ID: 715074
Sample Name: file.exe
Cookbook: default.jbs
Time: 15:57:31
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

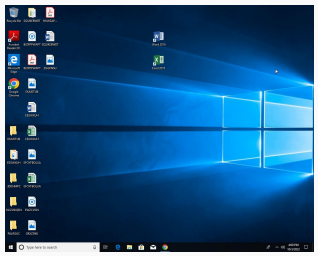
Windows Analysis Report

file.exe

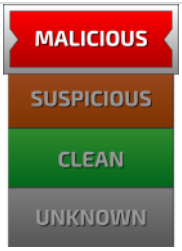
Overview

General Information

Sample Name:	file.exe
Analysis ID:	715074
MD5:	e337a4d30d5b3c..
SHA1:	739b485a3633b5..
SHA256:	bddb07a1bc6effa..
Tags:	exe SmokeLoader
Infos:	



Detection



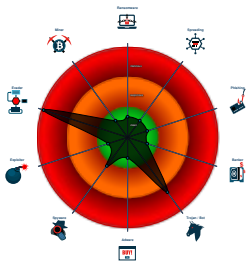
SmokeLoader

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
- 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

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5624 cmdline: C:\Users\user\Desktop\file.exe MD5: E337A4D30D5B3CC3BCF3D3789DAD3566)
  - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- vbfvrba (PID: 4616 cmdline: C:\Users\user\AppData\Roaming\vbfvrba MD5: E337A4D30D5B3CC3BCF3D3789DAD3566)
- vbfvrba (PID: 3312 cmdline: C:\Users\user\AppData\Roaming\vbfvrba MD5: E337A4D30D5B3CC3BCF3D3789DAD3566)
- **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
0000000E.00000002.458450131.00000000005B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000E.00000002.458450131.00000000005B0000.00000004.00000800.00020000.00000000.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

Source	Rule	Description	Author	Strings
0000000E.00000003.446586296.00000000005B0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.377030181.00000000021F0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.377030181.00000000021F0000.00000004.00000800.00020000.00000000.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 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.vbfvrba.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.3.vbfvrba.5b0000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.2.vbfvrba.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	
14.2.vbfvrba.5a0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 4 entries				

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

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

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

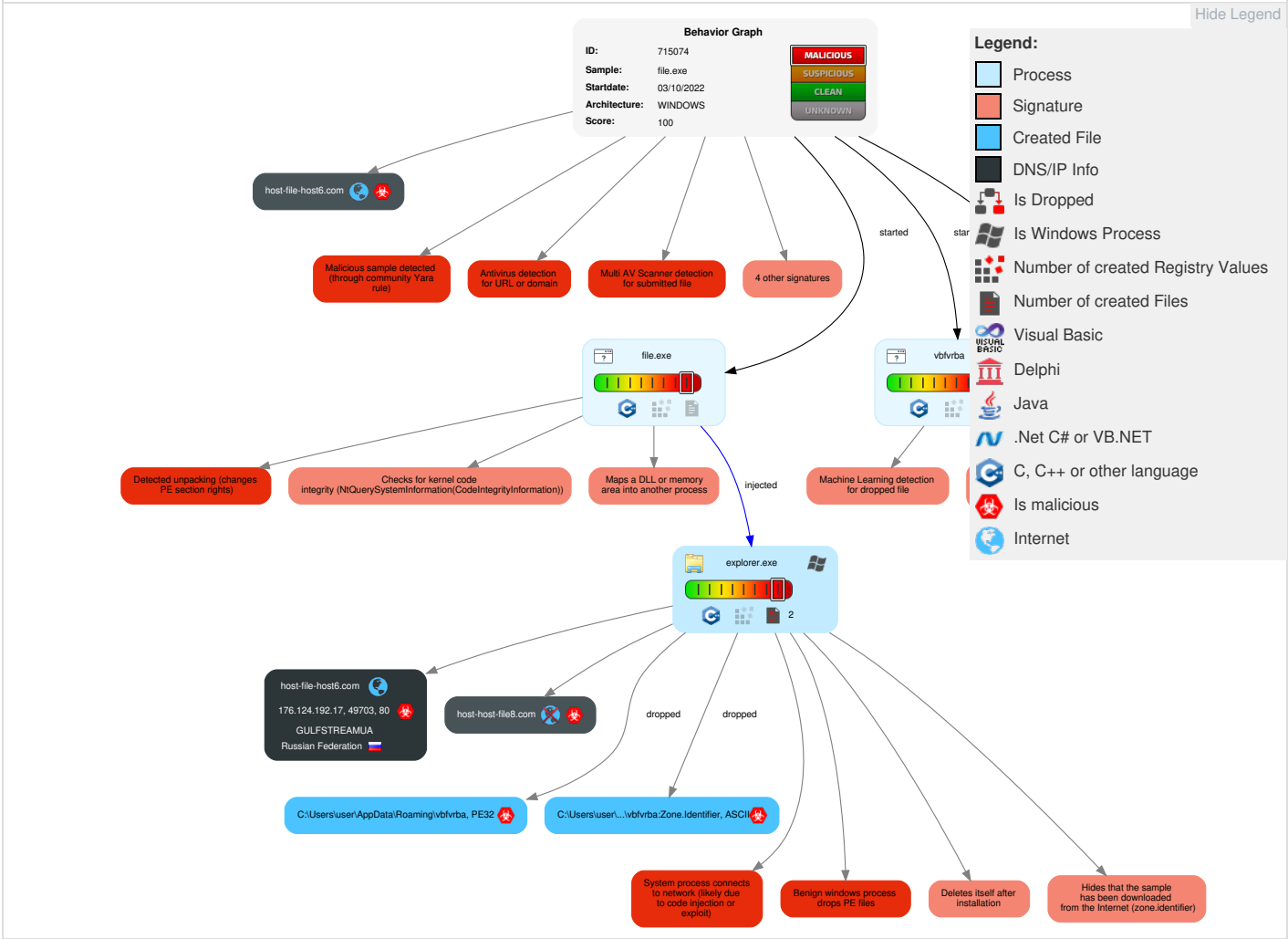
Yara detected SmokeLoader

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	1 Exploitation for Client Execution	1 DLL Side-Loading	3 2 Process Injection	1 1 Masquerading	1 Input Capture	3 1 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	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	Data from Removable Media	Exfiltration Over Bluetooth	1 1 2 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	Steganography	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
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	37%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
14.3.vbfvrba.5b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.vbfvrba.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.vbfvrba.6e0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.6b0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.file.exe.6c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.vbfvrba.21b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.vbfvrba.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.vbfvrba.5a0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.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

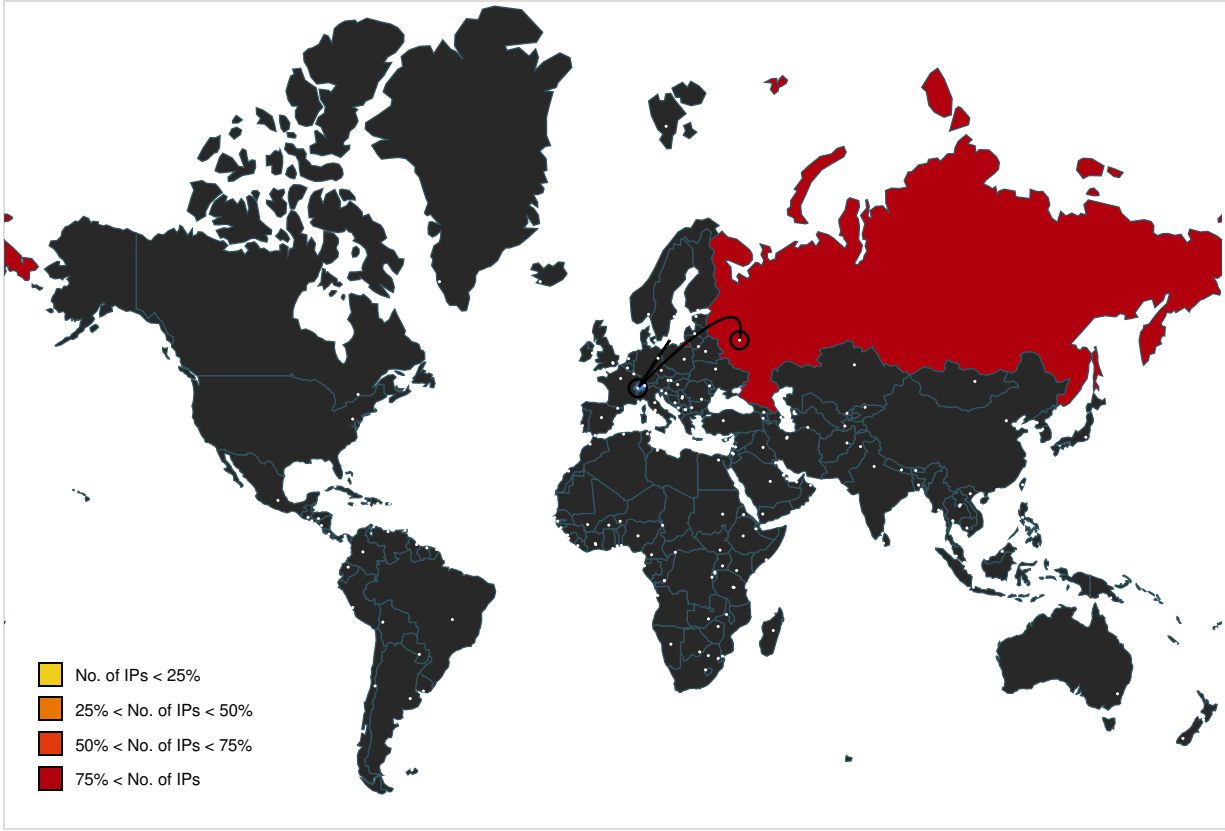
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	176.124.192.17	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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.124.192.17	host-file-host6.com	Russian Federation		59652	GULFSTREAMUA	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715074
Start date and time:	2022-10-03 15:57:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
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:	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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/2@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.8% (good quality ratio 24.4%) • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
15:59:22	Task Scheduler	Run new task: Firefox Default Browser Agent 937156EFB9A900F6 path: C:\Users\user\AppData\Roaming\vbfvrba

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\vbfvrba

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	150016
Entropy (8bit):	6.777924709615045
Encrypted:	false
SSDEEP:	3072:0jiakzWt9fGfGXLHuAr+ax7OwtUqzxsaCCSSbO:0j8qbHbKItdWaLV
MD5:	E337A4D30D5B3CC3BCF3D3789DAD3566
SHA1:	739B485A3633B500C43320E98488538C0BDA3106
SHA-256:	BDDB07A1BC6EFFA8751CE6B40FC5E86F6C31F0B2403E696C99B522D89DD179DD
SHA-512:	6C054CFC49CBADF90850F15CF7B6DFE3D801EEFD55E017F212B261FB3E03C4BB37EE94F0B31C2983EE3FC00BE32E90B2642994F24B05D4AA7D8E140EC79205B1

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L...4..`.....6.....L.....@.....y.....P.....K.....0,..@..... ...text..... ..`.data.....@....rsrc....K.....L.....@..@..... ....

C:\Users\user\AppData\Roaming\vbfvrba: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):	6.777924709615045
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:	150016
MD5:	e337a4d30d5b3cc3bcf3d3789dad3566
SHA1:	739b485a3633b500c43320e98488538c0bda3106
SHA256:	bddb07a1bc6effa8751ce6b40fc5e86f6c31f0b2403e696c99b522d89dd179dd
SHA512:	6c054cfc49cbadf90850f15cf7b6dfe3d801eefd55e017f212b261fb3e03c4bb37ee94f0b31c2983ee3fc00be32e90b2642994f24b05d4aa7d8e140ec79205b1
SSDEEP:	3072:0jiakzWt9fGfGXLHuAr+ax7OwtUqzxsaCCSSbO:0j8qbHbKItdWaLV
TLSH:	6AE3DF2139A0C473C616CA710874D964BB3FF9926B3985477B8C2B2D0F713D25EBA35A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich.....PE..L...4..`.....6.....

File Icon

Icon Hash:	32f2c4ccccc692a0

Static PE Info

General

Entrypoint:	0x404c07
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x60C1FF34 [Thu Jun 10 12:01:56 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:	2d5ec24fb9d2ee4cf8208f9e16125d4f

Entrypoint Preview
Instruction
call 00007F4DC8D091DBh
jmp 00007F4DC8D05D6Dh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F4DC8D05F16h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F4DC8D05F40h
test ecx, 00000003h
jne 00007F4DC8D05EE1h
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 00007F4DC8D05EDAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F4DC8D05F24h
test ah, ah
je 00007F4DC8D05F16h
test eax, 00FF0000h
je 00007F4DC8D05F05h
test eax, FF000000h

Instruction
je 00007F4DC8D05EF4h
jmp 00007F4DC8D05EBFh
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 [0042006Ch]
jne 00007F4DC8D05EF4h
rep ret
jmp 00007F4DC8D091C3h
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

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	0xe10c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17c000	0x4bf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1210	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	0x2c30	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.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	0xdc06	0xde00	False	0.48134853603603606	data	5.874806872478882	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xf000	0x16c2fc	0x11c00	False	0.8886168573943662	data	7.587752029512684	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x17c000	0x4bf8	0x4c00	False	0.47774465460526316	data	4.668681479659218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17c2b0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x17cb58	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x17f100	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_STRING	0x1803a8	0x42	data		
RT_STRING	0x1803f0	0x280	data		
RT_STRING	0x180670	0x3ce	data		
RT_STRING	0x180a40	0x1b2	data		
RT_ACCELERATOR	0x1801d8	0x80	data		
RT_GROUP_ICON	0x1801a8	0x30	data		
RT_VERSION	0x180268	0x140	MIPSEB-LE MIPS-III ECOFF executable not stripped - version 0.79		
None	0x180258	0xa	data		

Imports

DLL	Import
KERNEL32.dll	LoadLibraryA, InterlockedPushEntrySList, GetConsoleAliasesW, ReadFile, ReadConsoleW, GetVolumeInformationA, GetComputerNameA, LocalFree, InterlockedDecrement, SetSystemTimeAdjustment, SetLocaleInfoA, FindNextVolumeA, FindCloseChangeNotification, CopyFileExA, MoveFileWithProgressW, VerifyVersionInfoW, LocalSize, FileTimeToDosDateTime, DebugBreak, GlobalGetAtomNameW, IsBadWritePtr, FindResourceA, GetComputerNameExW, GetProcAddress, GetStringTypeW, GetFileTime, GetConsoleAliasesLengthW, GetVolumeNameForVolumeMountPointA, DeleteVolumeMountPointA, GetCPInfo, PostQueuedCompletionStatus, MoveFileWithProgressA, CopyFileA, lstrcpynW, WriteConsoleW, GetBinaryTypeA, WriteConsoleOutputW, GetCommandLineA, InterlockedIncrement, CreateActCtxW, FormatMessageA, GetModuleHandleW, GetModuleHandleA, LeaveCriticalSection, GetStringTypeExA, OpenMutexW, FindResourceW, RtlCaptureContext, InterlockedExchange, InitializeCriticalSectionAndSpinCount, DeleteFiber, InterlockedExchangeAdd, EnumDateFormatsA, GetPrivateProfileStructA, GetNamedPipeHandleStateW, RegisterWaitForSingleObject, LocalAlloc, QueryMemoryResourceNotification, SetLastError, GetProcessPriorityBoost, GetMailslotInfo, HeapWalk, SetFilePointer, SetConsoleMode, RaiseException, RtlUnwind, GetLastError, MoveFileA, DeleteFileA, GetStartupInfoA, HeapAlloc, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, EnterCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, LCMapStringA, LCMapStringW
USER32.dll	CharUpperBuffW
WINHTTP.dll	WinHttpCreateUrl

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:59:23.101623058 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.158726931 CEST	80	49703	176.124.192.17	192.168.2.7
Oct 3, 2022 15:59:23.158838034 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.158982992 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.159025908 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.215492964 CEST	80	49703	176.124.192.17	192.168.2.7
Oct 3, 2022 15:59:23.215522051 CEST	80	49703	176.124.192.17	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:59:23.225384951 CEST	80	49703	176.124.192.17	192.168.2.7
Oct 3, 2022 15:59:23.225481987 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.227018118 CEST	49703	80	192.168.2.7	176.124.192.17
Oct 3, 2022 15:59:23.283112049 CEST	80	49703	176.124.192.17	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:59:22.755625010 CEST	59477	53	192.168.2.7	8.8.8.8
Oct 3, 2022 15:59:23.084805012 CEST	53	59477	8.8.8.8	192.168.2.7
Oct 3, 2022 15:59:23.237786055 CEST	55752	53	192.168.2.7	8.8.8.8
Oct 3, 2022 15:59:24.234636068 CEST	55752	53	192.168.2.7	8.8.8.8
Oct 3, 2022 15:59:25.265894890 CEST	55752	53	192.168.2.7	8.8.8.8
Oct 3, 2022 15:59:27.263375998 CEST	53	55752	8.8.8.8	192.168.2.7
Oct 3, 2022 15:59:28.261560917 CEST	53	55752	8.8.8.8	192.168.2.7
Oct 3, 2022 15:59:29.293272972 CEST	53	55752	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 3, 2022 15:59:28.261730909 CEST	192.168.2.7	8.8.8.8	cffa	(Port unreachable)	Destination Unreachable
Oct 3, 2022 15:59:29.293365955 CEST	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
Oct 3, 2022 15:59:22.755625010 CEST	192.168.2.7	8.8.8.8	0x1f55	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:23.237786055 CEST	192.168.2.7	8.8.8.8	0xb9d5	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:24.234636068 CEST	192.168.2.7	8.8.8.8	0xb9d5	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:25.265894890 CEST	192.168.2.7	8.8.8.8	0xb9d5	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
Oct 3, 2022 15:59:23.084805012 CEST	8.8.8.8	192.168.2.7	0x1f55	No error (0)	host-file-host6.com		176.124.192.17	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:27.263375998 CEST	8.8.8.8	192.168.2.7	0xb9d5	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:28.261560917 CEST	8.8.8.8	192.168.2.7	0xb9d5	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:59:29.293272972 CEST	8.8.8.8	192.168.2.7	0xb9d5	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ucdldn.net
  - host-file-host6.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49703	176.124.192.17	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:23.158982992 CEST	103	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ucdldn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 334 Host: host-file-host6.com
Oct 3, 2022 15:59:23.225384951 CEST	104	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Mon, 03 Oct 2022 13:59:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Data Raw: 66 0d 0a 59 6f 75 72 20 49 50 20 62 6c 6f 63 6b 65 64 0d 0a 30 0d 0a 0d 0a Data Ascii: fYour IP blocked0

Statistics

Behavior

System Behavior

Analysis Process: file.exe PID: **5624**, Parent PID: **3320**

General

Target ID:	0
Start time:	15:58:26
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	150016 bytes
MD5 hash:	E337A4D30D5B3CC3BCF3D3789DAD3566
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.327668635.00000000006B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.243844808.00000000006C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.327792065.0000000000860000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.327792065.0000000000860000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.327934318.00000000008BA000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.327822813.0000000000881000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.327822813.0000000000881000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3320**, Parent PID: **5624**

General

Target ID:	1
Start time:	15:58:34
Start date:	03/10/2022
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
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.316092532.0000000002671000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.316092532.0000000002671000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vbfvrba	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	2671F42	CopyFileW
C:\Users\user\AppData\Roaming\vbfvrba\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2671F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	2671F53	DeleteFileW
C:\Users\user\AppData\Roaming\vbfvrba:Zone.Identifier	success or wait	1	2671F9E	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\vbfvrba	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 fd 7d 9f fd 1c fd fd fd 1c fd fd fd 1c fd fd fd 4e 31 fd fd 1c fd fd fd 4e 27 16 1c fd fd fd fd fd fd fd 1c fd fd fd 1c fd fd 44 1c fd fd fd 4e 20 fd fd 1c fd fd fd 4e 30 fd fd 1c fd fd fd 4e 35 fd fd 1c fd fd 52 69 63 68 fd 1c fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 34 fd fd 60 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 00 00 00 36 17 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$}N1N'DN N0N5RichPEL4`6	success or wait	2	2671F42	CopyFileW
C:\Users\user\AppData\Roaming\vbfvrba: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	2671F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbfvrba

PID: **4616**, Parent PID: **1100**

General

Target ID:	11
Start time:	15:59:22
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\vbfvrba
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vbfvrba
Imagebase:	0x400000
File size:	150016 bytes
MD5 hash:	E337A4D30D5B3CC3BCF3D3789DAD3566
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: 0000000B.00000002.377030181.00000000021F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.377030181.00000000021F0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.364685451.00000000021B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.376837614.00000000006E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.377400822.0000000002231000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.377400822.0000000002231000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.376742347.00000000005E9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: vbfvrba

PID: **3312**, Parent PID: **1100**

General	
Target ID:	14
Start time:	16:00:01
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\vbfvrba
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vbfvrba
Imagebase:	0x400000
File size:	150016 bytes
MD5 hash:	E337A4D30D5B3CC3BCF3D3789DAD3566
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: 0000000E.00000002.458450131.00000000005B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000E.00000002.458450131.00000000005B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000003.446586296.00000000005B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000E.00000002.458435299.00000000005A0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.458781769.00000000021D1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000E.00000002.458781769.00000000021D1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000E.00000002.458600340.00000000005EE000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly