ID: 800803
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:03:12
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

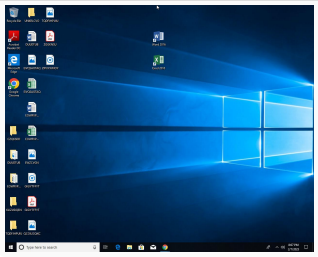
Windows Analysis Report

file.exe

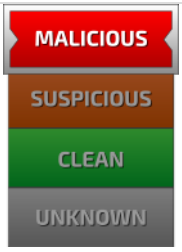
Overview

General Information

Sample Name:	file.exe
Analysis ID:	800803
MD5:	04a988e37b8e…
SHA1:	1182f9d0de33e..
SHA256:	7b734abb2015…
Tags:	exe
Infos:	



Detection



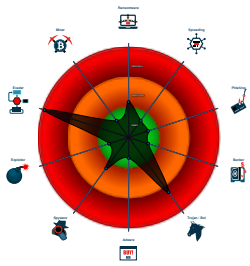
SmokeLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Checks for kernel code integrity (NtQ…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5856 cmdline: C:\Users\user\Desktop\file.exe MD5: 04A988E37B8EA5FACD28A7D42764F597)
  - file.exe (PID: 1720 cmdline: C:\Users\user\Desktop\file.exe MD5: 04A988E37B8EA5FACD28A7D42764F597)
    - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- vhefigi (PID: 4520 cmdline: C:\Users\user\AppData\Roaming\vhefigi MD5: 04A988E37B8EA5FACD28A7D42764F597)
  - vhefigi (PID: 4556 cmdline: C:\Users\user\AppData\Roaming\vhefigi MD5: 04A988E37B8EA5FACD28A7D42764F597)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://host-file-host6.com/",
    "http://host-host-file8.com/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.318591413.0000000002051000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.318591413.0000000002051000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0

Source	Rule	Description	Author	Strings
0000000B.00000002.387762045.00000000008C6000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x60a4:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000002.318398880.0000000000580000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.318398880.0000000000580000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x6f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.5815a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.2.vhefigi.7d15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
12.2.vhefigi.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected SmokeLoader

Remote Access Functionality

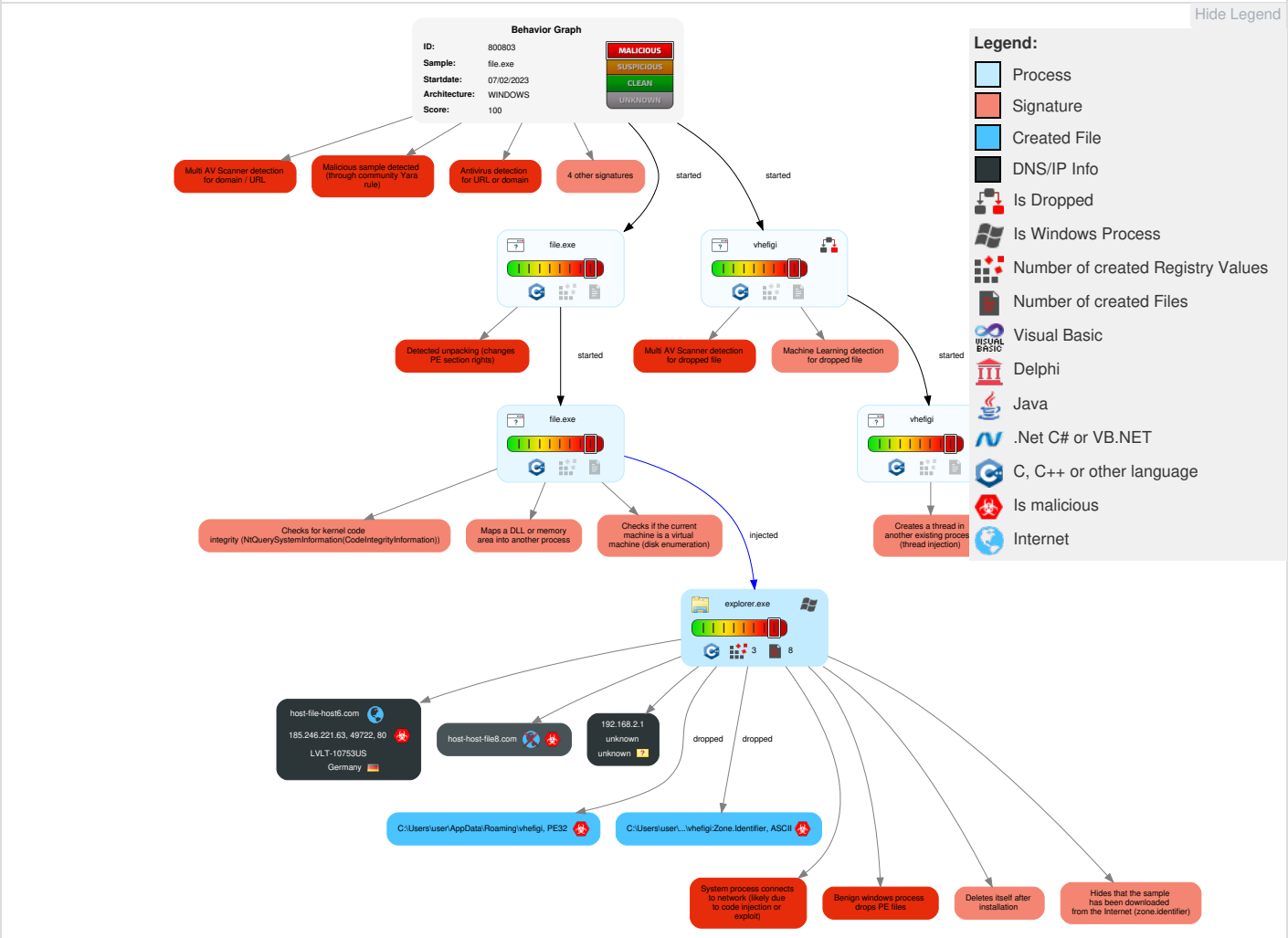
Yara detected SmokeLoader

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	3 Native API	1 DLL Side-Loading	3 1 3 Process Injection	1 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	3 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 3 Process Injection	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 2 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 Deobfuscate/Decode Files or Information	NTDS	3 Process 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 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
file.exe	46%	ReversingLabs	Win32.Ransomware.Stop	
file.exe	36%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\vhefigi	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\vhefigi	46%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Roaming\vhefigi	36%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.vhefigi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.5815a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.vhefigi.7d15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
host-file-host6.com	18%	Virustotal		Browse
host-host-file8.com	18%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://host-file-host6.com/	0%	URL Reputation	safe	
http://host-host-file8.com/	100%	URL Reputation	malware	

Domains and IPs

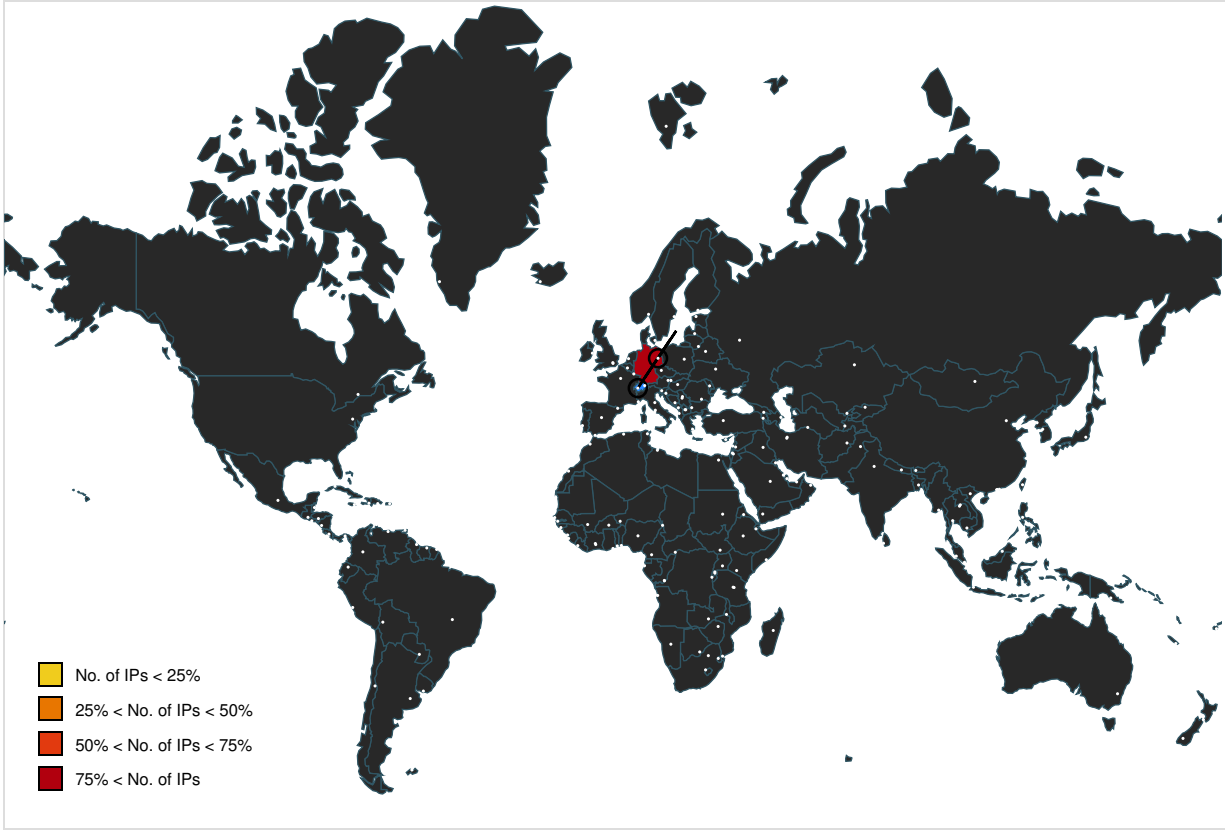
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	185.246.221.63	true	true	• 18%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 18%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://host-file-host6.com/	true	• URL Reputation: safe	unknown
http://host-host-file8.com/	true	• URL Reputation: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.246.221.63	host-file-host6.com	Germany		10753	LVLT-10753US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800803
Start date and time:	2023-02-07 20:03:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/2@4/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 91.6%) • Quality average: 71.9% • Quality standard deviation: 31.9%
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, login.live.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:05:07	API Interceptor	475x Sleep call for process: explorer.exe modified
20:05:41	Task Scheduler	Run new task: Firefox Default Browser Agent E85BC7988C711DBE path: C:\Users\user\AppData\Roaming\vhefigi

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\Roaming\vhefigi

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	198144
Entropy (8bit):	7.034848311694385
Encrypted:	false

SSDEEP:	3072:BJoObqrFdq4LsfErWQ5vk/HqHA0KK1HYRkqPSM3Fa59NhVwgy:BJoDa4LXrxk/cA0/FYeSLFU9Ncg
MD5:	04A988E37B8EA5FACD28A7D42764F597
SHA1:	1182F9D0DE33E9363C7777F3F76D26C179A856E6
SHA-256:	7B734ABB20157CA48892547A61F80013138E9659B0942895991A9AB49FDADF79
SHA-512:	24519302727DCDBB5B020FEB1729980E0602409A205534B4577461E321C95A54A872026809C50C75D04B3B6C112D4E761381E11197F4AC11F106F0165779F252
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46% • Antivirus: Virustotal, Detection: 36%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w...a.....q.....t....Rich.....PE..L...8}.a.....<.....or.....@.....l...P.....@.....p9..@.....text. ....`.data.....6.....@....rsrc..... .....@..@.reloc..n'.....(.....@..B..... ....

C:\Users\user\AppData\Roaming\vhefigi:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.034848311694385
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:	file.exe
File size:	198144
MD5:	04a988e37b8ea5facd28a7d42764f597
SHA1:	1182f9d0de33e9363c7777f3f76d26c179a856e6
SHA256:	7b734abb20157ca48892547a61f80013138e9659b0942895991a9ab49fdadf79
SHA512:	24519302727dcdbb5b020feb1729980e0602409a205534b4577461e321c95a54a872026809c50c75d04b3b6c112d4e761381e11197f4ac11f106f0165779f252
SSDEEP:	3072:BJoObqrFdq4LsfErWQ5vk/HqHA0KK1HYRkqPSM3Fa59NhVwgy:BJoDa4LXrxk/cA0/FYeSLFU9Ncg
TLSH:	DF14C0223980F372C06B25705874DBA53FFEB5309175895B7BA917AE4F302D2663A387
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B.s.....p.....f.....w.....a.....q.....t.....Rich.....PE..L...8}.a.....

File Icon

Icon Hash:	70d0eeeacacaeadd

Static PE Info

General	
Entrypoint:	0x40726f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x611A7D38 [Mon Aug 16 14:59:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	87e1f4e32d01d5a52e605f27fd138118

Entrypoint Preview
Instruction
call 00007F1340BE4E4Ch
jmp 00007F1340BDE7BEh
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F1340BDE966h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F1340BDE990h
test ecx, 00000003h
jne 00007F1340BDE931h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F1340BDE92Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F1340BDE974h
test ah, ah
je 00007F1340BDE966h
test eax, 00FF0000h
je 00007F1340BDE955h
test eax, FF000000h
je 00007F1340BDE944h

Instruction
jmp 00007F1340BDE90Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
cmp ecx, dword ptr [0042C190h]
jne 00007F1340BDE944h
rep ret
jmp 00007F1340BE4E3Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0042C190h]

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1876c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15a000	0x1ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15c000	0xf1c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1240	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3970	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1f4	.text
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	0x1831a	0x18400	False	0.5321560889175257	data	6.371835638411856	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x13f290	0x13600	False	0.9425277217741935	data	7.833380745851634	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x15a000	0x1ee8	0x2000	False	0.60888671875	data	5.786997654811944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15c000	0x276e	0x2800	False	0.32099609375	data	3.3385866771832506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Tibet
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	Nepal
RT_ICON	0x15a1c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Tibetan	India
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Tibet
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	Nepal
RT_ICON	0x15aa68	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Tibetan	India
RT_STRING	0x15bd90	0x4e	data	Tibetan	Tibet
RT_STRING	0x15bd90	0x4e	data	Tibetan	Nepal
RT_STRING	0x15bd90	0x4e	data	Tibetan	India
RT_STRING	0x15bde0	0x50	data	Tibetan	Tibet
RT_STRING	0x15bde0	0x50	data	Tibetan	Nepal
RT_STRING	0x15bde0	0x50	data	Tibetan	India
RT_STRING	0x15be30	0xb6	data	Tibetan	Tibet
RT_STRING	0x15be30	0xb6	data	Tibetan	Nepal
RT_STRING	0x15be30	0xb6	data	Tibetan	India
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Tibet
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	Nepal
RT_GROUP_ICON	0x15bb10	0x22	data	Tibetan	India
RT_VERSION	0x15bb38	0x258	data		

Imports

DLL	Import
KERNEL32.dll	RequestWakeupLatency, CreateFileA, FindActCtxSectionStringA, WriteConsoleInputA, ClearCommBreak, WriteFile, FindFirstVolumeMountPointW, CreateDirectoryExA, LocalSize, WaitForMultipleObjects, ReadConsoleInputA, GetProcessId, FreeUserPhysicalPages, WriteConsoleOutputAttribute, DebugActiveProcessStop, GetLocaleInfoW, GetProcAddress, LocalAlloc, GetCommandLineW, GetBinaryTypeW, InterlockedExchange, OpenMutexW, GetConsoleTitleA, SearchPathA, FreeConsole, EndUpdateResourceA, GetLastError, GetProfileSectionA, SetConsoleCursorInfo, GetConsoleAliasW, CreateSemaphoreA, GlobalFlags, GetConsoleAliasesLengthA, FindResourceW, SetVolumeMountPointW, GetModuleHandleW, HeapAlloc, GetComputerNameA, GetCurrentProcessId, CreateNamedPipeA, EnumResourceLanguagesA, SetHandleInformation, _hwrite, CreateActCtxA, DeleteVolumeMountPointA, MoveFileWithProgressA, AddRefActCtx, WritePrivateProfileStringA, GetUserDefaultLangID, QueryMemoryResourceNotification, WaitForSingleObject, GetLongPathNameW, InterlockedDecrement, VerifyVersionInfoA, EnumCalendarInfoW, FindNextFileW, EnumTimeFormatsA, SetLastError, SetCriticalSectionSpinCount, WritePrivateProfileSectionA, LoadLibraryA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, RtlUnwind, HeapFree, DeleteFileA, GetStartupInfoW, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, Sleep, ExitProcess, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapSize, InitializeCriticalSectionAndSpinCount, WideCharToMultiByte, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleCP, GetConsoleMode, FlushFileBuffers, SetFilePointer, CloseHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle
USER32.dll	GetComboBoxInfo
GDI32.dll	GetTextFaceW

Possible Origin

Language of compilation system	Country where language is spoken	Map
Tibetan	Tibet	
Tibetan	Nepal	
Tibetan	India	

Network Behavior

Network Port Distribution

Total Packets: 10

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:05:06.676763058 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.704660892 CET	80	49722	185.246.221.63	192.168.2.7
Feb 7, 2023 20:05:06.704898119 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.705308914 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.705343962 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.741307020 CET	80	49722	185.246.221.63	192.168.2.7
Feb 7, 2023 20:05:06.850627899 CET	80	49722	185.246.221.63	192.168.2.7
Feb 7, 2023 20:05:06.850774050 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.852236986 CET	49722	80	192.168.2.7	185.246.221.63
Feb 7, 2023 20:05:06.880031109 CET	80	49722	185.246.221.63	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:05:06.647430897 CET	51007	53	192.168.2.7	8.8.8.8
Feb 7, 2023 20:05:06.667443037 CET	53	51007	8.8.8.8	192.168.2.7
Feb 7, 2023 20:05:06.864218950 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 20:05:07.911704063 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 20:05:08.936582088 CET	50513	53	192.168.2.7	8.8.8.8
Feb 7, 2023 20:05:10.893774986 CET	53	50513	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:05:11.939722061 CET	53	50513	8.8.8.8	192.168.2.7
Feb 7, 2023 20:05:12.966223001 CET	53	50513	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 7, 2023 20:05:11.939827919 CET	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable
Feb 7, 2023 20:05:12.966365099 CET	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 20:05:06.647430897 CET	192.168.2.7	8.8.8.8	0x921e	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:06.864218950 CET	192.168.2.7	8.8.8.8	0x19d6	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:07.911704063 CET	192.168.2.7	8.8.8.8	0x19d6	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:08.936582088 CET	192.168.2.7	8.8.8.8	0x19d6	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 20:05:06.667443037 CET	8.8.8.8	192.168.2.7	0x921e	No error (0)	host-file-host6.com		185.246.221.63	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:10.893774986 CET	8.8.8.8	192.168.2.7	0x19d6	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:11.939722061 CET	8.8.8.8	192.168.2.7	0x19d6	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Feb 7, 2023 20:05:12.966223001 CET	8.8.8.8	192.168.2.7	0x19d6	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- uclahet.com
  - host-file-host6.com

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: file.exe PID: **5856**, Parent PID: **3320**

General	
Target ID:	0
Start time:	20:04:48
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	04A988E37B8EA5FACD28A7D42764F597
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.270582685.00000000005B6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: file.exe PID: **1720**, Parent PID: **5856**

General	
Target ID:	1
Start time:	20:04:54
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	04A988E37B8EA5FACD28A7D42764F597
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.318591413.0000000002051000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.318591413.0000000002051000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.318398880.0000000000580000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.318398880.0000000000580000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3320**, Parent PID: **1720**

General

Target ID:	2
Start time:	20:05:00
Start date:	07/02/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vhefigi	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4501F42	CopyFileW
C:\Users\user\AppData\Roaming\vhefigi\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	4501F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	4501F53	DeleteFileW
C:\Users\user\AppData\Roaming\vhefigi:Zone.Identifier	success or wait	1	4501F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vhefigi	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 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 fd fd fd fd fd fd fd fd fd 42 fd 73 fd fd fd fd 70 fd fd fd fd 66 fd fd fd fd 08 fd fd fd fd fd fd fd 77 fd fd fd 61 fd fd fd fd 71 fd fd fd fd 74 fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 38 7d 1a 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$BspfwaqtRichPEL8}a	success or wait	2	4501F42	CopyFileW
C:\Users\user\AppData\Roaming\vhefigi:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	4501F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vhefigi PID: **4520**, Parent PID: **1100**

General

Target ID:	11
Start time:	20:05:41
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\vhefigi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vhefigi
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	04A988E37B8EA5FACD28A7D42764F597
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.387762045.00000000008C6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, ReversingLabs • Detection: 36%, Virustotal, Browse
Reputation:	low

Analysis Process: vhefigi PID: **4556**, Parent PID: **4520**

General	
Target ID:	12
Start time:	20:05:49
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\vhefigi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vhefigi
Imagebase:	0x400000
File size:	198144 bytes
MD5 hash:	04A988E37B8EA5FACD28A7D42764F597
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000C.00000002.398871259.0000000002070000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000C.00000002.398871259.0000000002070000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000C.00000002.398929809.0000000002091000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000C.00000002.398929809.0000000002091000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly