



ID: 764039
Sample Name: file.exe
Cookbook: default.jbs
Time: 10:55:09
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: SmokeLoader 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 5
System Summary 5
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Roaming\rudwagu 11
C:\Users\user\AppData\Roaming\rudwagu:Zone.Identifier 12
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 13
Rich Headers 14
Data Directories 14
Sections 14
Resources 15
Imports 16
Possible Origin 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 17
ICMP Packets 17

Copyright Joe Security LLC 2022

DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 17
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: file.exePID: 5164, Parent PID: 3452 18
General 18
Analysis Process: file.exePID: 6088, Parent PID: 5164 18
General 18
Analysis Process: explorer.exePID: 3452, Parent PID: 6088 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
Analysis Process: rudwaguPID: 5400, Parent PID: 1064 20
General 20
Analysis Process: rudwaguPID: 1324, Parent PID: 5400 20
General 20
Disassembly 21

Copyright Joe Security LLC 2022

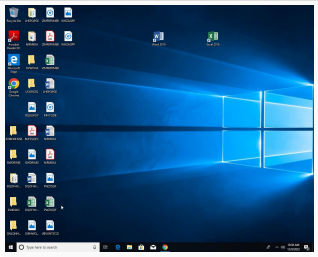
Windows Analysis Report

file.exe

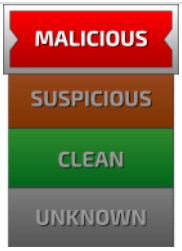
Overview

General Information

Sample Name:	file.exe
Analysis ID:	764039
MD5:	0d810e582a95de.
SHA1:	486a963c02b9e7..
SHA256:	c57cafedd2e461...
Tags:	exe
Infos:	



Detection



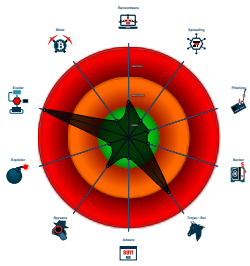
SmokeLoader

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...
- Injects a PE file into a foreign proce...
- Checks for kernel code integrity (NtQ...
- Contains functionality to inject code...
- Deletes itself after installation

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5164 cmdline: C:\Users\user\Desktop\file.exe MD5: 0D810E582A95DEBFF5E1A72A76C602C9)
  - file.exe (PID: 6088 cmdline: C:\Users\user\Desktop\file.exe MD5: 0D810E582A95DEBFF5E1A72A76C602C9)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- rudwagu (PID: 5400 cmdline: C:\Users\user\AppData\Roaming\rudwagu MD5: 0D810E582A95DEBFF5E1A72A76C602C9)
  - rudwagu (PID: 1324 cmdline: C:\Users\user\AppData\Roaming\rudwagu MD5: 0D810E582A95DEBFF5E1A72A76C602C9)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.344568009.0000000000420000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.344568009.0000000000420000.00000004.00000800.00020000.00000000.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

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
0000000B.00000002.408393791.00000000004E1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.408393791.00000000004E1000.00000004.10000000.00040000.00000000.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
0000000B.00000002.408296472.00000000004A0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.2.rudwagu.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.0.rudwagu.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
10.2.rudwagu.6e15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
11.0.rudwagu.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 2 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)

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

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information



Yara detected SmokeLoader

Remote Access Functionality



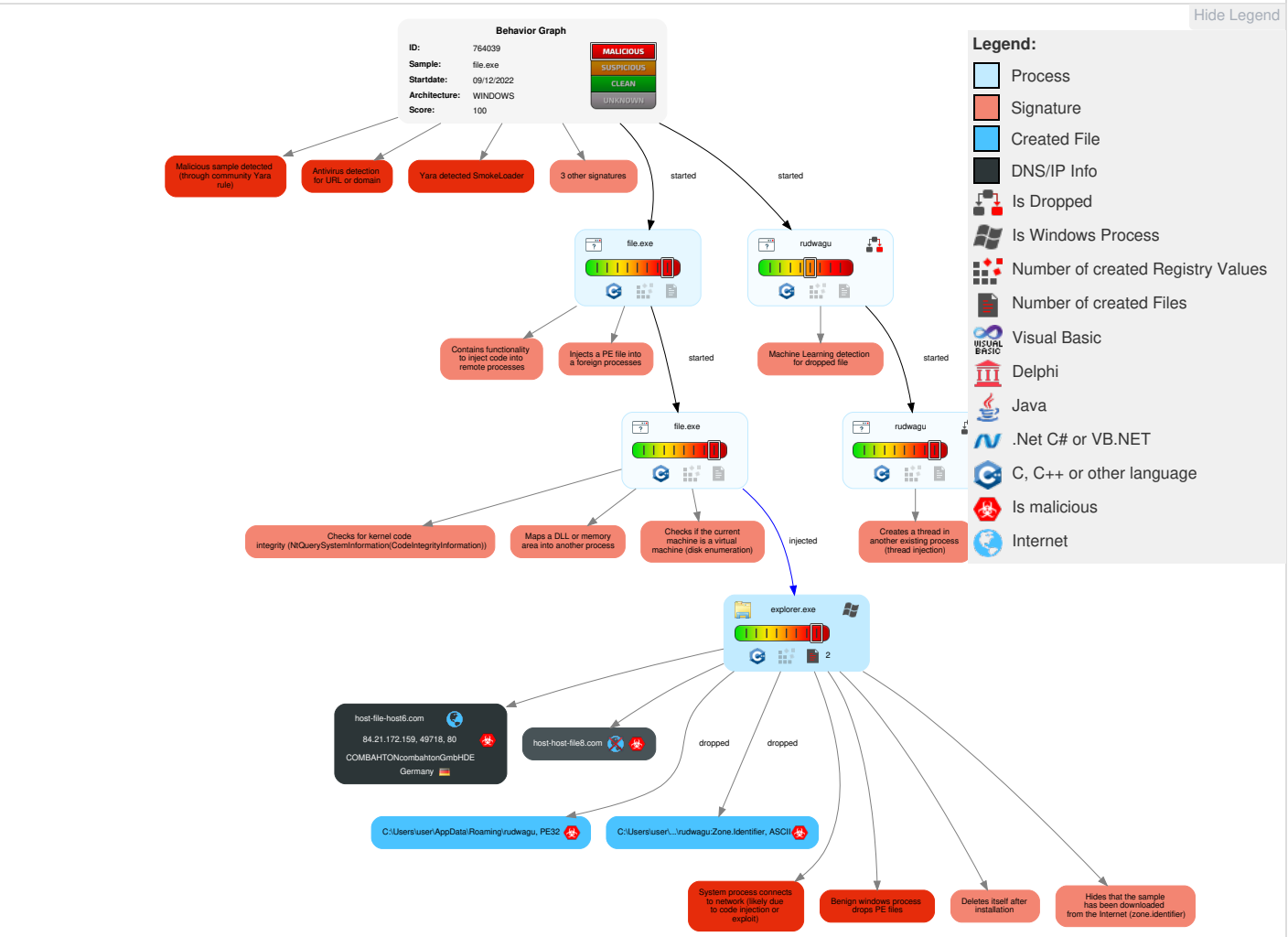
Yara detected SmokeLoader

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	5 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)	5 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	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	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

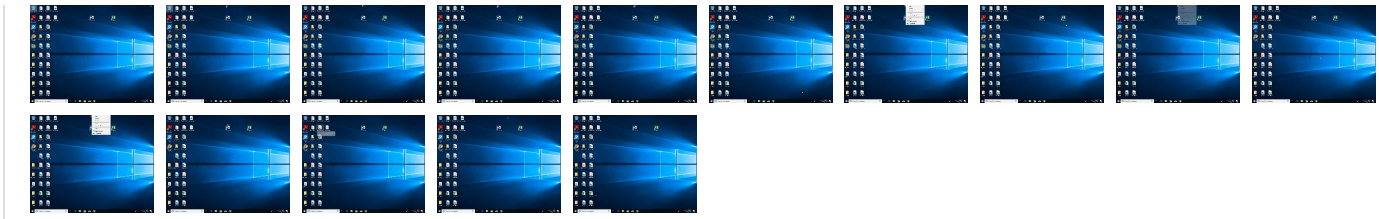


Screenshots

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\rudwagu	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.file.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
11.0.rudwagu.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rudwagu.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rudwagu.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.rudwagu.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.rudwagu.6e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rudwagu.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.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
11.0.rudwagu.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rudwagu.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.file.exe.8e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rudwagu.400000.2.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

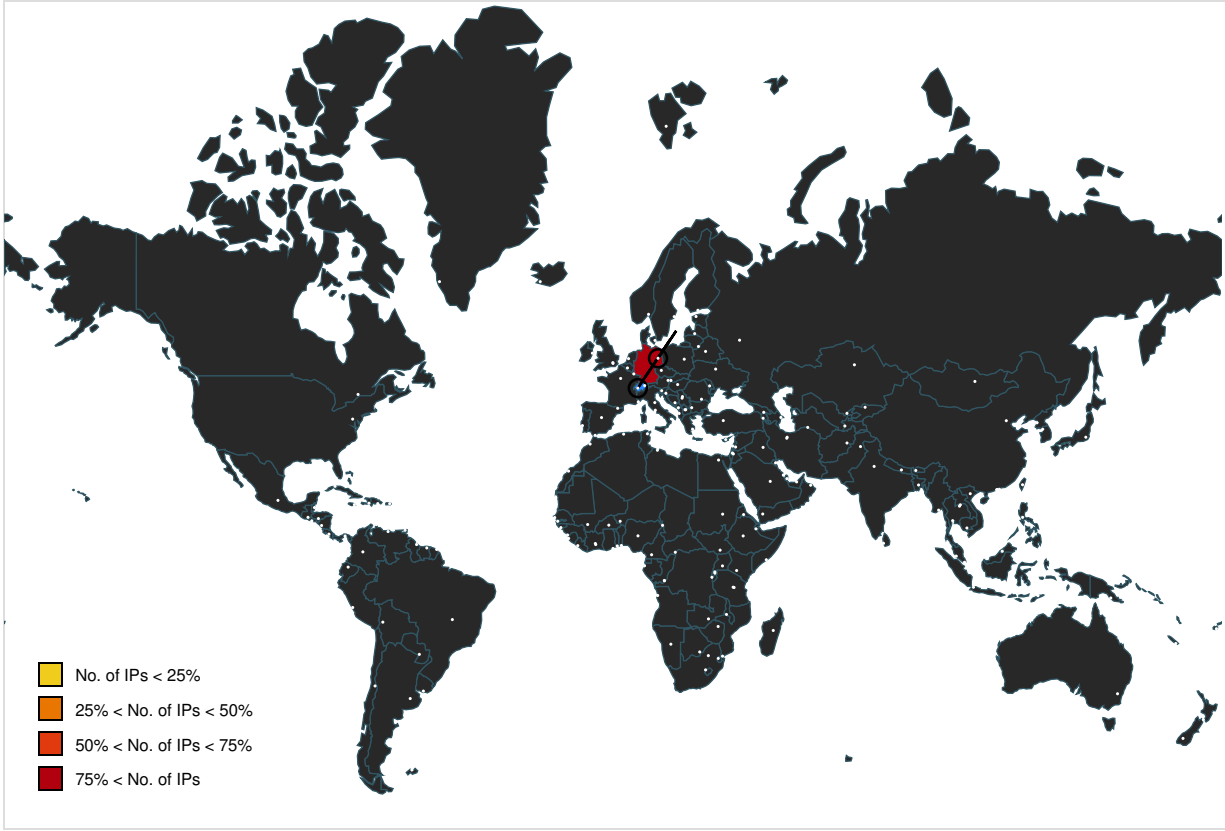
Contacted URLs

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
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.29980367 1.0000000000AC8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 002.00000000.329320639.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.259861471.0000000 0000AC8000.00000004.00000020.00020000.00 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:	764039
Start date and time:	2022-12-09 10:55:09 +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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
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: 91% (good quality ratio 83.5%) • Quality average: 71.6% • Quality standard deviation: 31.8%

Copyright Joe Security LLC 2022

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): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, cdn.onenote.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
10:57:01	Task Scheduler	Run new task: Firefox Default Browser Agent 635557CDEDEC7374 path: C:\Users\user\AppData\Roaming\rudwagu

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\rudwagu

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	391680
Entropy (8bit):	5.905176085960016
Encrypted:	false
SSDEEP:	6144:rc/EL7Tgx5oWtxKD82s8hh6K9W9Ix5nKded89kTR:rXHTgvz/2TIK9W9Ix5nLaw
MD5:	0D810E582A95DEBFF5E1A72A76C602C9
SHA1:	486A963C02B9E7D5ECC2941C4DCB7F589954D7D7
SHA-256:	C57CAFEDD2E4617E24315CDE0DE7A6393610FB924E8BD4D3561EE3C4B2D90372
SHA-512:	FA74B3FBE4C9EEE7CF9FA8C27760E8315693380683A29BABEF33B30F6AD1FEAB670C6E2ABE92B5E0CBF9D44598C5ACD571A5C885D6DB7CA37C8947A01068D4E7

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.....@.....`.....Z.....s..<.....@..... ....0I..@.....text...Vm.....n..... ..`.data.....r.....@....lokeris.....p.....&.....@..@.zoyan..p.....2.....@..@.rsrc..... ...6.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Roaming\rudwagu: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):	5.905176085960016
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:	0d810e582a95debff5e1a72a76c602c9
SHA1:	486a963c02b9e7d5ecc2941c4dcb7f589954d7d7
SHA256:	c57cafedd2e4617e24315cde0de7a6393610fb924e8bd4d3561ee3c4b2d90372
SHA512:	fa74b3fbe4c9eee7cf9fa8c27760e8315693380683a29babef33b30f6ad1feab670c6e2abe92b5e0cbf9d44598c5acd571a5c885d6db7ca37c8947a01068d4e7
SSDEEP:	6144:rc/EL7Tgx5oWtxKD82s8hh6K9W9lx5nKded89kTR:rXHTgvz/2TIK9W9lx5nLaw
TLSH:	0384CF013195C8F2C7A20D774816CBF1EA3BB42BFB249927F7583B5F6EF22914562A05
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:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x622EE3A4 [Mon Mar 14 06:41:40 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 00007F3448BA22FCh
jmp 00007F3448B9C65Eh
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 [004432C4h], eax
je 00007F3448B9C7F0h
push dword ptr [00446268h]
call 00007F3448BA1228h
pop ecx
jmp 00007F3448B9C7E7h
mov eax, 0040CC48h
mov ecx, dword ptr [ebp+14h]
mov edx, 000000A6h
cmp ecx, edx
jg 00007F3448B9C95Ah
je 00007F3448B9C941h
cmp ecx, 19h
jg 00007F3448B9C8DEh
je 00007F3448B9C8CFh
mov edx, ecx
push 00000002h
pop ecx
sub edx, ecx
je 00007F3448B9C8B3h
dec edx
je 00007F3448B9C8A3h
sub edx, 05h
je 00007F3448B9C88Bh

Instruction
dec edx
je 00007F3448B9C86Ch
sub edx, 05h
je 00007F3448B9C853h
dec edx
je 00007F3448B9C827h
sub edx, 09h
jne 00007F3448B9C9BAh
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	0.5953295765027322	data	6.7023696076283805	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x18000	0x2e284	0x2b400	False	0.484662888367052	data	4.836772173500047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.lokeris	0x47000	0xbb8	0xc00	False	0.008138020833333334	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zoyan	0x48000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x49000	0x1a510	0x1a600	False	0.6376721712085308	data	6.242624809610504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x64000	0x1c12	0x1e00	False	0.3893229166666667	data	3.8825366238972383	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
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

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5edf0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Slovak	Slovakia
RT_STRING	0x62fc8	0x542	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



Total Packets: 10

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:02.208288908 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.234762907 CET	80	49718	84.21.172.159	192.168.2.6
Dec 9, 2022 10:57:02.234988928 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.237436056 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.237474918 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.264326096 CET	80	49718	84.21.172.159	192.168.2.6
Dec 9, 2022 10:57:02.354650021 CET	80	49718	84.21.172.159	192.168.2.6
Dec 9, 2022 10:57:02.354938984 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.357903957 CET	49718	80	192.168.2.6	84.21.172.159
Dec 9, 2022 10:57:02.386727095 CET	80	49718	84.21.172.159	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:57:02.137377977 CET	63229	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:57:02.156404972 CET	53	63229	8.8.8.8	192.168.2.6
Dec 9, 2022 10:57:02.368879080 CET	62538	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:57:03.383023024 CET	62538	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:57:04.449312925 CET	62538	53	192.168.2.6	8.8.8.8
Dec 9, 2022 10:57:06.409364939 CET	53	62538	8.8.8.8	192.168.2.6
Dec 9, 2022 10:57:07.409687996 CET	53	62538	8.8.8.8	192.168.2.6
Dec 9, 2022 10:57:08.477850914 CET	53	62538	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 9, 2022 10:57:07.412796974 CET	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Dec 9, 2022 10:57:08.478075027 CET	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:57:02.137377977 CET	192.168.2.6	8.8.8.8	0xe31c	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:02.368879080 CET	192.168.2.6	8.8.8.8	0x7334	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:03.383023024 CET	192.168.2.6	8.8.8.8	0x7334	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:04.449312925 CET	192.168.2.6	8.8.8.8	0x7334	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

DNS Answers

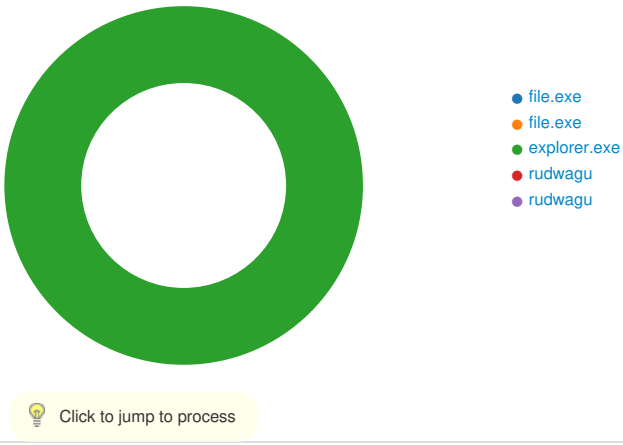
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:57:02.156404972 CET	8.8.8.8	192.168.2.6	0xe31c	No error (0)	host-file-host6.com		84.21.172.159	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:06.409364939 CET	8.8.8.8	192.168.2.6	0x7334	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:07.409687996 CET	8.8.8.8	192.168.2.6	0x7334	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:57:08.477850914 CET	8.8.8.8	192.168.2.6	0x7334	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- hhsselotxu.net
  - host-file-host6.com

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **5164**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:55:58
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:	0D810E582A95DEBFF5E1A72A76C602C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.248700871.0000000000573000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: file.exe PID: **6088**, Parent PID: **5164**

General

Target ID:	1
Start time:	10:56:04
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:	0D810E582A95DEBFF5E1A72A76C602C9
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: 00000001.00000002.344568009.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.344568009.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.344687233.0000000000521000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.344687233.0000000000521000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **6088**

General

Target ID:	2
Start time:	10:56:10
Start date:	09/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
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: 00000002.00000000.333482536.0000000004EC1000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000002.00000000.333482536.0000000004EC1000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rudwagu	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device | compressed	sequential only | non directory file	success or wait	1	4EC1F42	CopyFileW
C:\Users\user\AppData\Roaming\rudwagu\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device | compressed	sequential only | synchronous io non alert	success or wait	1	4EC1F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	4EC1F53	DeleteFileW
C:\Users\user\AppData\Roaming\rudwagu:Zone.Identifier	success or wait	1	4EC1F9E	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\rudwagu	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 00 40 00 00 00 00 00 00 00 00

File size:	391680 bytes
MD5 hash:	0D810E582A95DEBFF5E1A72A76C602C9
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.00000002.408393791.00000000004E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.408393791.00000000004E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.408296472.00000000004A0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.408296472.00000000004A0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly