ID: 830512
Sample Name: download.exe
Cookbook: default.jbs
Time: 13:11:48
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

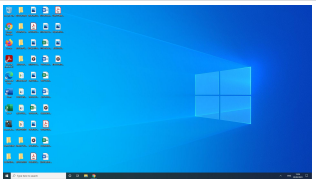
Windows Analysis Report

download.exe

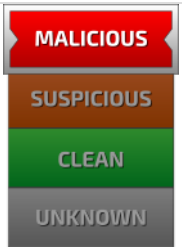
Overview

General Information

Sample Name:	download.exe
Analysis ID:	830512
MD5:	064fa36da0c2c..
SHA1:	a6623c33cbd8…
SHA256:	6974c5051372…
Infos:	



Detection



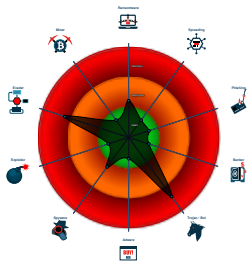
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected GuLoader
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64native**
- download.exe (PID: 8540 cmdline: C:\Users\user\Desktop\download.exe MD5: 064FA36DA0C2CA360B0906CC5BFE67C6)
  - CasPol.exe (PID: 924 cmdline: C:\Users\user\Desktop\download.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 4728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.1798739196.0000000000B02000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000004.00000002.5807012371.00000000025EF000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.1806817167.00000000069EF000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: download.exe PID: 8540	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

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)

HIPS / PFW / Operating System Protection Evasion

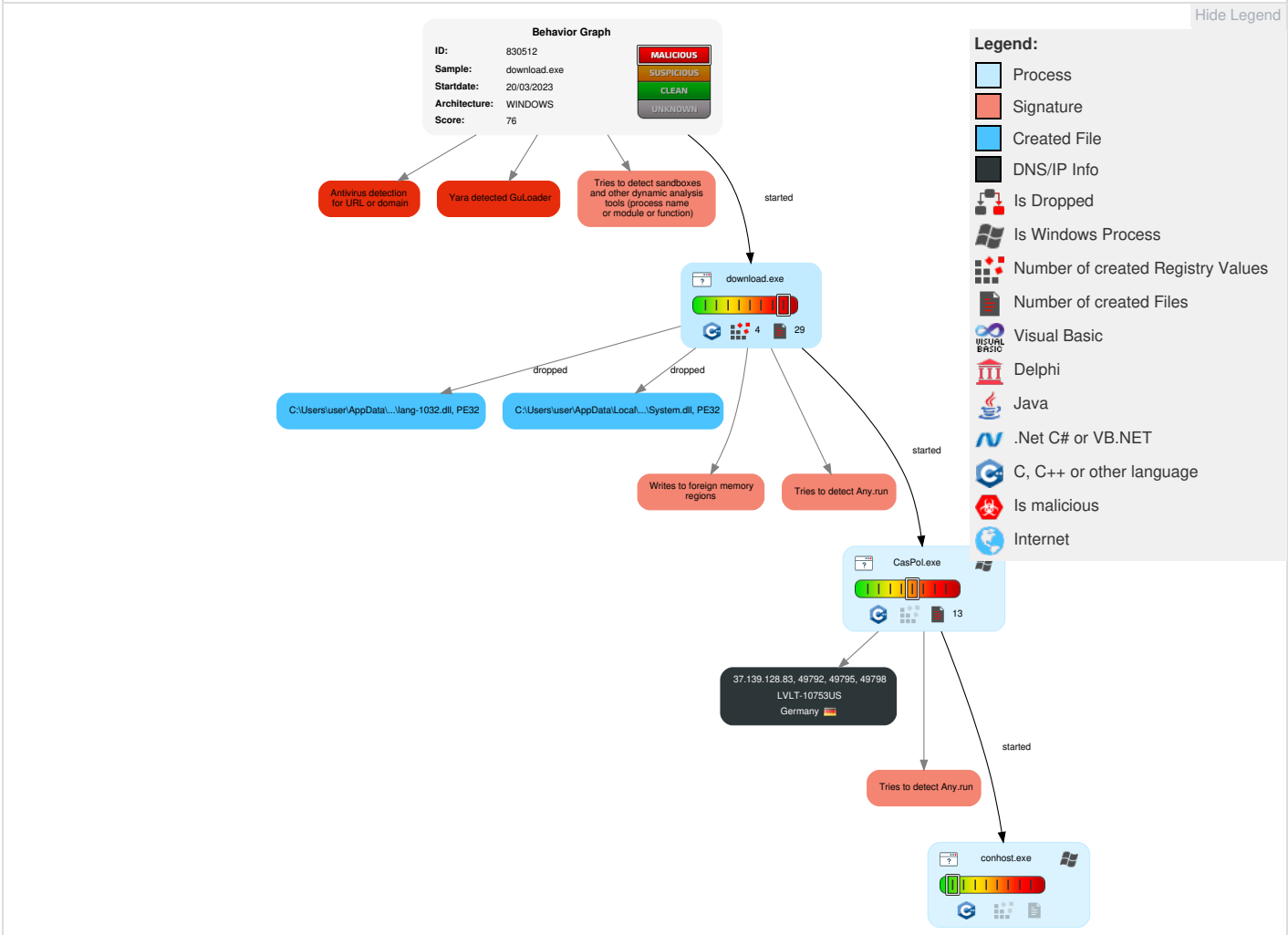
Writes to foreign memory regions

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

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 Masquerading	OS Credential Dumping	2 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 1 Process Injection	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	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	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	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

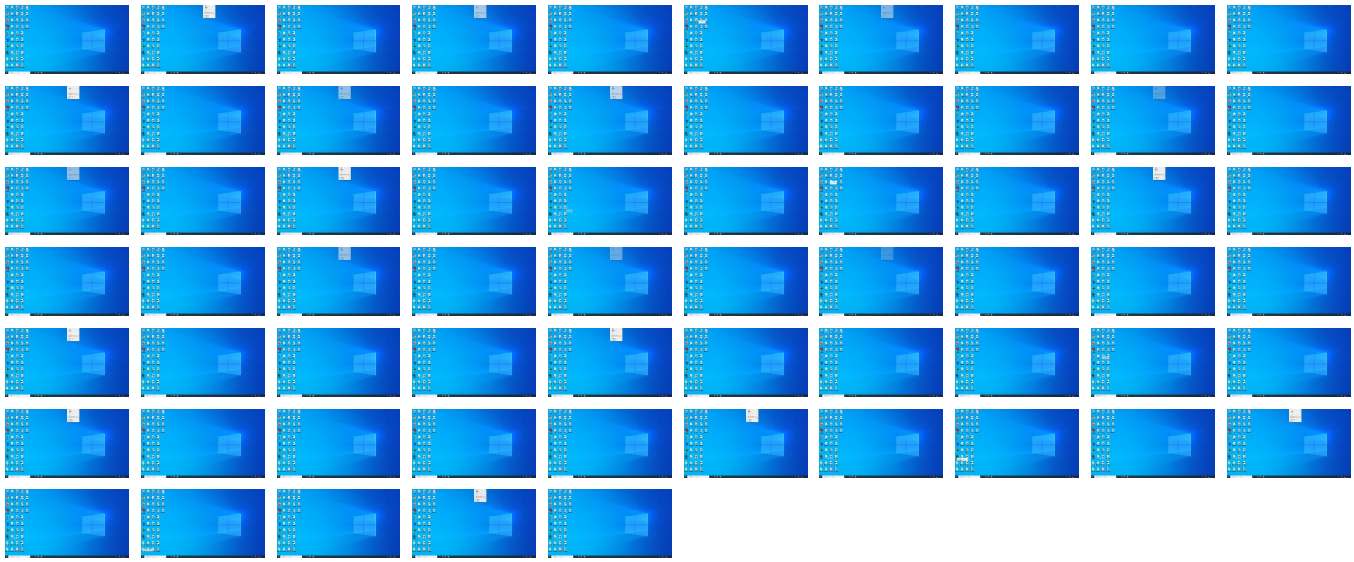
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nse224D.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.download.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
2.0.download.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://37.139.128.83/2-2	100%	Avira URL Cloud	malware	
http://37.139.128.83/2k	100%	Avira URL Cloud	malware	
http://37.139.128.83/2	100%	Avira URL Cloud	malware	
http://37.139.128.83/2Data	100%	Avira URL Cloud	malware	
http://37.139.128.83/2M	100%	Avira URL Cloud	malware	
http://37.139.128.83/2W7	100%	Avira URL Cloud	malware	
http://37.139.128.83/2R2	100%	Avira URL Cloud	malware	
http://37.139.128.83/2e	100%	Avira URL Cloud	malware	
http://37.139.128.83/l	100%	Avira URL Cloud	malware	
http://www.avast.com0/	0%	Avira URL Cloud	safe	
http://37.139.128.83/2gsLMEM8	100%	Avira URL Cloud	malware	
http://37.139.128.83/2$2	100%	Avira URL Cloud	malware	
http://37.139.128.83/262hk	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

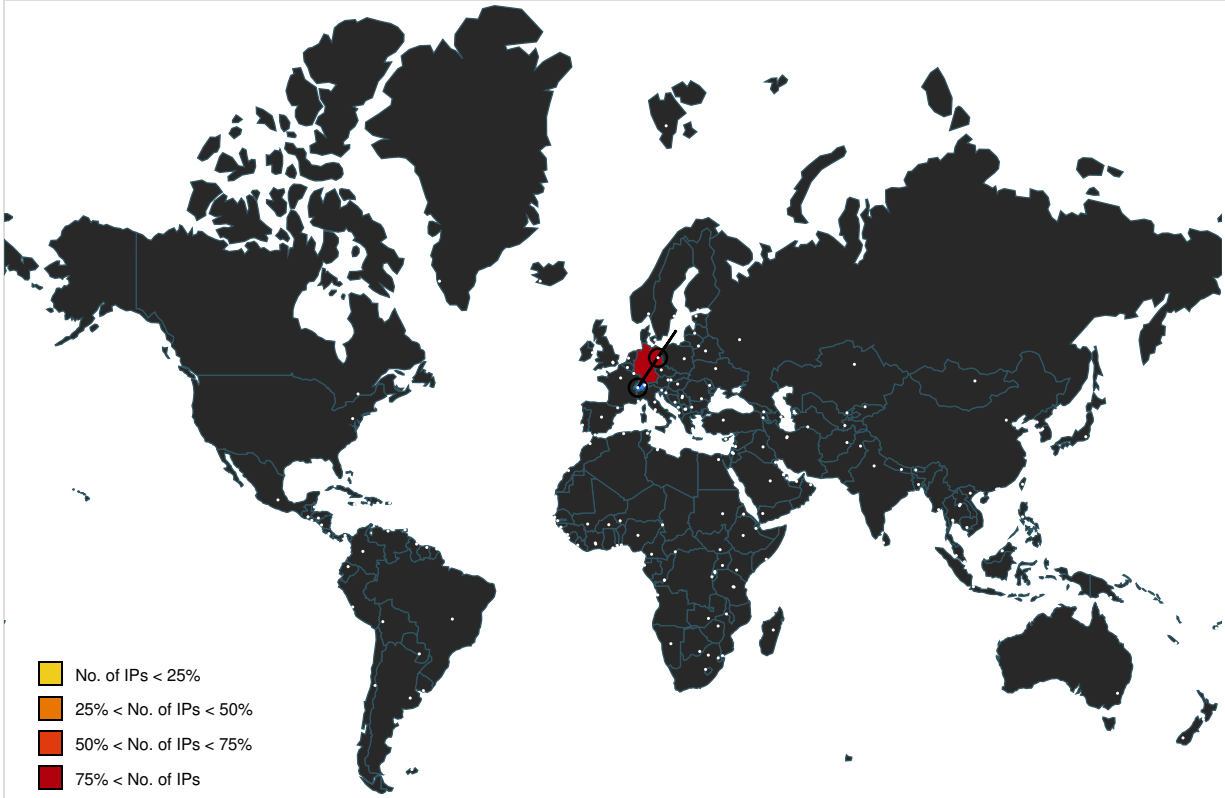
Name	Malicious	Antivirus Detection	Reputation
http://37.139.128.83/2	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://37.139.128.83/2-2	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://nsis.sf.net/NSIS_Error	download.exe	false		high
http://37.139.128.83/2M	CasPol.exe, 00000004.00000002.5897618619.0000000003EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/2Data	CasPol.exe, 00000004.00000002.5897618619.0000000003EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/2k	CasPol.exe, 00000004.00000002.5897618619.0000000003EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/2R2	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://37.139.128.83/2W7	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/2e	CasPol.exe, 00000004.00000002.5897618619.0000000003EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.avast.com0/	lang-1032.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://37.139.128.83/l	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://nsis.sf.net/NSIS_ErrorError	download.exe	false		high
http://37.139.128.83/2gsLMEM8	CasPol.exe, 00000004.00000002.5897618619.0000000003EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/2$2	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://37.139.128.83/262hk	CasPol.exe, 00000004.00000002.5897618619.0000000003F0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.139.128.83	unknown	Germany		10753	LVLT-10753US	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830512
Start date and time:	2023-03-20 13:11:48 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 48s
Hypervisor based Inspection enabled:	false
Report type:	light

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
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	download.exe
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@4/5@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.9%) • Quality average: 88.9% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wdcp.microsoft.com
- Execution Graph export aborted for target CasPol.exe, PID 924 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- 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\nse224D.tmp\System.dll

Process:	C:\Users\user\Desktop\download.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.825582780706362
Encrypted:	false
SSDEEP:	192:yPtkiQJr7V9r3Ftr87NfwXQ6whlgi62V7i77blbTc4DI:N7Vxr8lgLgi3sVc4
MD5:	FBE295E5A1ACFBD0A6271898F885FE6A
SHA1:	D6D205922E61635472EFB13C2BB92C9AC6CB96DA
SHA-256:	A1390A78533C47E55CC364E97AF431117126D04A7FAED49390210EA3E89DD0E1
SHA-512:	2CB596971E504EAF1CE8E3F09719EBFB3F6234CEA5CA7B0D33EC7500832FF4B97EC2BBE15A1FBF7E6A5B02C59DB824092B9562CD8991F4D027FEAB6FD3177E06
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....~.\.....!..... .....(.....0.....`.....@.....2.....0..P.....P.....0..X..... .....text...O..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Afreager.For

Process:	C:\Users\user\Desktop\download.exe
File Type:	data
Category:	dropped
Size (bytes):	310762
Entropy (8bit):	7.153872132508062
Encrypted:	false
SSDEEP:	6144:gjumg/DuSWsGx6RZLOMqkcjpwn2+3VJInGwhTFLI:gjumgbhWsGWZ+kcj2n2OJInJhTS
MD5:	A1C8FEE704DB305175D7A96481B66C73
SHA1:	F26BE75182187BB5AA73C170605CF171D62DC023
SHA-256:	004CC2CA7789AB32D71678F5174DFC0F8EF1BA70A457929037E8CE0E4FD625C2
SHA-512:	4F5865B975DDD54A7770D89A28ADD620C5A675225F8F7974E68A6173B33C6FCA853D98AD1E2B054147B2ACD6C810BF90A252C30034973AB08B9CBACD69E6B95
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Poserne\Bedugget39.Rus

Process:	C:\Users\user\Desktop\download.exe
File Type:	data
Category:	dropped
Size (bytes):	142071
Entropy (8bit):	**7.998708530523099**
Encrypted:	**true**
SSDEEP:	3072:NZcIfJJvbMxWCmEblH1ZC0+UM53+9l1dPg4kh89+08iFRbleoK:5DMxW4fz1e3+9Sg9Z1iFRleoK
MD5:	2CB77C7D9E16C0EF410FA8BC1CC1185A
SHA1:	0FCBA04A0B4B4563D62A073080E173590BEEBEDD

SHA-256:	A0BFB53FAD74C41F699F171902C1D6A0AC33A81963697A3F674234B2FF36203A
SHA-512:	33FDB3488F9BF085D7CDA649984BAE271194ECB64B569B5BDB1D09DE48C5D5407D75CDC2EA1A59E8E199F821CE4DA5F101D0A7CAA44E544E78C8D8507B6BC751
Malicious:	false
Preview:	>2'...JuK.(p@wC..D.5i....C....M%.*..O.0D.]...N.....%...*xu...k).~.Pz..1/....*..}a.....`.a.k.N%Ze..a..o~..=..\...^'...v/.\K...\.....5.....B..{.A..t..vh.....sl}*...Fft>..`....`.>.27(...J.....u{..csucM...a.V.'..a<.N3f.$.....%@h8G..).G.>..M{....o...3..~X...w.AS.X...7.Y...v2..+....!u.... n&..vt..FR#s..w.j.....}...J...sA..w.....L@....+X3dq(.; ...k|....i...G...z~sF`Q}a....[..Q...I.....A..[.?...i.D..e..$d..e..KC....4+J....c..'."><6R.2.0....<R+.}.H0)u49..oK.v._...F).8.e..J..;.!....[.&E...V.....[.%.H....p3..*.....M.!.`,WX..J....an.e..h.u%P...{.....s...Q../.e?..R,..$)..N.^.P..Z\...mj8*D.<3...ke...j...W...9..7D.I?...Zp|.3.....M.s.S.4....ll.].aW.=v..Q...9..?...u...0.N....Sg....~..8....,[./.....8P\....S..k.....\..._...[=.P.....d./gKdP-_.5BU..u2u6x...)..E..`.{..@.....!.....g.j.r.\.6.\.+...vr.b..oE..h.;..I.,...(.....=.d..p./lr)*...bH....gjJ.....:.x...K)xh.C...../....L..~B..Vh..l.zb.V.6qm...p..ER

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll

Process:	C:\Users\user\Desktop\download.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	178696
Entropy (8bit):	4.4006904456537335
Encrypted:	false
SSDEEP:	3072:A8kCKqgt37ZJvMQSOnMIomX6YZVG5dWCR7+nyadqLEzBUyQj2UGBOyj:CvM7yj
MD5:	8AD3A9D8C3DDA9854C13D213D00A8DB8
SHA1:	74283E98F0426DFA7854CEEF9BA43217F39DAB36
SHA-256:	DA07C1D13136E3BAABB9D0598AF99BCB48898BF5DBCA0F0477602BEA957198E9
SHA-512:	C30CA6FA4A62A6383C15AB8B95CD88714AF5C3A63F7FC9C8F767FED18E295B885B765B630831F456D16DB5DA7AA037CA931FCB3F412AB95A8D5E46B1B44497CA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.@...R.@.P...R.Rich..R.....PE..L....\)b.....!.....@..... ..`..... .....rdata..p.....@..@.rsrc...`.... .....@..@.....\)b.....T.....rdata.....T....rdata$zzdbg.... ... ...rsrc$01.....@...s...rsrc$02.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\microphone-sensitivity-low-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\download.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	291
Entropy (8bit):	6.913400639640828
Encrypted:	false
SSDEEP:	6:6v/lhPysSFX/Fd8cy2TY3594VW6yTpm/v4pRw+jGbcnFbp:6v/7yFvn8cGJkv3twD
MD5:	303E1921A67BAE379BC4B36352F391AA
SHA1:	AB361F32C8F1811EC7DB6EB96DAD417753323DB4
SHA-256:	1FC1141E644151384931853426BD36B5293BCAFE380189515850B9CC8FF158D7
SHA-512:	0A355819B8EB530A30710D536CCF6F5AACA7E9050C7CA9F591E31DC8BCBCEFC83EC9EA5B1E3B9356D64A66B42D04A0DD504A97B7AFC6CA35E7CED23A82A74C93
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1N.Q.....V6R.H....w...A.`.5v..`mK.ZH.Z8.l`.l._2y.....k..8....a.il...8.~.I@.Y.Le.'<G.....a....h...W@.q.3..n..(jb.P.`.....X....1..1...!f./..h.~..!..q....3...x.g.7u.{St3.....w./Q..g.....*a.]..T..T.~.?.+2.pM.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.546765550553085
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:	download.exe
File size:	680560
MD5:	064fa36da0c2ca360b0906cc5bfe67c6
SHA1:	a6623c33cbd86bdaee063f897bea1692621494e5

SHA256:	6974c5051372213d0e90147660c4b21bfff238e20c6449acb19f1901bf4729c8
SHA512:	39845a084b66442a1eb114621df67fe6db88e758b4564b79c01eff6a1935dcaba4149f0d3c68e243258b7da5f3ce197a904e226f561a0dfc1377ff22419a6026
SSDEEP:	12288:Z4oLK6+zAX00AF1pOSJe3xbIvli343lKZwIcBRPgYxFz18+t9Z1kU:6PQ00AF1pOSJeBUyqKKrf318U9Z1z
TLSH:	F2E4F15A2B7AC815D065E9F85AE3C50D5C749E14183CABD25BB1283EEBFC2527B0F047
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...../.....s.../.....+.....Rich.....PE..L.....\.....b....9....

File Icon

Icon Hash:	c4ccc6e6e4f6f640

Static PE Info

General

Entrypoint:	0x4031e9
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:	0x5C157F01 [Sat Dec 15 22:24:01 2018 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:	3abe302b6d9a1256e6a915429af4ffd2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=barket, OU="Biselg Halo Uvitinic ", E=Strammende@Kummerfuld.Kur, O=barket, L=Middleton, S=Tennessee, C=US
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	• 24/01/2023 23:36:10 23/01/2026 23:36:10
Subject Chain	• CN=barket, OU="Biselg Halo Uvitinic ", E=Strammende@Kummerfuld.Kur, O=barket, L=Middleton, S=Tennessee, C=US
Version:	3
Thumbprint MD5:	F856691DCF4BB6A788E55B70FE388011
Thumbprint SHA-1:	0C5E3286DBBB50FA720930F437DDBC472FF1EFDF
Thumbprint SHA-256:	7BCC618A115B3494BA1A7F1A5EDFACF31559C85478D2F90A7916E2A476BCF411
Serial:	807C3D2B116DDE7C

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A0h]

Instruction
call dword ptr [0040809Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A2F4Ch], eax
je 00007FBDE865E5C3h
push ebx
call 00007FBDE866169Ah
cmp eax, ebx
je 00007FBDE865E5B9h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007FBDE8661616h
push esi
call dword ptr [00408098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FBDE865E59Dh
push 0000000Ah
call 00007FBDE866166Eh
push 00000008h
call 00007FBDE8661667h
push 00000006h
mov dword ptr [007A2F44h], eax
call 00007FBDE866165Bh
cmp eax, ebx
je 00007FBDE865E5C1h
push 0000001Eh
call eax
test eax, eax
je 00007FBDE865E5B9h
or byte ptr [007A2F4Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [007A3018h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0079E500h
call dword ptr [00408178h]
push 0040A188h

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	0x8430	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c7000	0x37c28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa4d40	0x1530	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x298	.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	0x6068	0x6200	False	0.671875	data	6.450713900012796	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1250	0x1400	False	0.430078125	data	5.041636133183931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x399058	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a4000	0x23000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c7000	0x37c28	0x37e00	False	0.4934109340044743	data	6.083319493650987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3c7460	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x3d7c88	0xd177	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x3e4e00	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x3ee2a8	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x3f3730	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x3f7958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x3f9f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x3fafa8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x3fbe50	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x3fc7d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x3fd080	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x3fd6e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x3fdc50	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x3fe0b8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x3fe3a0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x3fe4c8	0x100	data	English	United States
RT_DIALOG	0x3fe5c8	0x11c	data	English	United States
RT_DIALOG	0x3fe6e8	0xc4	data	English	United States
RT_DIALOG	0x3fe7b0	0x60	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x3fe810	0xd8	data	English	United States
RT_MANIFEST	0x3fe8e8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetCurrentDirectoryA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, CreateThread, GlobalLock, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:16:46.897514105 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:46.916491985 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.916826963 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:46.917243958 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:46.943846941 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.943917990 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.943964958 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.944006920 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.944037914 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:46.944081068 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:46.944143057 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:46.944204092 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:52.480920076 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:52.481168032 CET	49792	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:56.963512897 CET	49792	80	192.168.11.20	37.139.128.83

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:16:56.963851929 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:56.981890917 CET	80	49792	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:56.981976986 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:56.982162952 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:56.982340097 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:57.030054092 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:57.030136108 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:57.030189991 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:57.030237913 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:57.030291080 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:16:57.030379057 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:57.030380011 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:16:57.030443907 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:02.530766964 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:02.531013012 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.039050102 CET	49795	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.039249897 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.057694912 CET	80	49795	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.057790995 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.058085918 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.058161974 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.129527092 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.129926920 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.143343925 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.143439054 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.143497944 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.143510103 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.143595934 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:07.143606901 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.143656015 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:07.143703938 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:12.658093929 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:12.658453941 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.161452055 CET	49798	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.161731958 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.179919958 CET	80	49798	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.179985046 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.180273056 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.180488110 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.208664894 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.208734035 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.208784103 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.208827019 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.208869934 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:17.208889008 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.208889961 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:17.208966970 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:22.709000111 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:22.709415913 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.221820116 CET	49800	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.222153902 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.239955902 CET	80	49800	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.240132093 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.240246058 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.240505934 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.312999010 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.319519997 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.319586039 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.319698095 CET	49801	80	192.168.11.20	37.139.128.83

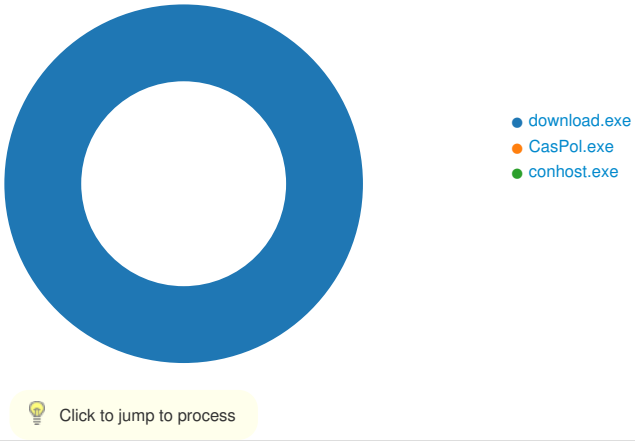
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:17:27.319760084 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.336045980 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.336110115 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.336155891 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:27.336225986 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:27.336298943 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:32.872137070 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:32.872304916 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.344167948 CET	49801	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.344499111 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.362550020 CET	80	49801	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.362641096 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.362831116 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.362966061 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.437429905 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.437498093 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.437544107 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.437587023 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.437632084 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:37.437645912 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.437716961 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.437817097 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:37.437818050 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:42.944545031 CET	80	49804	37.139.128.83	192.168.11.20
Mar 20, 2023 13:17:42.945274115 CET	49804	80	192.168.11.20	37.139.128.83
Mar 20, 2023 13:17:47.451338053 CET	49804	80	192.168.11.20	37.139.128.83

HTTP Request Dependency Graph

- 37.139.128.83

Statistics

Behavior



System Behavior

Analysis Process: download.exe PID: 8540, Parent PID: 4476

General

Target ID:	2
Start time:	13:15:59
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\download.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\download.exe
Imagebase:	0x400000
File size:	680560 bytes
MD5 hash:	064FA36DA0C2CA360B0906CC5BFE67C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000002.00000002.1798739196.0000000000B02000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.1806817167.00000000069EF000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: 924, Parent PID: 8540

General

Target ID:	4
Start time:	13:16:37
Start date:	20/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\download.exe
Imagebase:	0x10000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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: 00000004.00000002.5807012371.00000000025EF000.00000040.00000400.00020000.00000000.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: 4728, Parent PID: 924

General

Target ID:	5
Start time:	13:16:37
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d7f70000
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