ID: 830512
Sample Name: download.exe
Cookbook: default.jbs
Time: 13:00:18
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

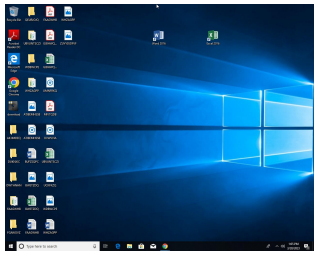
Windows Analysis Report

download.exe

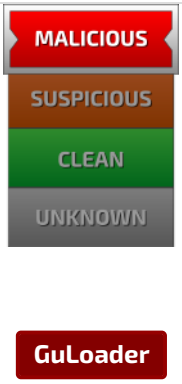
Overview

General Information

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



Detection



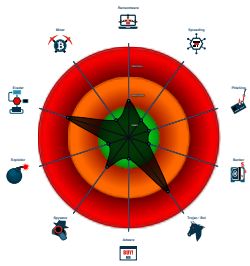
GuLoader

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- PE file does not import any functions
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Found dropped PE file which has no…
- PE file contains executable resourc…

Classification



Process Tree

- **System is w10x64**
- download.exe (PID: 5412 cmdline: C:\Users\user\Desktop\download.exe MD5: 064FA36DA0C2CA360B0906CC5BFE67C6)
- **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-usering/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
00000000.00000002.779236025.000000000693F000.00000040.00001000.00020000.00000000.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

Data Obfuscation

Yara detected GuLoader

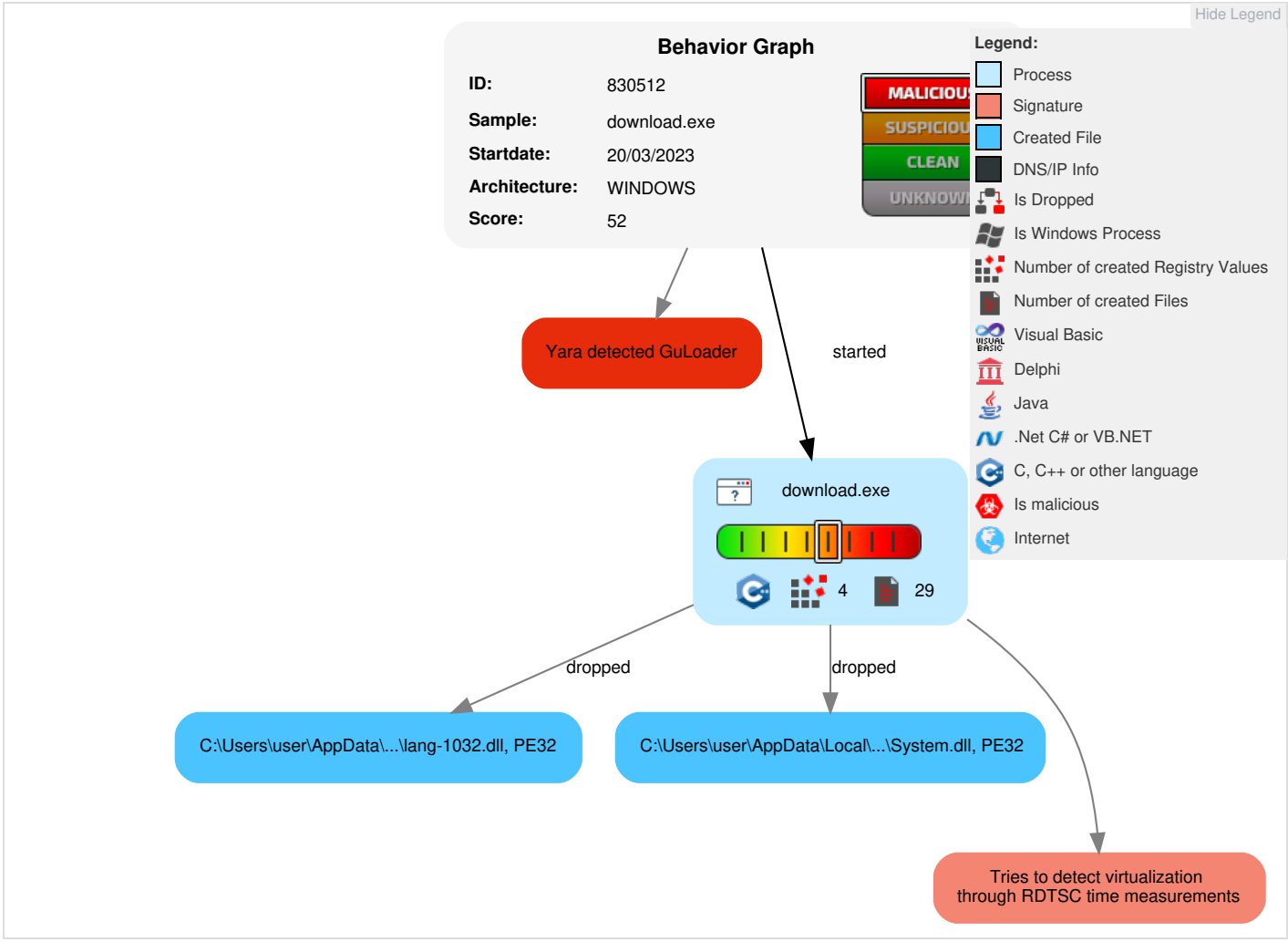
Malware Analysis System Evasion

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	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	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	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll	0%	Virustotal		Browse

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.avast.com0/	0%	URL Reputation	safe	
http://www.avast.com0/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.avast.com0/	lang-1032.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	download.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	download.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830512
Start date and time:	2023-03-20 13:00:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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:	mal52.troj.evad.winEXE@1/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.8% (good quality ratio 62.4%) • Quality average: 88.8% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsp8E94.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% • Antivirus: Virustotal, Detection: 0%, Browse
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:NZclfJJvbMxWCmEblH1ZC0+UM53+9l1dPg4kh89+08iFRbleoK:5DMxW4fz1e3+9Sg9Z1iFRleoK
MD5:	2CB77C7D9E16C0EF410FA8BC1CC1185A
SHA1:	0FCBA04A0B4B4563D62A073080E173590BEEBEDD
SHA-256:	A0BFB53FAD74C41F699F171902C1D6A0AC33A81963697A3F674234B2FF36203A
SHA-512:	33FDB3488F9BF085D7CDA649984BAE271194ECB64B569B5BDB1D09DE48C5D5407D75CDC2EA1A59E8E199F821CE4DA5F101D0A7CAA44E544E78C8D8507B6BC751
Malicious:	false
Reputation:	low
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.$.....%@h8G..).G.>..M{....o...3..~X...w.AS.X...7.Y...v2..+....!u.... n&..vt..FR#s..w.j.....}...J...sA..w.....L@....+X3dq(.; ...k|....i...G... ..z~sF`Q}a....[..Q...l.....A..[.?...i.D..e..$d..e..KC....4+J....c...'."><R.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..I.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% • Antivirus: Virustotal, Detection: 0%, Browse

Reputation:	low
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$zzzdbg.... ... ...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
Reputation:	low
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.~.l@.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+zAX00AF1pOSJe3xblvli343lKZwlcBRPgYxFz18+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	• 1/24/2023 3:36:10 PM 1/23/2026 3:36:10 PM
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]
call dword ptr [0040809Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A2F4Ch], eax
je 00007F4174AB06C3h
push ebx
call 00007F4174AB379Ah
cmp eax, ebx
je 00007F4174AB06B9h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007F4174AB3716h
push esi
call dword ptr [00408098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F4174AB069Dh
push 0000000Ah
call 00007F4174AB376Eh
push 00000008h

Instruction
call 00007F4174AB3767h
push 00000006h
mov dword ptr [007A2F44h], eax
call 00007F4174AB375Bh
cmp eax, ebx
je 00007F4174AB06C1h
push 0000001Eh
call eax
test eax, eax
je 00007F4174AB06B9h
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	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
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

DLL	Import
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

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: download.exe PID: 5412, Parent PID: 3452

General

Target ID:	0
Start time:	13:01:17
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_2, Description: Yara detected GuLoader, Source: 00000000.00000002.779236025.000000000693F000.00000040.00001000.00020000.00000000.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	4055F3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz8D99.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B79	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405B79	GetTempFileNameA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsp8E94.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	4055B3	CreateDirectoryA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
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	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4055F3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Afreager.For	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B42	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B42	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Poserne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4055F3	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Poserne\Bedugget39.Rus	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B42	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\microphone-sensitivity-low-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B42	CreateFileA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405B42	CreateFileA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	2	405B42	CreateFileA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	17896	405B42	CreateFileA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	6	405B42	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz8D99.tmp	success or wait	1	403460	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp	success or wait	1	405774	DeleteFileA

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\Heize\Afreager.For	0	32768	fd fd		success or wait	10	405BD7	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\lang-1032.dll	0	32768	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 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 0c 5c 29 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL\)b!	success or wait	6	405BD7	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Poserne\Bedugget39.Rus	0	32768	3e 32 27 1b 97 fd 4a 75 4b fd 28 70 40 77 43 fd fd 44 fd 35 69 fd fd fd 1a 43 fd fd fd fd 4d 25 fd 2a 18 03 4f fd 30 44 fd 5d fd fd fd 4e fd fd fd fd fd fd 13 fd fd 25 fd 19 fd 2a 78 75 1e fd fd 6b 29 fd 7e 16 50 7a fd fd 31 2f fd fd 66 fd 2a fd fd 7d 61 fd fd fd 13 fd fd fd fd fd fd 5f fd fd fd fd fd 01 fd 1a 60 7f 61 fd 6b fd 4e 25 5a 65 fd fd 61 fd 07 6f 7e fd fd 3d fd fd 5c 06 fd fd 5e 27 fd fd fd 76 2f e9 5c 4b 1b fd fd 5c 06 fd fd fd 16 35 03 fd fd fd fd 19 fd 42 fd 2e 7b fd 41 fd fd 74 1a fd 76 68 fd fd fd fd fd 73 6c 7d 2a fd 42 fd 46 66 74 3e fd fd 60 fd fd c6 fd 60 0f 3e fd 32 37 28 fd fd fd 4a 2e fd fd fd fd fd 10 fd 1e fd 75 7b fd fd 63 73 75 63 4d 2e 07 07 61 1c 56 fd 27 fd fd 61 3c fd 4e 33 66 fd	>2'JuK(p@wCD5iCM%*O0D]N%*xuk)~Pz1/*}a_`akN%Zeao~=\^'v/\K\5B.{Atvhsl}*Fft>``>27(J.u{csucM.aV'a<N3f	success or wait	5	405BD7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\microphone-sensitivity-low-symbolic.symbolic.png	0	291	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 31 4e 02 51 10 fd fd 1f fd fd fd fd 56 36 52 fd 48 fd 09 33 fd 77 fd 04 1e 41 fd 60 fd 35 76 fd fd 60 6d 4b 02 5a 48 fd 5a 38 fd 6c 60 fd 6c fd 5f 32 79 fd fd fd fd 7c d2 6b 0f 17 38 fd fd 0f fd 61 fd 69 6c fd 00 06 38 fd 7e fd 49 40 fd 59 fd 4c 65 fd 27 3c 47 fd cc fd 1a fd 61 fd fd fd fd 68 fd fd fd 57 40 fd 71 fd 33 fd fd 6e fd 0a 28 6a 62 0b 50 fd 60 fd fd 3f fd 06 fd 58 fd fd 01 fd 31 fd fd 31 01 fd fd 21 66 fd 2f fd fd 68 fd 7e fd fd 21 fd 2e 71 fd 1e fd fd 33 fd 00 07 78 fd 67 18 37 75 1d 7b 53 74 33 00 fd 06 fd fd 04 77 11 2f 51 fd fd 67 fd fd fd	PNGIHDRasBIT|dIDAT81NQV6RHwA`5v`mKZHZ8l`l_2yk8ail8~l@YLe'<GahW@q3n(jbP`X11!f/h~!.q3xg7u{St3w/Qg	success or wait	1	405BD7	WriteFile
C:\Users\user\AppData\Local\Temp\nsp8E94.tmp\System.dll	0	11776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 69 72 2a fd 2d 13 44 fd 2d 13 44 fd 2d 13 44 fd fd 0f 4a fd 2a 13 44 fd 2d 13 45 fd 3e 13 44 fd fd 1c 19 fd 2a 13 44 fd 79 30 74 fd 29 13 44 fd 4e 31 6e fd 2c 13 44 fd fd 33 40 fd 2c 13 44 fd 52 69 63 68 2d 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 7e 15 5c 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 fd 28 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$ir*-D-D-DJ*D-E>D*Dy0t)DN1n,D3@,DRich-DPEL~\.! (	success or wait	1	405BD7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download.exe	unknown	512	success or wait	525	405BA8	ReadFile
C:\Users\user\Desktop\download.exe	unknown	4	success or wait	2	405BA8	ReadFile
C:\Users\user\Desktop\download.exe	unknown	4	success or wait	27	405BA8	ReadFile
C:\Users\user\Desktop\download.exe	unknown	4	success or wait	2	405BA8	ReadFile
C:\Users\user\Desktop\download.exe	unknown	4	success or wait	12	405BA8	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Poserne\Bedugget39.Rus	unknown	1	success or wait	317	405BA8	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Heize\Afreager.For	unknown	58617856	success or wait	1	73B62AB9	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Congested	success or wait	1	405E60	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Congested\Named	success or wait	1	405E60	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Congested	success or wait	1	405E60	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Congested\Named	success or wait	1	405E60	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Studieplaner	success or wait	1	405E60	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Studieplaner\Brnebogspris	success or wait	1	405E60	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Miasms	success or wait	1	405E60	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Miasms\Maskinskriverskerne38	success or wait	1	405E60	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Miasms\Maskinskriverskerne38\Skrosten	success or wait	1	405E60	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Congested\Named	Zoophagous	unicode	Lseoplevelsen	success or wait	1	402464	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Congested\Named	Zoophagous	unicode	Lseoplevelsen	success or wait	1	402464	RegSetValueExA
HKEY_CURRENT_USER\Software\Studieplaner\Brnebogspris	Esurient57	expand unicode	%Forudsaetter%\Oliebilledernes.Pre	success or wait	1	402464	RegSetValueExA
HKEY_CURRENT_USER\Software\Miasms\Maskinskriverskerne38\Skrosten	Antigonorrheal	binary	FF F6 9F 2F	success or wait	1	402464	RegSetValueExA

Disassembly

No disassembly