ID: 764031
Sample Name: file.exe
Cookbook: default.jbs
Time: 10:33:06
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

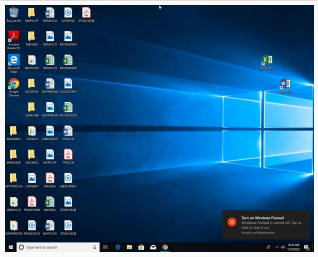
Windows Analysis Report

file.exe

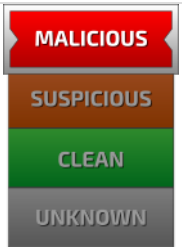
Overview

General Information

Sample Name:	file.exe
Analysis ID:	764031
MD5:	56df4686b20d79..
SHA1:	ceceec6ec094b4..
SHA256:	f6a9c1724adebd..
Tags:	exe
Infos:	



Detection



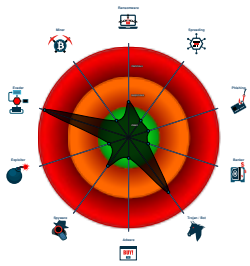
SmokeLoader

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

Signatures

- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Checks for kernel code integrity (NtQ…
- Deletes itself after installation
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 1440 cmdline: C:\Users\user\Desktop\file.exe MD5: 56DF4686B20D79D1E9070C908DBF9058)
  - file.exe (PID: 864 cmdline: C:\Users\user\Desktop\file.exe MD5: 56DF4686B20D79D1E9070C908DBF9058)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- ehddsbh (PID: 6128 cmdline: C:\Users\user\AppData\Roaming\ehddsbh MD5: 56DF4686B20D79D1E9070C908DBF9058)
  - ehddsbh (PID: 5140 cmdline: C:\Users\user\AppData\Roaming\ehddsbh MD5: 56DF4686B20D79D1E9070C908DBF9058)
- **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
00000005.00000002.446345716.0000000000583000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x785e:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000006.00000002.457448235.00000000005A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000006.00000002.457448235.00000000005A1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000002.00000000.382917780.0000000002951000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000002.00000000.382917780.0000000002951000.00000020.80000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$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
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.file.exe.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.0.ehddsbh.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.0.ehddsbh.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.0.ehddsbh.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 5 entries				

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

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)

Copyright Joe Security LLC 2022

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

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

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

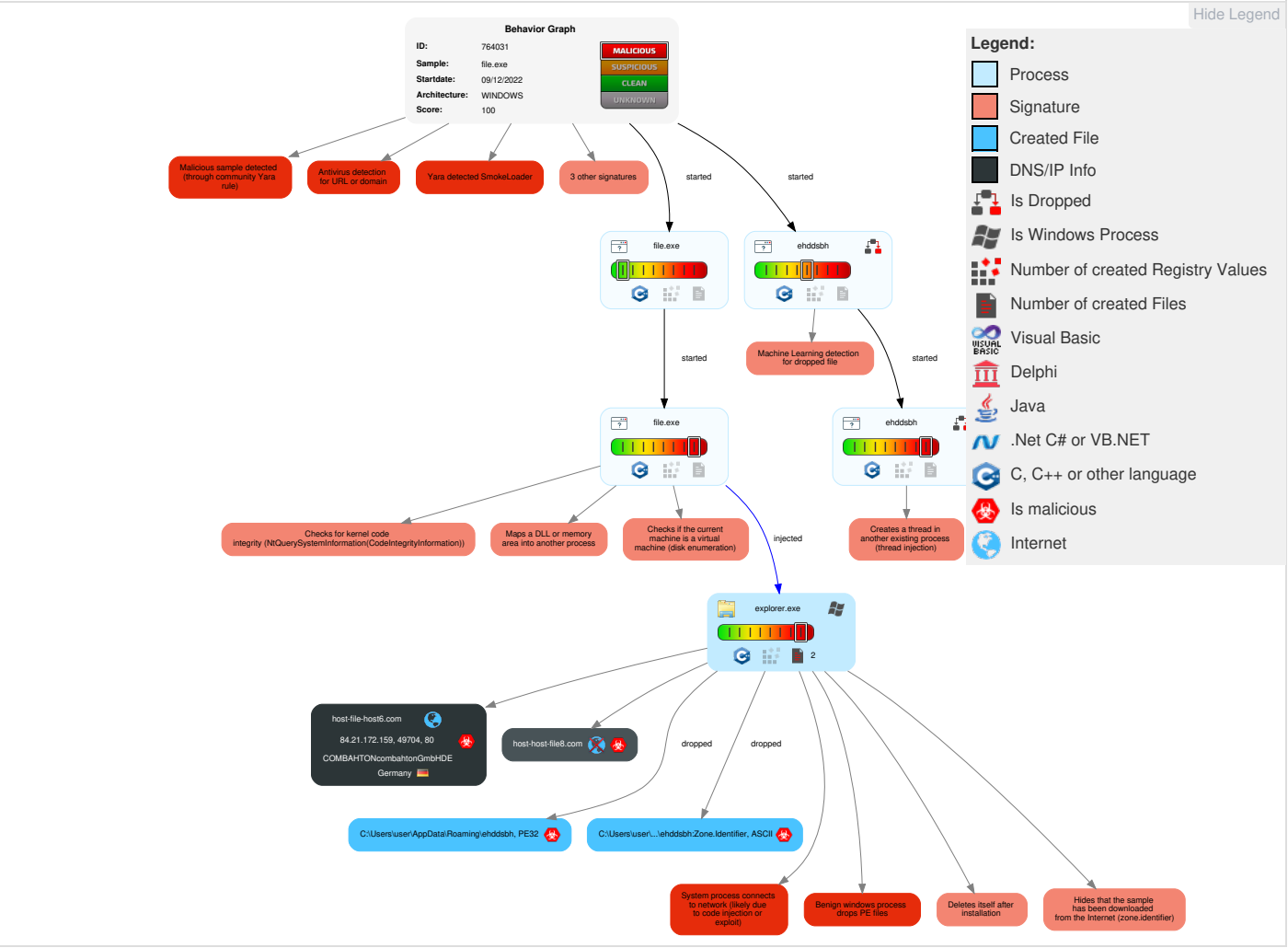
Yara detected SmokeLoader

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	2 Command and Scripting Interpreter	1 DLL Side-Loading	3 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 System Time 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	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	3 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	3 1 2 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	2 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
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	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	Network Service Scanning	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.

Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ehddsbh	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.ehddsbh.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
6.0.ehddsbh.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.file.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.ehddsbh.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.file.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.ehddsbh.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.ehddsbh.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.ehddsbh.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.ehddsbh.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.file.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.file.exe.5a15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.ehddsbh.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.file.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.file.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.file.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.ehddsbh.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

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	84.21.172.159	true	true		unknown
host-host-file8.com	unknown	unknown	true		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

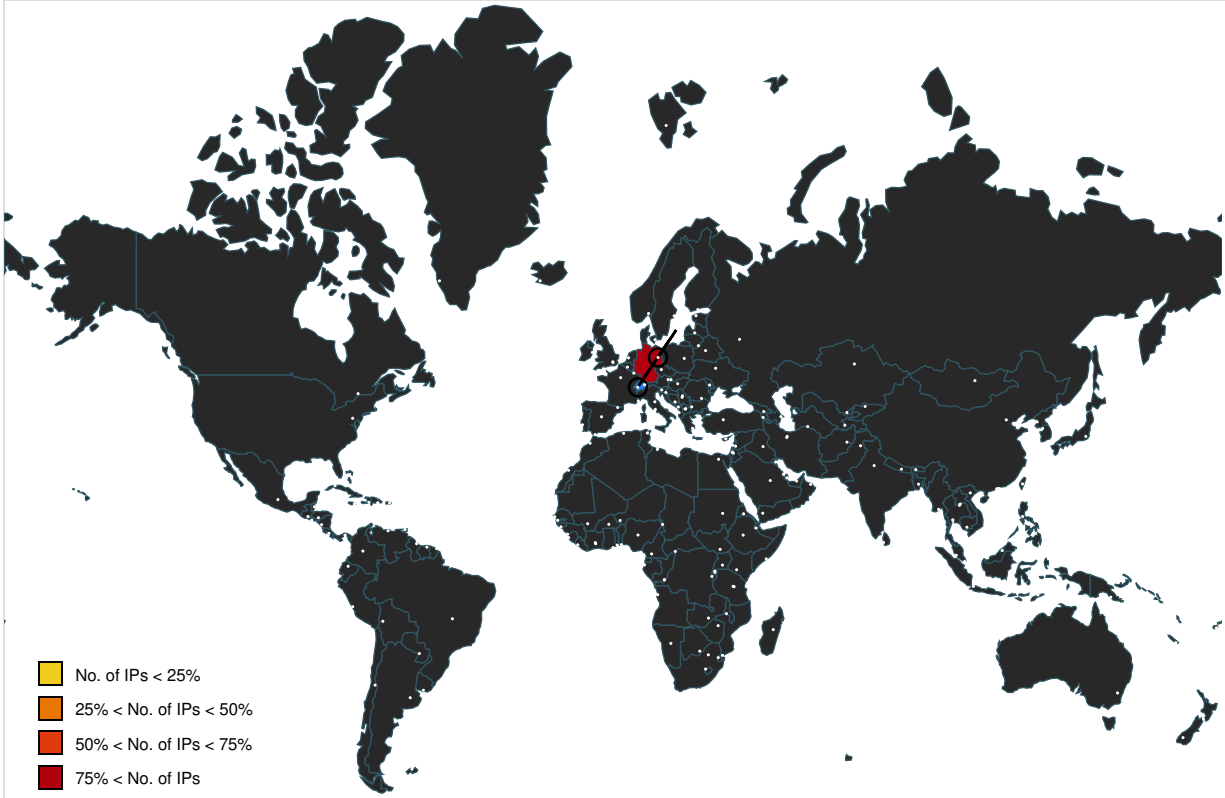
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.32225323 8.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 002.00000000.355553490.0000000000921000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.382336860.000000 000091F000.00000004.00000020.00020000.00 000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.21.172.159	host-file-host6.com	Germany		30823	COMBAHTONcombahtonGmbHDE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764031
Start date and time:	2022-12-09 10:33:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
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:	7
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

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/2@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.6% (good quality ratio 91.3%) • Quality average: 71.5% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 100% • 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, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
10:35:01	Task Scheduler	Run new task: Firefox Default Browser Agent F555D525CEDA98ED path: C:\Users\user\AppData\Roaming\ehddsbh

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\ehddsbh

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	391680
Entropy (8bit):	5.907475331882966
Encrypted:	false
SSDEEP:	6144:Qkf1yLTGbxZo30sCs+D7b8u5tiwhh6K9W92/oF4sded89kTt:XQfGbPGCs2ZNIK9W92/oOac
MD5:	56DF4686B20D79D1E9070C908DBF9058
SHA1:	CECEEC6EC094B4979A4B9AC4049A38449982F8B2
SHA-256:	F6A9C1724ADEBD1E1BC54CB2B2E6CC49B8A6F11910A3B6ACDFC6C5531A1D742B
SHA-512:	A7D9B82FDBAA18195C2E7E4DF8A81AC4279401E64C9F59A6B5DEAD2B00C204179955AD328D12B7A5B6109D0499A13C3FCA07AF678D899324F8AE87B849BDEC E7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.m....C...C...C...C(..C...C...C...C...C$%xC...C...C}..C...C.. .C...C...C...C...CRich...C.....PE..L.....b.....n.....p.....@.....`.....|.....s..<.....@.....0I..@. .....text...Vm.....n..... ..`.data.....r.....@....tutesay.....p.....&.....@..@.nuyus..p.....2.....@..@.rsrc.....6..... .....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Roaming\ehddsbh: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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
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):	5.907475331882966
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:	391680
MD5:	56df4686b20d79d1e9070c908dbf9058
SHA1:	ceceec6ec094b4979a4b9ac4049a38449982f8b2
SHA256:	f6a9c1724adebd1e1bc54cb2b2e6cc49b8a6f11910a3b6acdfc6c5531a1d742b
SHA512:	a7d9b82fdbaa18195c2e7e4df8a81ac4279401e64c9f59a6b5dead2b00c204179955ad328d12b7a5b6109d0499a13c3fca07af678d899324f8ae87b849bdece7
SSDEEP:	6144:Qkf1yLTGbxZo30sCs+D7b8u5tiwhh6K9W92/oF4sded89kTt:XQfGbPGCs2ZNIK9W92/oOac
TLSH:	5F84D0013284C4F2C7621D77491ACBE1E53BB43BFA346977F7182B6FBEB029195A2215
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.m....C...C...C...C(..C...C...C...C...C$%xC...C...C}..C...C...C...C...C...CRich...C.....PE..L.....b.....n.

File Icon

Icon Hash:	8286dccea68c9c84

Static PE Info

General

Entrypoint:	0x407096
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:	0x62A586AD [Sun Jun 12 06:24:45 2022 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:	eeffe9860bc9c6507e24465b9b5239be

Entrypoint Preview

Instruction
call 00007F7798B6579Ch
jmp 00007F7798B5FAFEh
mov edi, edi
push ebp
mov ebp, esp
sub esp, 28h
xor eax, eax
push ebx
mov ebx, dword ptr [ebp+0Ch]
push esi
mov esi, dword ptr [ebp+10h]
push edi
mov edi, dword ptr [ebp+08h]
mov byte ptr [ebp-08h], al
mov byte ptr [ebp-07h], al
mov byte ptr [ebp-06h], al
mov byte ptr [ebp-05h], al
mov byte ptr [ebp-04h], al
mov byte ptr [ebp-03h], al
mov byte ptr [ebp-02h], al
mov byte ptr [ebp-01h], al
cmp dword ptr [00443324h], eax
je 00007F7798B5FC90h
push dword ptr [004462C8h]
call 00007F7798B646C8h
pop ecx
jmp 00007F7798B5FC87h
mov eax, 0040CC48h
mov ecx, dword ptr [ebp+14h]
mov edx, 000000A6h
cmp ecx, edx
jg 00007F7798B5FDFAh
je 00007F7798B5FDE1h
cmp ecx, 19h
jg 00007F7798B5FD7Eh

Instruction
je 00007F7798B5FD6Fh
mov edx, ecx
push 00000002h
pop ecx
sub edx, ecx
je 00007F7798B5FD53h
dec edx
je 00007F7798B5FD43h
sub edx, 05h
je 00007F7798B5FD2Bh
dec edx
je 00007F7798B5FD0Ch
sub edx, 05h
je 00007F7798B5FCF3h
dec edx
je 00007F7798B5FCC7h
sub edx, 09h
jne 00007F7798B5FE5Ah
mov dword ptr [ebp-28h], 00000003h
mov dword ptr [ebp-24h], 00401348h
fld qword ptr [edi]
lea ecx, dword ptr [ebp-28h]
fstp qword ptr [ebp-20h]
push ecx
fld qword ptr [ebx]
fstp qword ptr [ebp+00h]

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [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	0x173c4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x49000	0x1a510	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	0xda4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11f0	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	0x4930	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x19c	.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	0x16d56	0x16e00	False	0.5953829405737705	data	6.7039529820863955	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x18000	0x2e2e4	0x2b400	False	0.48512576770231214	data	4.841536392944569	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tutesay	0x47000	0xbb8	0xc00	False	0.008138020833333334	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nuyus	0x48000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x49000	0x1a510	0x1a600	False	0.6380054058056872	data	6.252448863423772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0x1c12	0x1e00	False	0.38958333333333334	data	3.8825952867996567	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x61450	0x2	data	Slovak	Slovakia
AFX_DIALOG_LAYOUT	0x61438	0x2	data	Slovak	Slovakia
AFX_DIALOG_LAYOUT	0x61440	0xc	data	Slovak	Slovakia
SUXUMOWUDAKOLA	0x5f2d0	0x2107	ASCII text, with very long lines (8455), with no line terminators	Slovak	Slovakia
RT_CURSOR	0x61458	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_CURSOR	0x62300	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia
RT_CURSOR	0x62bd0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0	Slovak	Slovakia
RT_CURSOR	0x62d00	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0	Slovak	Slovakia
RT_ICON	0x49990	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x4a058	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x4c600	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x4ca98	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x4d940	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x4e1e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x4e750	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x50cf8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x51da0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x52728	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x52bf8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x53aa0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x54348	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x54a10	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Slovak	Slovakia
RT_ICON	0x54f78	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x57520	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x585c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x58a98	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Slovak	Slovakia

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_ICON	0x59940	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Slovak	Slovakia
RT_ICON	0x5a1e8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Slovak	Slovakia
RT_ICON	0x5a8b0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Slovak	Slovakia
RT_ICON	0x5ae18	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Slovak	Slovakia
RT_ICON	0x5d3c0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Slovak	Slovakia
RT_ICON	0x5e468	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Slovak	Slovakia
RT_ICON	0x5edf0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Slovak	Slovakia
RT_STRING	0x62fc8	0x546	data	Slovak	Slovakia
RT_ACCELERATOR	0x613d8	0x40	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x62ba8	0x22	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x62db0	0x22	data	Slovak	Slovakia
RT_GROUP_ICON	0x58a30	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x4ca68	0x30	data	Slovak	Slovakia
RT_GROUP_ICON	0x52b90	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x5f258	0x76	data	Slovak	Slovakia
RT_VERSION	0x62dd8	0x1f0	MS Windows COFF PowerPC object file	Slovak	Slovakia
None	0x61418	0xa	data	Slovak	Slovakia
None	0x61428	0xa	data	Slovak	Slovakia

Imports

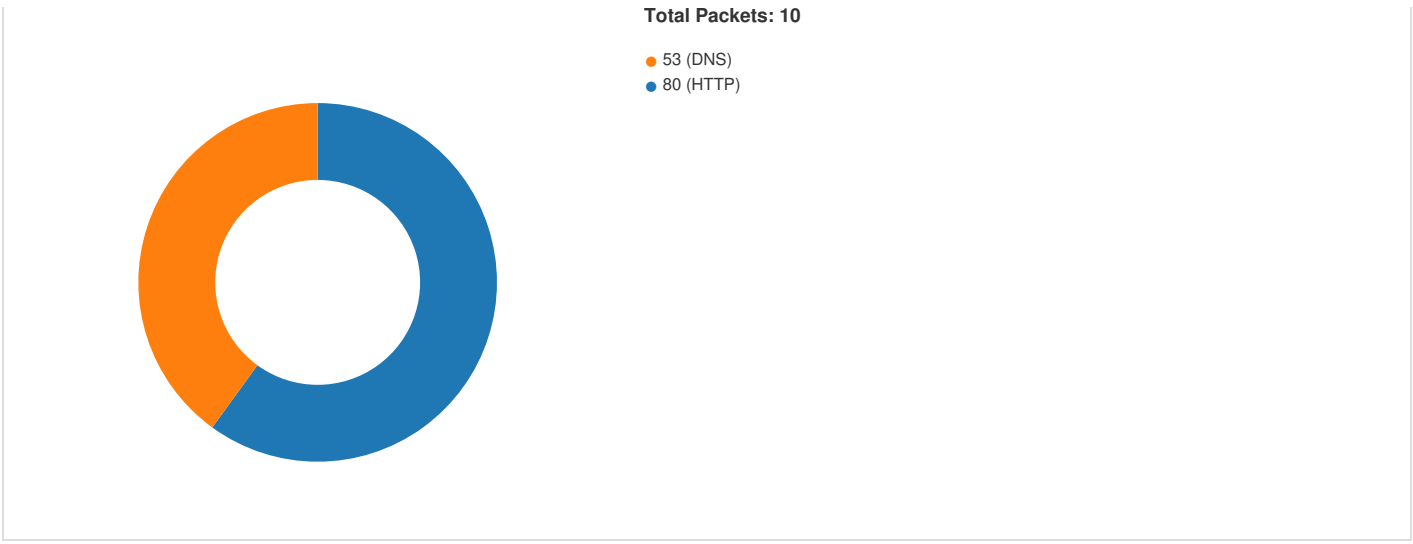
DLL	Import
KERNEL32.dll	FillConsoleOutputCharacterA, GetCPInfo, GetProfileIntW, GetSystemDefaultLCID, GetModuleHandleW, WaitNamedPipeW, TlsSetValue, GetPriorityClass, GetVolumeInformationA, LoadLibraryW, IsProcessInJob, AssignProcessToJobObject, GetCalendarInfoW, GetFileAttributesA, TransactNamedPipe, WriteConsoleW, GetVolumePathNameA, CreateJobObjectA, GetVolumeNameForVolumeMountPointA, FillConsoleOutputCharacterW, GetLastError, GetProcAddress, VirtualAlloc, EnumSystemCodePagesW, SetFileAttributesA, LoadLibraryA, WriteConsoleA, GetProcessWorkingSetSize, LocalAlloc, OpenJobObjectW, FoldStringW, FoldStringA, FindFirstChangeNotificationA, GetFileInformationByHandle, FindActCtxSectionStringW, LCMapStringW, GetConsoleAliasesW, GetFullPathNameW, HeapFree, HeapAlloc, Sleep, ExitProcess, GetStartupInfoW, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapReAlloc, WriteFile, GetStdHandle, GetModuleFileNameA, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlUnwind, SetHandleCount, GetFileType, GetStartupInfoA, SetFilePointer, TlsGetValue, TlsAlloc, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, InitializeCriticalSectionAndSpinCount, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, RaiseException, GetConsoleOutputCP, MultiByteToWideChar, SetStdHandle, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, CreateFileA, GetModuleHandleA, HeapSize, GetLocaleInfoA, LCMapStringA, GetStringTypeA, GetStringTypeW, SetEndOfFile, GetProcessHeap, ReadFile
ADVAPI32.dll	BackupEventLogW

Possible Origin

Language of compilation system	Country where language is spoken	Map
Slovak	Slovakia	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:35:01.859349012 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:01.885931015 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:35:01.886043072 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:01.886162996 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:01.886178970 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:01.914613962 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:35:02.003720999 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:35:02.003875017 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:02.005376101 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:35:02.032603025 CET	80	49704	84.21.172.159	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:35:01.559169054 CET	49724	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:35:01.852946043 CET	53	49724	8.8.8.8	192.168.2.5
Dec 9, 2022 10:35:02.013329029 CET	61452	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:35:03.018937111 CET	61452	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:35:04.034967899 CET	61452	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:35:06.042310953 CET	53	61452	8.8.8.8	192.168.2.5
Dec 9, 2022 10:35:07.043878078 CET	53	61452	8.8.8.8	192.168.2.5
Dec 9, 2022 10:35:08.090504885 CET	53	61452	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 9, 2022 10:35:07.045248032 CET	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
Dec 9, 2022 10:35:08.090667009 CET	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:35:01.559169054 CET	192.168.2.5	8.8.8.8	0x54a4	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:02.013329029 CET	192.168.2.5	8.8.8.8	0xc44f	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:03.018937111 CET	192.168.2.5	8.8.8.8	0xc44f	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:04.034967899 CET	192.168.2.5	8.8.8.8	0xc44f	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

DNS Answers

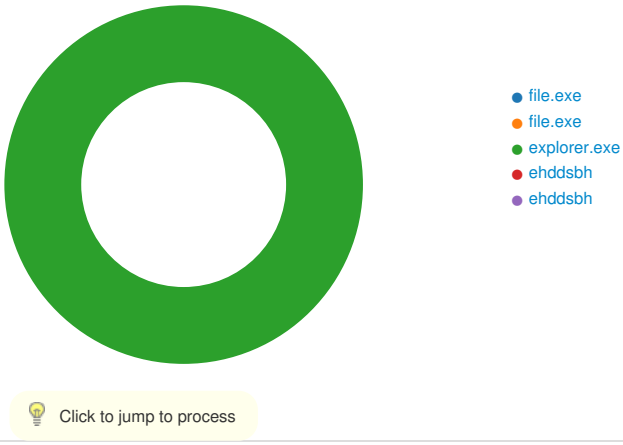
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:35:01.852946043 CET	8.8.8.8	192.168.2.5	0x54a4	No error (0)	host-file-host6.com		84.21.172.159	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:06.042310953 CET	8.8.8.8	192.168.2.5	0xc44f	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:07.043878078 CET	8.8.8.8	192.168.2.5	0xc44f	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:35:08.090504885 CET	8.8.8.8	192.168.2.5	0xc44f	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- nwisehi.com
  - host-file-host6.com

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **1440**, Parent PID: **3324**

General

Target ID:	0
Start time:	10:33:59
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	391680 bytes
MD5 hash:	56DF4686B20D79D1E9070C908DBF9058
Has elevated privileges:	true

Copyright Joe Security LLC 2022

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.311136016.00000000005C3000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: file.exe PID: **864**, Parent PID: **1440**

General

Target ID:	1
Start time:	10:34:05
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	391680 bytes
MD5 hash:	56DF4686B20D79D1E9070C908DBF9058
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: 00000001.00000002.396112310.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.396112310.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.396068143.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.396068143.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3324**, Parent PID: **864**

General

Target ID:	2
Start time:	10:34:11
Start date:	09/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000002.00000000.382917780.0000000002951000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000002.00000000.382917780.0000000002951000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ehddsbh	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	2951F42	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ehddsbh\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2951F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	2951F53	DeleteFileW
C:\Users\user\AppData\Roaming\ehddsbh:Zone.Identifier	success or wait	1	2951F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ehddsbh	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 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 47 fd 6d 10 03 fd 03 43 03 fd 03 43 03 fd 03 43 1d fd fd 43 28 fd 03 43 1d fd fd 43 19 fd 03 43 1d fd fd 43 fd fd 03 43 24 25 78 43 06 fd 03 43 03 fd 02 43 7d fd 03 43 1d fd fd 43 02 fd 03 43 1d fd fd 43 02 fd 03 43 1d fd fd 43 02 fd 03 43 52 69 63 68 03 fd 03 43 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 6e 01	MZ@!L!This program cannot be run in DOS mode.$GmCCCC(CCCCC$%xCCC}CCCCCCCRichCPELbn	success or wait	3	2951F42	CopyFileW
C:\Users\user\AppData\Roaming\ehddsbh: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	2951F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ehddsbh

PID: **6128**, Parent PID: **1084**

General

Target ID:	5
Start time:	10:35:01
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\ehddsbh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ehddsbh
Imagebase:	0x400000
File size:	391680 bytes
MD5 hash:	56DF4686B20D79D1E9070C908DBF9058
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: 00000005.00000002.446345716.0000000000583000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Copyright Joe Security LLC 2022

Analysis Process: ehddsbh PID: **5140**, Parent PID: **6128**

General	
Target ID:	6
Start time:	10:35:08
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\ehddsbh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ehddsbh
Imagebase:	0x400000
File size:	391680 bytes
MD5 hash:	56DF4686B20D79D1E9070C908DBF9058
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: 00000006.00000002.457448235.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.457448235.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000002.457358703.0000000000570000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.457358703.0000000000570000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly