ID: 753428
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:12:05
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

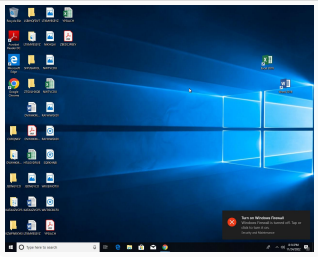
Windows Analysis Report

file.exe

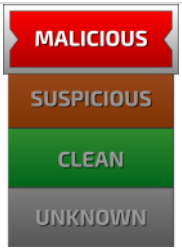
Overview

General Information

Sample Name:	file.exe
Analysis ID:	753428
MD5:	4ae4a84eba3264.
SHA1:	bc8ee7fb36f3e3c..
SHA256:	bb531c53e5dc8f...
Tags:	exe
Infos:	



Detection



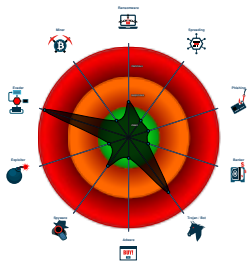
SmokeLoader

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...
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Maps a DLL or memory area into an...
- Machine Learning detection for sam...
- Checks for kernel code integrity (NtQ...
- Deletes itself after installation
- Machine Learning detection for drop...

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5996 cmdline: C:\Users\user\Desktop\file.exe MD5: 4AE4A84EBA3264C433E0C1B92594C61B)
  - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- vvtsewb (PID: 5936 cmdline: C:\Users\user\AppData\Roaming\vvtsewb MD5: 4AE4A84EBA3264C433E0C1B92594C61B)
- **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
00000002.00000002.412766859.00000000007B0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000002.00000002.412803739.00000000007E1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.412803739.00000000007E1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000002.00000002.413033982.00000000009D8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x5260:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.371278858.00000000022A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.vvtsewb.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
2.3.vvtsewb.7c0000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
2.2.vvtsewb.7b0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.7e0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 1 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

Multi AV Scanner detection for domain / URL

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

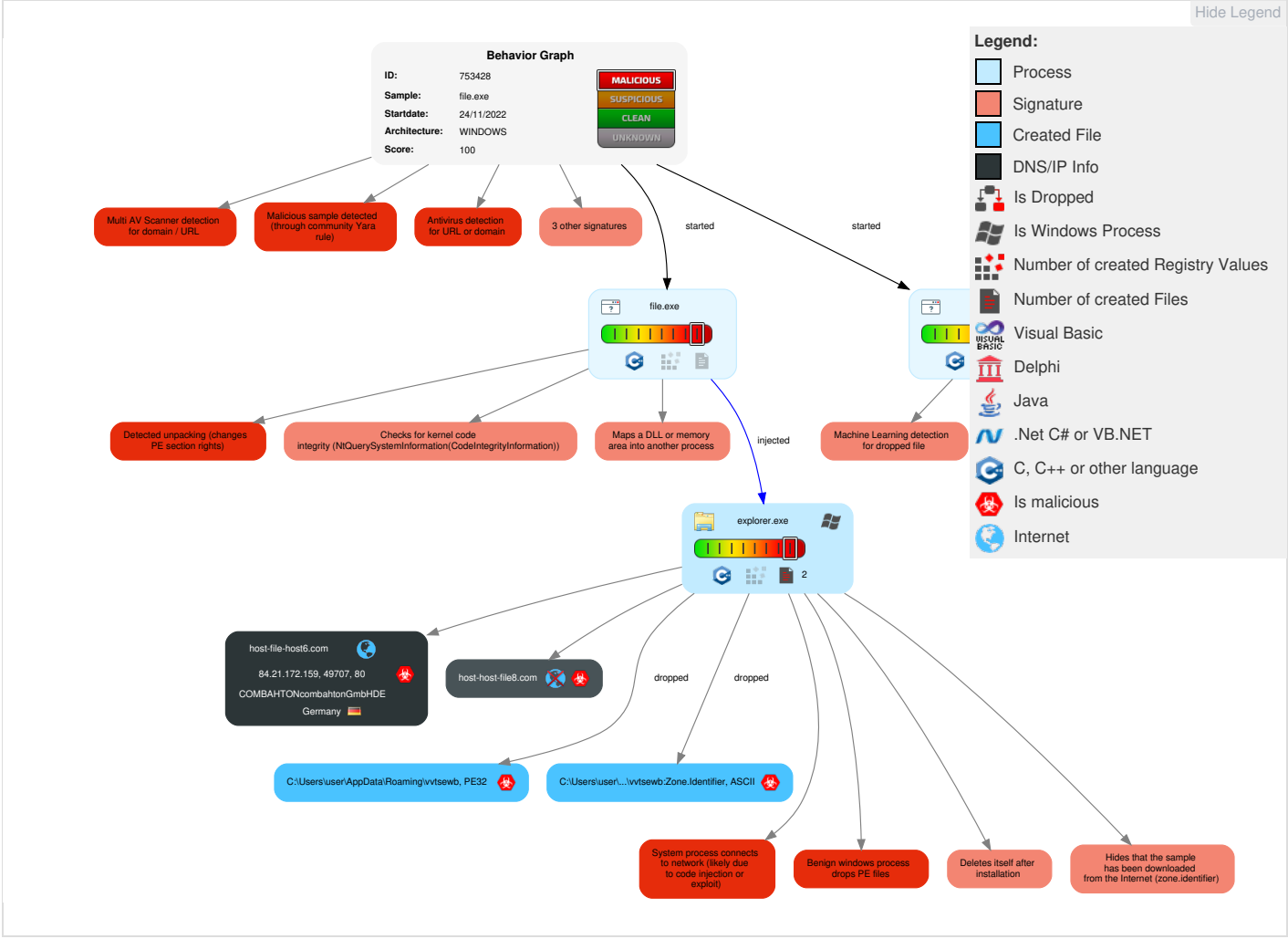
Yara detected SmokeLoader

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	1 Exploitation for Client Execution	1 DLL Side-Loading	3 2 Process Injection	1 1 Masquerading	1 Input Capture	2 1 1 Security Software 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	1 2 Virtualization/Sandbox Evasion	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 2 Process Injection	Security Account Manager	3 Process Discovery	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 Hidden Files and Directories	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	3 System Information 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	1 Software Packing	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	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 File Deletion	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

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	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.3.vvtsewb.7c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.vvtsewb.7b0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.vvtsewb.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.file.exe.800000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.7e0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
host-file-host6.com	20%	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	84.21.172.159	true	true	• 20%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 18%, Virustotal, Browse	unknown

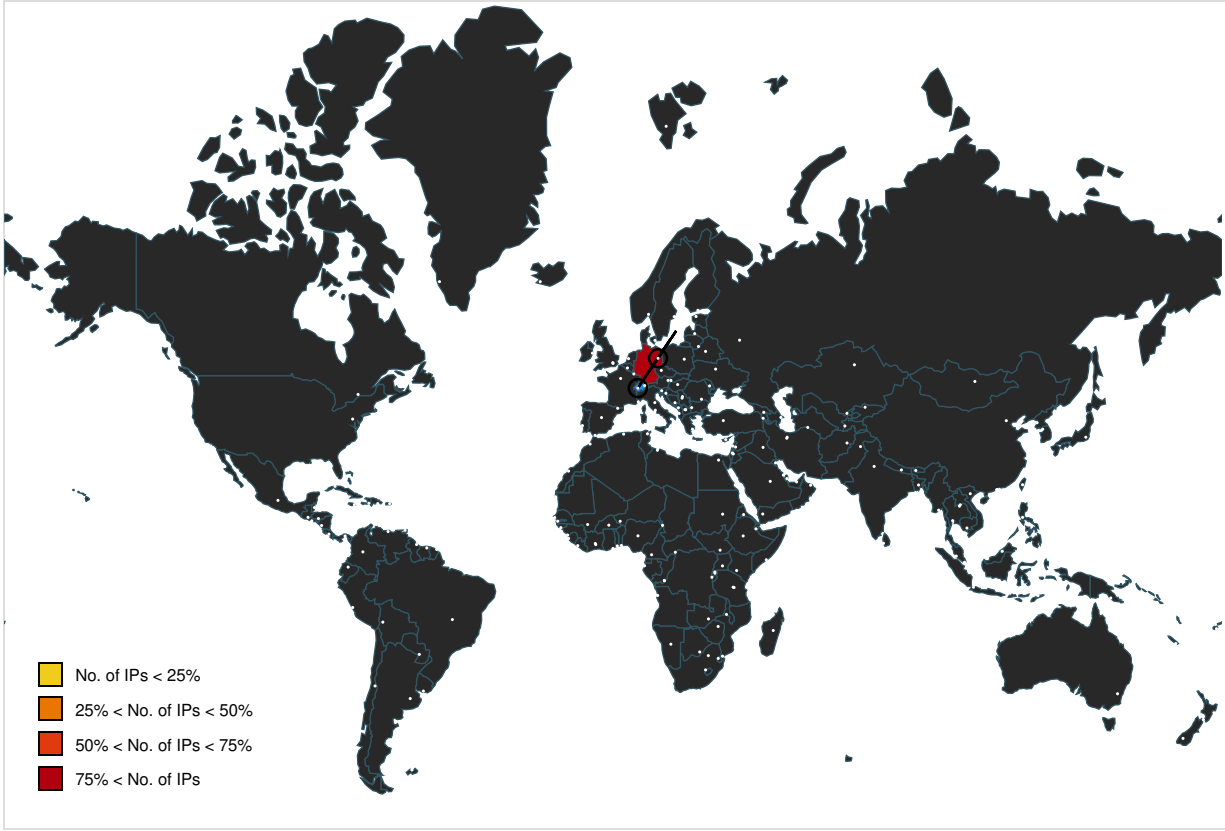
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.33305569 4.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000000.303883320.000000000091F000. 00000004.00000020.00020000.00000000.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:	753428
Start date and time:	2022-11-24 20:12:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
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:	5
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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@2/2@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 14% (good quality ratio 11.9%) • Quality average: 45.2% • Quality standard deviation: 27.1%

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
20:13:46	Task Scheduler	Run new task: Firefox Default Browser Agent 0A8EA222D941D8E8 path: C:\Users\user\AppData\Roaming\vvtsewb

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\vvtsewb

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	6.91435980932861
Encrypted:	false
SSDEEP:	3072:WsKq2R3GPBzO0uLLO1PtKl5JOLAtsDXi2D4VSZAwbUOrsIUwUT7:0qmLLObVAtsDXi2lrbUOrwNP
MD5:	4AE4A84EBA3264C433E0C1B92594C61B
SHA1:	BC8EE7FB36F3E3C03638BC5B6BF0BC9DD7CC034B
SHA-256:	BB531C53E5DC8FCC1FE71EF481253B9D3FA86446E7205E750DC3D6EE5C2A5636
SHA-512:	E9E1878DE9D124BD52EAE169A398C2DB91B12B5B832D5ED03B659EDA9B0B105892339ED47A8890EA5363F03D35EF8E0C59D19A36D98F321601C70FC05C144B9

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich..... .....PE..L.....a.....>#.....o.....@.....$.....S.....\...d....$.....p.....P<..@..... .....text..... ..`.data....."..... @....rsrc.....$..0.....@..@.....

C:\Users\user\AppData\Roaming\vvtsewb: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):	6.91435980932861
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:	192512
MD5:	4ae4a84eba3264c433e0c1b92594c61b
SHA1:	bc8ee7fb36f3e3c03638bc5b6bf0bc9dd7cc034b
SHA256:	bb531c53e5dc8fcc1fe71ef481253b9d3fa86446e7205e750dc3d6ee5c2a5636
SHA512:	e9e1878de9d124bd52eae169a398c2db91b12b5b832d5ed03b659eda9b0b105892339ed47a8890ea5363f03d35ef8e0c59d19a36d98f321601c70fc05c144be9
SSDEEP:	3072:WsKq2R3GPBzO0uLLO1PtKl5JOLAtsDXi2D4VSZAwbUOrsIUwUT7:0qmLLObVAtsDXi2lrbUOrwNP
TLSH:	3F14C03236C0C432C5AB55708D24EAA0EF7EB9315579964B7BE80B6D5F702D0A63B34B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich.....PE..L.....a...

File Icon

Icon Hash:	20e0c4ccccc6b214

Static PE Info

General

Entrypoint:	0x406fe6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE

DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x612E2E88 [Tue Aug 31 13:28:40 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:	5a0f5eee1a1d8df02fd40c6cf3174a3d

Entrypoint Preview
Instruction
call 00007FBFFCA0D3C6h
jmp 00007FBFFCA05A4Eh
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007FBFFCA05BF6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007FBFFCA05C20h
test ecx, 00000003h
jne 00007FBFFCA05BC1h
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 00007FBFFCA05BBAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007FBFFCA05C04h
test ah, ah
je 00007FBFFCA05BF6h
test eax, 00FF0000h
je 00007FBFFCA05BE5h
test eax, FF000000h
je 00007FBFFCA05BD4h
jmp 00007FBFFCA05B9Fh
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]

Instruction
sub eax, ecx
ret
cmp ecx, dword ptr [0042B980h]
jne 00007FBFFCA05BD4h
rep ret
jmp 00007FBFFCA0D3BDh
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 [0042B980h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp+00h], 00000000h

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	0x1a05c	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x249000	0x2ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1270	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	0x3c50	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x220	.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	0x19cf4	0x19e00	False	0.5225505736714976	data	6.34350345002809	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x22dae8	0x11e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x249000	0x2ee8	0x3000	False	0.537353515625	data	4.913683051285504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2491f0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x2498b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x249e20	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Raeto-Romance	Switzerland
RT_ICON	0x24aec8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Raeto-Romance	Switzerland
RT_ICON	0x24b850	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x24bd08	0x98	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x24bcb8	0x4c	data	Raeto-Romance	Switzerland
RT_VERSION	0x24bda0	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	WriteConsoleInputA, EnumDateFormatsA, OpenMutexA, GetConsoleAliasExesLengthW, CopyFileExA, ReadConsoleOutputCharacterA, GetEnvironmentStrings, FreeUserPhysicalPages, QueryDosDeviceA, EnumCalendarInfoExA, GetProcessPriorityBoost, LocalSize, AddConsoleAliasW, CreateFileW, GetMailslotInfo, GetWindowsDirectoryA, GetModuleHandleW, VirtualFree, CreateDirectoryExA, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerW, GetVersionExA, SearchPathA, RequestWakeupLatency, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotW, BuildCommDCBAndTimeoutsA, GetProcAddress, GetModuleHandleA, LocalAlloc, FindNextFileA, TerminateThread, GetCommandLineW, FindFirstChangeNotificationA, VerifyVersionInfoA, DeleteTimerQueue, FindFirstVolumeA, GlobalFlags, GetTickCount, GetACP, GlobalWire, GetTapeParameters, HeapWalk, GetConsoleTitleA, InterlockedCompareExchange, EnumCalendarInfoA, GetNamedPipeHandleStateW, InterlockedDecrement, SetCalendarInfoA, TerminateProcess, MoveFileA, AddAtomW, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointA, VirtualAlloc, SetConsoleActiveScreenBuffer, GetCPInfo, GetProcessIoCounters, GlobalFindAtomA, CreateFileA, CloseHandle, GetVolumeInformationA, EnumSystemCodePagesA, MoveFileWithProgressA, LoadLibraryW, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, RtlUnwind, GetLastError, DeleteFileA, GetStartupInfoW, HeapAlloc, HeapFree, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameW, GetEnvironmentStringsW, HeapCreate, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, GetOEMCP, IsValidCodePage, HeapSize, LoadLibraryA, InitializeCriticalSectionAndSpinCount, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, ReadFile
USER32.dll	GetComboBoxInfo, GetMessageExtraInfo, GetListBoxInfo
GDI32.dll	GetBoundsRect
ADVAPI32.dll	SetThreadToken

Possible Origin

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Network Port Distribution

Total Packets: 10

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:47.187021017 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.215519905 CET	80	49707	84.21.172.159	192.168.2.5
Nov 24, 2022 20:13:47.216058016 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.216236115 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.216314077 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.244088888 CET	80	49707	84.21.172.159	192.168.2.5
Nov 24, 2022 20:13:47.335669041 CET	80	49707	84.21.172.159	192.168.2.5
Nov 24, 2022 20:13:47.335818052 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.337459087 CET	49707	80	192.168.2.5	84.21.172.159
Nov 24, 2022 20:13:47.366754055 CET	80	49707	84.21.172.159	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:46.928529978 CET	61452	53	192.168.2.5	8.8.8.8
Nov 24, 2022 20:13:47.183770895 CET	53	61452	8.8.8.8	192.168.2.5
Nov 24, 2022 20:13:47.349159956 CET	51484	53	192.168.2.5	8.8.8.8
Nov 24, 2022 20:13:48.338735104 CET	51484	53	192.168.2.5	8.8.8.8
Nov 24, 2022 20:13:49.370031118 CET	51484	53	192.168.2.5	8.8.8.8
Nov 24, 2022 20:13:51.378423929 CET	53	51484	8.8.8.8	192.168.2.5
Nov 24, 2022 20:13:52.380325079 CET	53	51484	8.8.8.8	192.168.2.5
Nov 24, 2022 20:13:53.396895885 CET	53	51484	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 24, 2022 20:13:52.380429983 CET	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
Nov 24, 2022 20:13:53.397217989 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
Nov 24, 2022 20:13:46.928529978 CET	192.168.2.5	8.8.8.8	0xa2c5	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:47.349159956 CET	192.168.2.5	8.8.8.8	0x417e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:48.338735104 CET	192.168.2.5	8.8.8.8	0x417e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:49.370031118 CET	192.168.2.5	8.8.8.8	0x417e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

DNS Answers

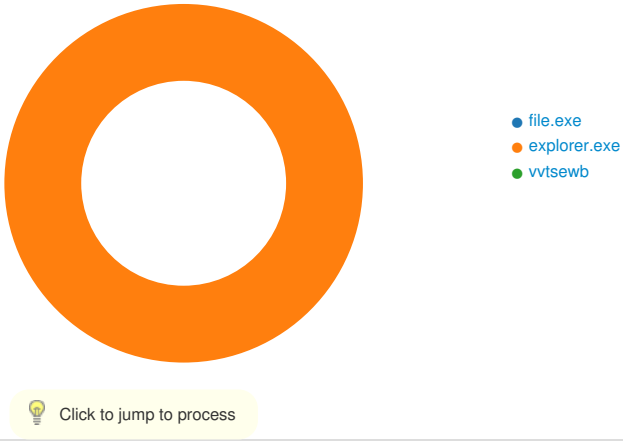
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:47.183770895 CET	8.8.8.8	192.168.2.5	0xa2c5	No error (0)	host-file-host6.com		84.21.172.159	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:51.378423929 CET	8.8.8.8	192.168.2.5	0x417e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:52.380325079 CET	8.8.8.8	192.168.2.5	0x417e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:53.396895885 CET	8.8.8.8	192.168.2.5	0x417e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- dkkgeh.net
  - host-file-host6.com

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **5996**, Parent PID: **3324**

General

Target ID:	0
Start time:	20:12:55
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	4AE4A84EBA3264C433E0C1B92594C61B
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: 00000000.00000002.371278858.00000000022A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.371278858.00000000022A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.292353244.0000000000800000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.371129358.00000000007E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.371194689.0000000000800000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.371194689.0000000000800000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.371011318.00000000006E8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3324**, Parent PID: **5996**

General

Target ID:	1
Start time:	20:13:02
Start date:	24/11/2022
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: 00000001.00000000.352581275.0000000002901000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.352581275.0000000002901000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vvtsewb	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	2901F42	CopyFileW
C:\Users\user\AppData\Roaming\vvtsewb\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2901F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	2901F53	DeleteFileW
C:\Users\user\AppData\Roaming\vvtsewb:Zone.Identifier	success or wait	1	2901F9E	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\vvtsewb	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 57 fd fd fd 13 cf fd 13 cf fd 13 cf fd fd fd 19 fd 12 cf fd 0d fd 1a fd 0c cf fd 0d fd 0c fd fd cf fd 34 11 fd fd 1a cf fd 13 ce fd fd cf fd 0d fd 0b fd 3d cf fd 0d fd 1b fd 12 cf fd 0d fd 1e fd 12 cf fd 52 69 63 68 13 cf fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 2e 2e 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$W4=RichPEL..a	success or wait	2	2901F42	CopyFileW
C:\Users\user\AppData\Roaming\vvtsewb: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	2901F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vvtsewb PID: **5936**, Parent PID: **1084**

General

Target ID:	2
Start time:	20:13:46
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Roaming\vvtsewb
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vvtsewb
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	4AE4A84EBA3264C433E0C1B92594C61B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000002.00000002.412766859.00000000007B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.412803739.00000000007E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000002.00000002.412803739.00000000007E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000002.00000002.413033982.00000000009D8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.412778372.00000000007C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000002.00000002.412778372.00000000007C0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000003.401198999.00000000007C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Disassembly

No disassembly