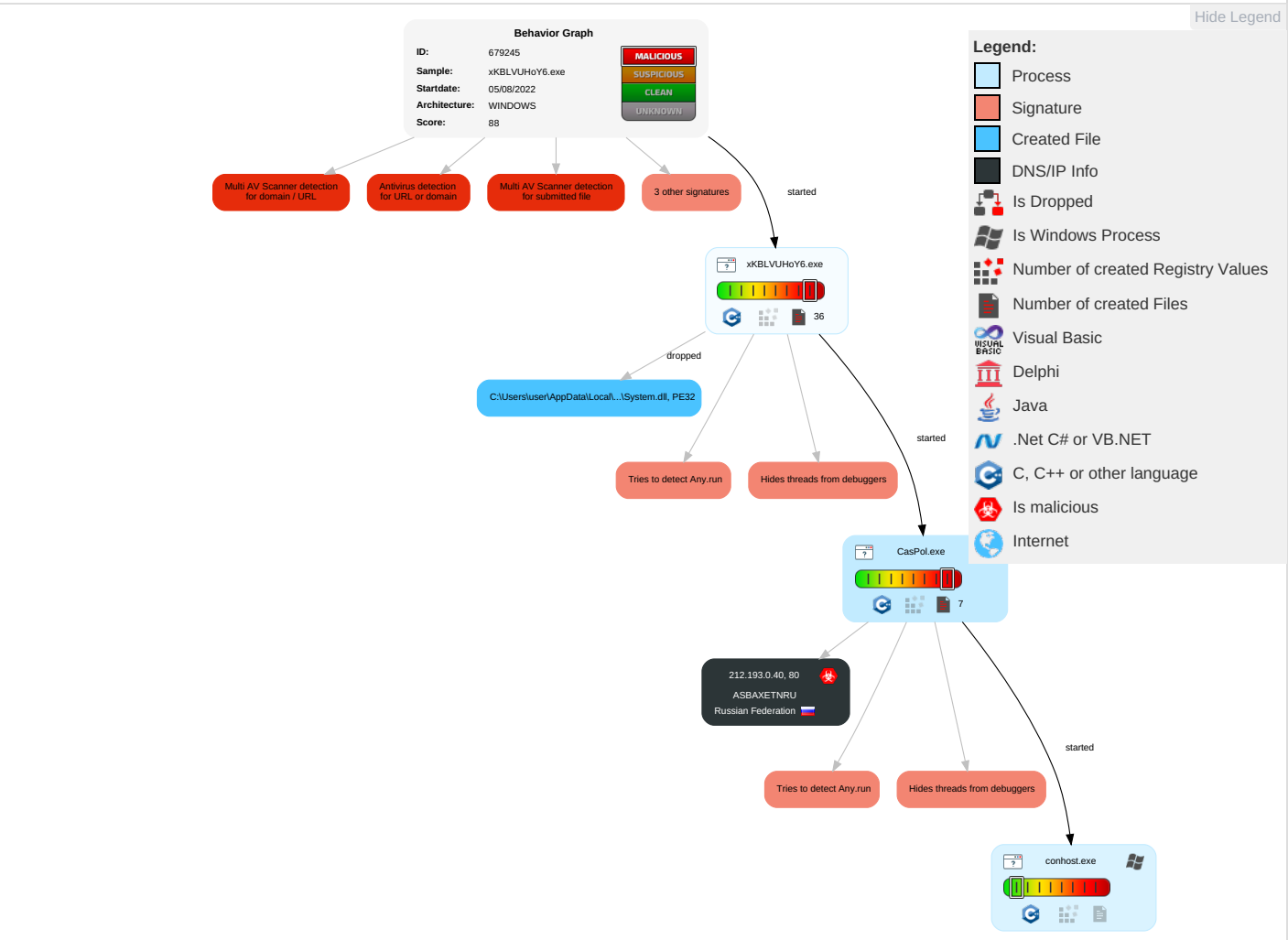
Hides threads from debuggers

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 DLL Side-Loading	1 Access Token Manipulation	1 1 Masquerading	OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	2 1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Virtualization/Sandbox Evasion	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)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	2 File and Directory 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

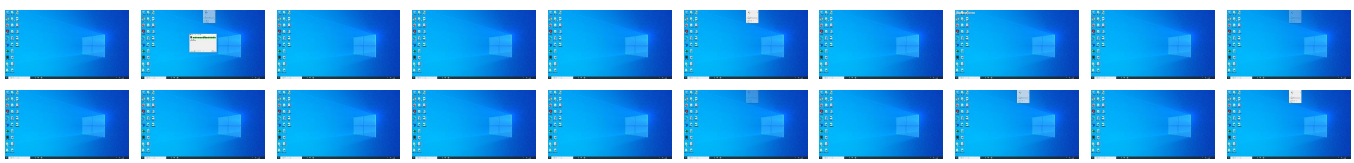
Behavior Graph

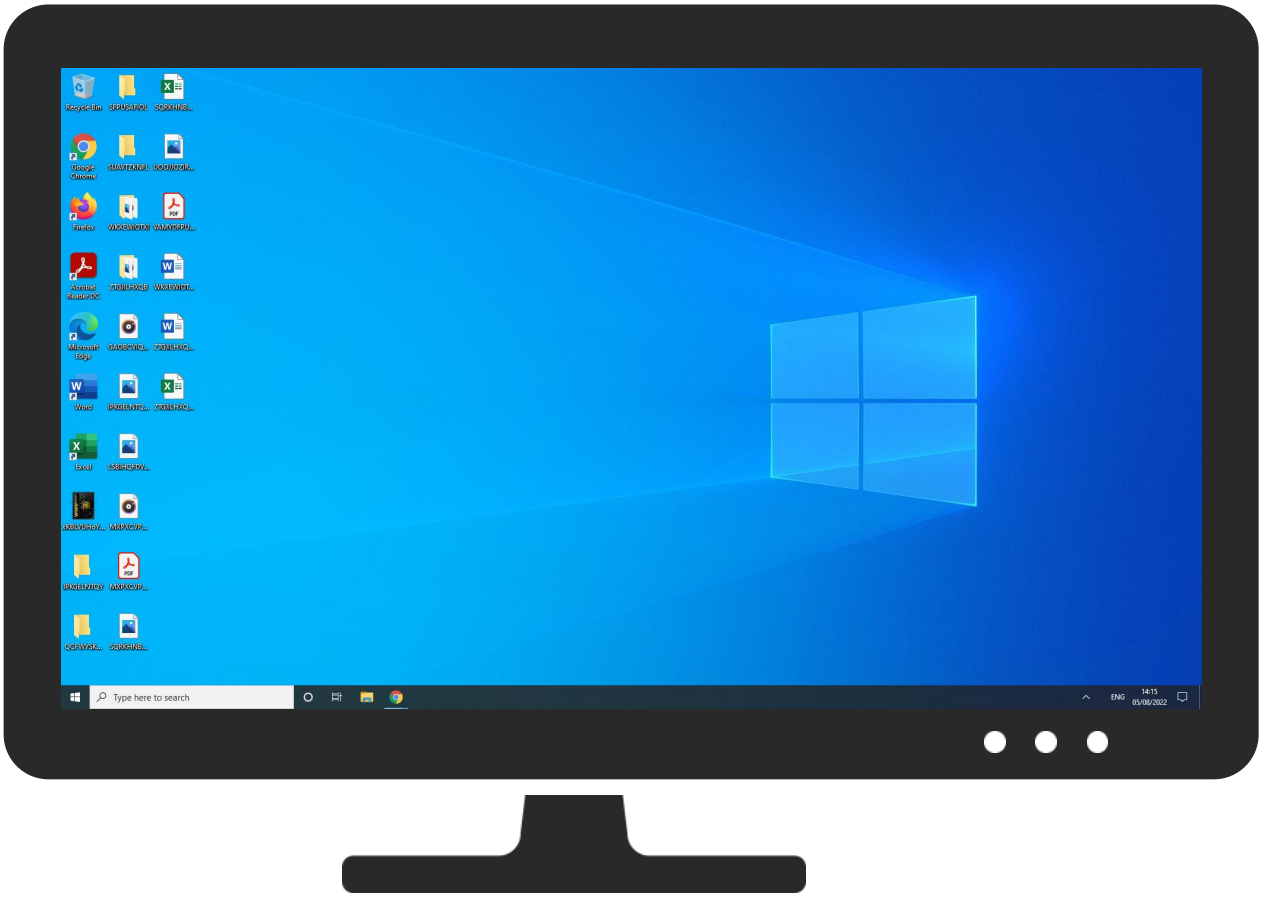


Screenshots

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\nsx50C8.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsx50C8.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.binn	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.bin~	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.bin	16%	Virustotal		Browse
http://212.193.0.40/redi_oXifXcNSpB69.bin	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.binsvY	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.bing	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.binH	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.binoe	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.binZ	100%	Avira URL Cloud	malware	
http://212.193.0.40/redi_oXifXcNSpB69.binalm	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://212.193.0.40/redi_oXifXcNSpB69.binn	CasPol.exe, 00000003.00000002.5715874012.00000000014D7000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000002.5718024276.0000000001541000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.bin~	CasPol.exe, 00000003.00000002.5718024276.0000000001541000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.binsvY	CasPol.exe, 00000003.00000002.5717397048.0000000001520000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://nsis.sf.net/NSIS_ErrorError	xKBLVUHoY6.exe	false		high
http://212.193.0.40/redi_oXifXcNSpB69.bing	CasPol.exe, 00000003.00000002.5715874012.00000000014D7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.binH	CasPol.exe, 00000003.00000002.5718024276.0000000001541000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.binoe	CasPol.exe, 00000003.00000002.5715874012.00000000014D7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.binZ	CasPol.exe, 00000003.00000002.5718024276.0000000001541000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://212.193.0.40/redi_oXifXcNSpB69.binalm	CasPol.exe, 00000003.00000002.5717397048.0000000001520000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.0.40	unknown	Russian Federation		49392	ASBAXETNRU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679245
Start date and time: 05/08/202214:04:09	2022-08-05 14:04:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xKBLVUHoY6.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	34
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:	mal88.troj.evad.winEXE@4/4@0/1
EGA Information:	• Successful, ratio: 50%

HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.6%) • Quality average: 87.5% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.5.88, 20.93.58.141, 20.54.122.82
- Excluded domains from analysis (whitelisted): evoke-windowsservices-tas-msedge-net.e-0009.e-msedge.net, wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, e-0009.e-msedge.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, ris.api.iris.microsoft.com, wd-prod-cp-eu-north-1-fe.northeurope.cloudapp.azure.com, wdcpalt.microsoft.com, login.live.com, evoke-windowsservices-tas.msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com
- Execution Graph export aborted for target CasPol.exe, PID 8740 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:07:08	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\nsx50C8.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: 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:	0D98927E56B9EF0C16EBB1BD075E3B3489CBD7AB3D9074B798D18969AEC044DE91663F607D4EB24F9B9789F04BA683BC779ECD6F94D75E09A354801AF4E30ED
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/alXuprPQ5VIbIrGDRt:ojWCRNtAecFZwDT/AJsD7
MD5:	DE8960A1E15CF658A3FE4A2CAFDAA0D1
SHA1:	7EC7A95E4BC7BA19B3EC19366E87038C3902B430
SHA-256:	DF5925D3EC8C8EDD53FCEC6D7249888D9909B3D245E056028FD668DB4E23CB9B
SHA-512:	91D29A34227DD0DD672519999D32A68F8EB61A2A731495F1A5BCCCF18468BABE9FEA48F1A371A4C6C67D411C29B5ACBDA6430419924F2990DD004FF9564346A9
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-.796.215-1.032.455C4.202.707 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:mixed;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	• 24/10/2021 22:57:56 23/10/2024 22:57:56
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 00007EFF1033089Ah
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 00007EFF1033086Ah
and word ptr [ebp-00000132h], 0000h

Instruction
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
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

Name	RVA	Size	Type	Language	Country
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
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

TCP Packets

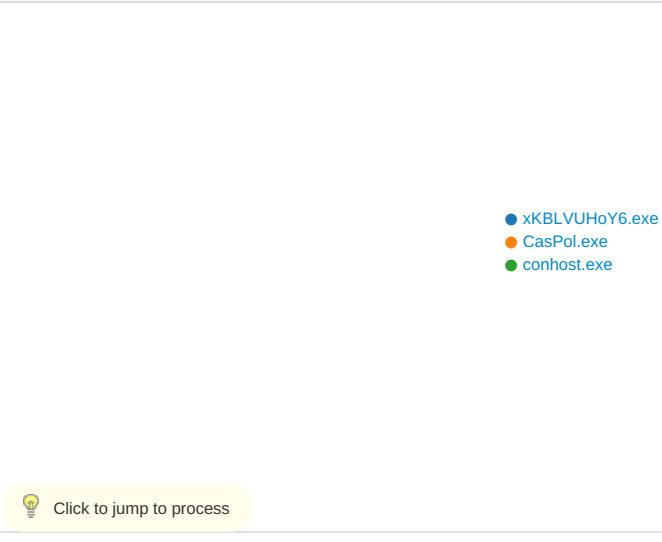
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:07:32.152435064 CEST	49727	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:33.159872055 CEST	49727	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:35.159363985 CEST	49727	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:39.174120903 CEST	49727	80	192.168.11.20	212.193.0.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:07:47.188000917 CEST	49727	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:54.218904018 CEST	49740	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:55.233010054 CEST	49740	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:07:57.232618093 CEST	49740	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:01.247330904 CEST	49740	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:09.261444092 CEST	49740	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:16.292191982 CEST	49760	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:17.306272030 CEST	49760	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:19.321695089 CEST	49760	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:23.336309910 CEST	49760	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:31.350100040 CEST	49760	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:38.382898092 CEST	49762	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:39.379566908 CEST	49762	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:41.394762993 CEST	49762	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:45.409439087 CEST	49762	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:08:53.423372030 CEST	49762	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:00.454098940 CEST	49765	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:01.468534946 CEST	49765	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:03.483611107 CEST	49765	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:07.498469114 CEST	49765	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:15.512239933 CEST	49765	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:22.543256998 CEST	49768	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:23.557393074 CEST	49768	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:25.572673082 CEST	49768	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:29.587294102 CEST	49768	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:37.601310968 CEST	49768	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:44.633246899 CEST	49770	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:45.646311998 CEST	49770	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:47.661587000 CEST	49770	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:51.676271915 CEST	49770	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:09:59.690076113 CEST	49770	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:06.721107006 CEST	49771	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:07.735119104 CEST	49771	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:09.750307083 CEST	49771	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:13.765036106 CEST	49771	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:21.778992891 CEST	49771	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:28.810158968 CEST	49772	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:29.824213982 CEST	49772	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:31.839329958 CEST	49772	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:35.853876114 CEST	49772	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:43.867840052 CEST	49772	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:50.899960995 CEST	49773	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:51.912887096 CEST	49773	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:53.928108931 CEST	49773	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:10:57.942816019 CEST	49773	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:05.956773043 CEST	49773	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:12.987570047 CEST	49775	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:14.001897097 CEST	49775	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:16.017164946 CEST	49775	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:20.031699896 CEST	49775	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:28.045557976 CEST	49775	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:35.076654911 CEST	49776	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:36.090778112 CEST	49776	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:38.106137991 CEST	49776	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:42.120623112 CEST	49776	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:50.134536028 CEST	49776	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:57.166372061 CEST	49777	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:11:58.164046049 CEST	49777	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:00.179128885 CEST	49777	80	192.168.11.20	212.193.0.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:12:04.194000959 CEST	49777	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:12.207859039 CEST	49777	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:19.240605116 CEST	49778	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:20.252856970 CEST	49778	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:22.268033028 CEST	49778	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:26.282752991 CEST	49778	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:34.296644926 CEST	49778	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:41.328217983 CEST	49779	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:42.341773033 CEST	49779	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:44.357043982 CEST	49779	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:48.371671915 CEST	49779	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:12:56.385699987 CEST	49779	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:03.417860031 CEST	49780	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:04.430660009 CEST	49780	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:06.445909023 CEST	49780	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:10.460551977 CEST	49780	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:18.474405050 CEST	49780	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:25.508054972 CEST	49788	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:26.519665956 CEST	49788	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:28.534674883 CEST	49788	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:32.549573898 CEST	49788	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:40.563359022 CEST	49788	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:47.595875025 CEST	49789	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:48.608536005 CEST	49789	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:50.623610020 CEST	49789	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:13:54.638317108 CEST	49789	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:02.652225971 CEST	49789	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:09.687903881 CEST	49796	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:10.697413921 CEST	49796	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:12.712574959 CEST	49796	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:16.727325916 CEST	49796	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:24.741096020 CEST	49796	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:31.774460077 CEST	49797	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:32.786245108 CEST	49797	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:34.801412106 CEST	49797	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:38.816270113 CEST	49797	80	192.168.11.20	212.193.0.40
Aug 5, 2022 14:14:46.830014944 CEST	49797	80	192.168.11.20	212.193.0.40

Statistics

Behavior



System Behavior

Analysis Process: xKBLVUHoY6.exe PID: 8532, Parent PID: 7312

General

Target ID:	0
Start time:	14:07:07
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: 00000000.00000002.1475620205.0000000003360000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: 8740, Parent PID: 8532

General

Target ID:	3
Start time:	14:07:21
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xKBLVUHoY6.exe"
Imagebase:	0xe50000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 00000003.00000000.817511706.0000000001230000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000003.00000002.5715131175.0000000001230000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **8764**, Parent PID: **8740**

General	
Target ID:	4
Start time:	14:07:21
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff750a30000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly