

JoeSandbox Cloud BASIC



ID: 764038

Sample Name: file.exe

Cookbook: default.jbs

Time: 10:53:08

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	6
System Summary	6
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	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	10
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	12
C:\Users\user\AppData\Roaming\dubewge	12
C:\Users\user\AppData\Roaming\dubewge.Zone.Identifier	12
Static File Info	12
General	12
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	14
Data Directories	14
Sections	15
Resources	15
Imports	16
Possible Origin	16
Network Behavior	16
Snort IDS Alerts	16
Network Port Distribution	17
TCP Packets	17
UDP Packets	17

ICMP Packets	17
DNS Queries	17
DNS Answers	18
HTTP Request Dependency Graph	18
Statistics	18
Behavior	18
System Behavior	18
Analysis Process: file.exePID: 4700, Parent PID: 3324	19
General	19
Analysis Process: file.exePID: 3340, Parent PID: 4700	19
General	19
Analysis Process: explorer.exePID: 3324, Parent PID: 3340	19
General	19
File Activities	20
File Created	20
File Deleted	20
File Written	20
Analysis Process: dubewgePID: 5576, Parent PID: 1084	20
General	20
Analysis Process: dubewgePID: 4036, Parent PID: 5576	21
General	21
Disassembly	21

Windows Analysis Report

file.exe

Overview

General Information

Sample Name:

file.exe

Analysis ID:

764038

MD5:

6b8486d9065fb3..

SHA1:

b341177019c211..

SHA256:

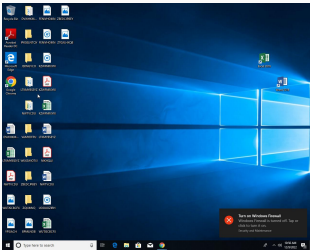
6acc6c36c8492b..

Tags:

exe

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

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

Multi AV Scanner detection for dom...

Snort IDS alert for network traffic

Maps a DLL or memory area into an...

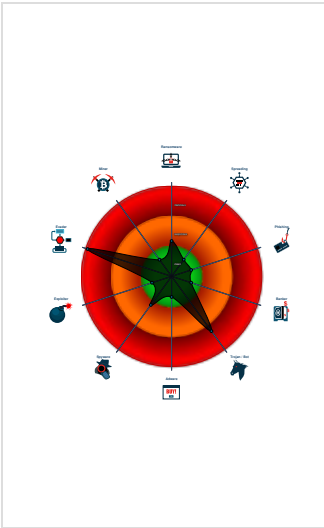
Tries to detect sandboxes and other...

Machine Learning detection for sam...

Injects a PE file into a foreign proce...

Checks for kernel code integrity (NtQ...

Classification



Process Tree

System is w10x64

file.exe (PID: 4700 cmdline: C:\Users\user\Desktop\file.exe MD5: 6B8486D9065FB3105E8C8A14C58DD0ED)

file.exe (PID: 3340 cmdline: C:\Users\user\Desktop\file.exe MD5: 6B8486D9065FB3105E8C8A14C58DD0ED)

explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)

dubewge (PID: 5576 cmdline: C:\Users\user\AppData\Roaming\dubewge MD5: 6B8486D9065FB3105E8C8A14C58DD0ED)

dubewge (PID: 4036 cmdline: C:\Users\user\AppData\Roaming\dubewge MD5: 6B8486D9065FB3105E8C8A14C58DD0ED)

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
00000002.00000000.377043487.0000000002971000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000002.00000000.377043487.0000000002971000.00000020.80000000.00040000.00000000.sdmp	Windows_Trojan_SmokeLoader_4e31426e	unknown	unknown	0x2f4:\$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0

Copyright Joe Security LLC 2022

Page 4 of 21

Source	Rule	Description	Author	Strings
00000006.00000002.453507425.0000000000460000.0000004.000000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000006.00000002.453507425.0000000000460000.0000004.000000800.00020000.00000000.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
00000001.00000002.389552753.00000000005A1000.0000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.file.exe.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.0.dubewge.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.0.file.exe.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.0.dubewge.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.4915a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 5 entries				

Sigma Signatures

 No Sigma rule has matched
--

Snort Signatures

ETPRO TROJAN Sharik/SmokeLoader CnC Beacon 18 - Source IP: 192.168.2.5 - Destination IP: 84.21.172.159	
Timestamp:	192.168.2.584.21.172.15949704802851815 12/09/22-10:55:01.226456
SID:	2851815
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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)
Snort IDS alert for network traffic
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



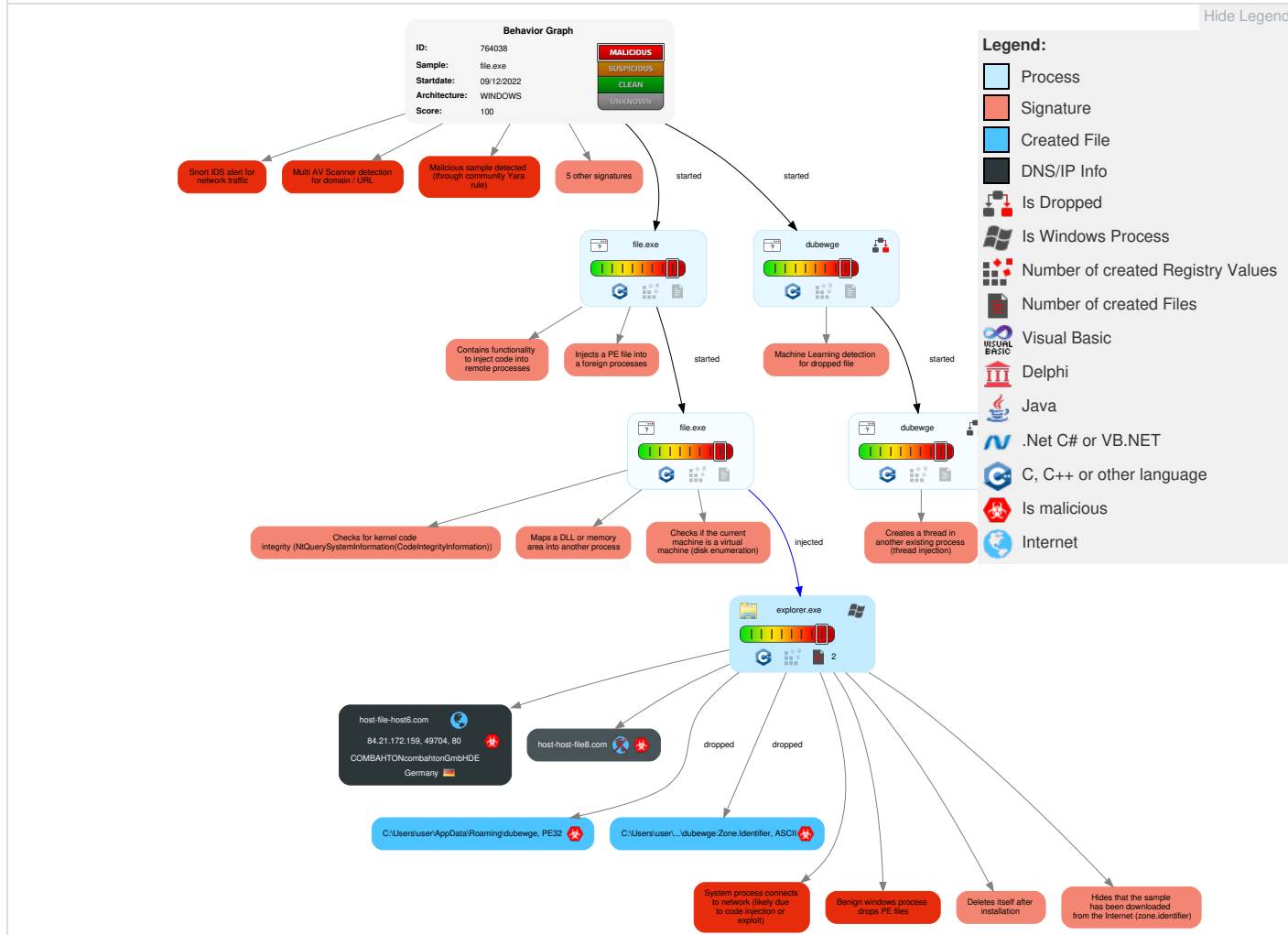
Yara detected SmokeLoader

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
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

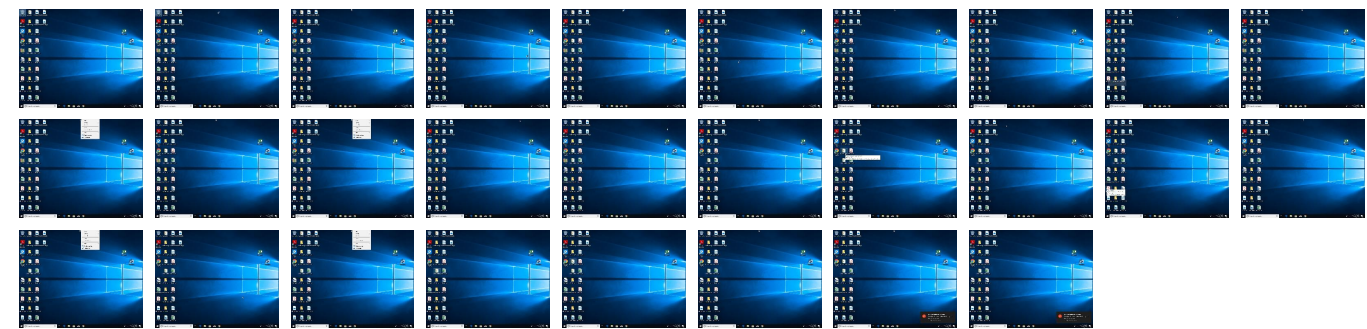
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



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\dubewge	100%	Joe Sandbox ML		

Unpacked PE Files					
Source	Detection	Scanner	Label	Link	Download
1.0.file.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.2.dubewge.400000.0.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.0.dubewge.400000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
1.0.file.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
6.0.dubewge.400000.6.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.0.dubewge.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
0.2.file.exe.4915a0.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
1.0.file.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
5.2.dubewge.7e15a0.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.0.dubewge.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.file.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.file.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.0.dubewge.400000.4.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
1.0.file.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.0.dubewge.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
6.0.dubewge.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File

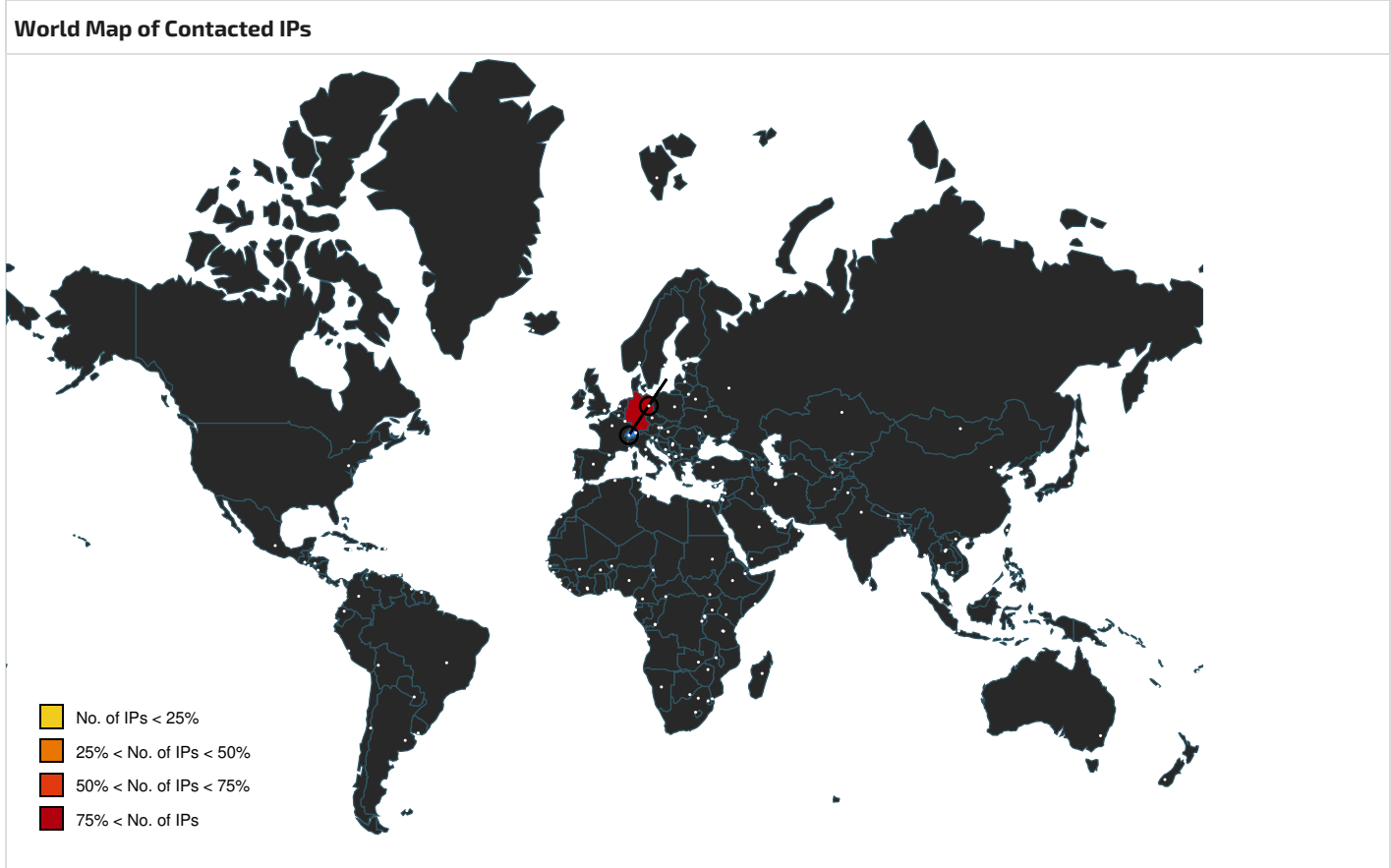
Domains				
Source	Detection	Scanner	Label	Link
host-file-host6.com	20%	Virustotal		Browse
host-host-file8.com	18%	Virustotal		Browse

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, 00000002.00000000.37609077 0.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 002.00000000.348098249.000000000091F000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.316275876.000000 000091F000.00000004.00000020.00020000.00 000000.sdmp	false		high



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:	764038
Start date and time:	2022-12-09 10:53:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
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:	8
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@5/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 91% (good quality ratio 83.5%) • Quality average: 71.6% • Quality standard deviation: 31.8%
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, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
10:55:00	Task Scheduler	Run new task: Firefox Default Browser Agent 0242EB7423704CDD path: C:\Users\user\AppData\Roaming\dubewge

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\dubewge  

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	391168
Entropy (8bit):	5.909021649149733
Encrypted:	false
SSDEEP:	6144:rOxLsKWxyoaRyxDnbHHawhh6K9W9ub8ded89kTt:rM4KWk0xD7pIK9W9Cac
MD5:	6B8486D9065FB3105E8C8A14C58DD0ED
SHA1:	B341177019C21155A02477B71A613B6C427CF067
SHA-256:	6ACC6C36C8492B91F4FE44AEABC3AD69EEA2765259108BACBFBC9B57BFF24133
SHA-512:	7CE1E07A979E4A65B6BC7C80178AA41E3845BBAF79B6685F1E07ECDCADC5EF5E556F6F48468B31F9D928F30B4F51AC138F012F85B31685AD3395A7C71A5F613
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\$%xC...C...C)..C...C...C...C.Rich...C.....PE..L.....`.....n.....p.....@.....`.....s.<.....@.....0l..@..text...Vm.....n.....`.data.....f.....@...weme.....p.....\$......@..@.hoseotp.....0.....@..@.rsrc.....4.....@..@.reloc.....@.....@..B.....

C:\Users\user\AppData\Roaming\dubewge: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]....Zoneld=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.909021649149733
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:	391168
MD5:	6b8486d9065fb3105e8c8a14c58dd0ed
SHA1:	b341177019c21155a02477b71a613b6c427cf067
SHA256:	6acc6c36c8492b91f4fe44aeabc3ad69eea2765259108bacbfbc9b57bff24133
SHA512:	7ce1e07a979e4a65b6bc7c80178aa41e3845bba79b6685f1e07ecdadc5ef5e556f6f48468b31f9d928f30b4f51ac138f012f85b31685ad3395a7c71a5f6f3
SSDEEP:	6144:rOxLsKWxyoaRyxDnbHHawhh6K9W9ub8ded89kTt:rM4KWk0xD7pIK9W9Cac
TLSH:	3B84CF013689CBF2C7234D778815CBE0DA3FB46AFA245927F35A3B6F6E703915662211

Instruction
mov ecx, dword ptr [ebp+14h]
mov edx, 000000A6h
cmp ecx, edx
jg 00007FDBF106CE7Ah
je 00007FDBF106CE61h
cmp ecx, 19h
jg 00007FDBF106CDEh
je 00007FDBF106CDEFh
mov edx, ecx
push 00000002h
pop ecx
sub edx, ecx
je 00007FDBF106CDD3h
dec edx
je 00007FDBF106CDC3h
sub edx, 05h
je 00007FDBF106CDABh
dec edx
je 00007FDBF106CD8Ch
sub edx, 05h
je 00007FDBF106CD73h
dec edx
je 00007FDBF106CD47h
sub edx, 09h
jne 00007FDBF106CEDAh
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	0.5951054474043715	data	6.700639978901342	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x18000	0x2e204	0x2b200	False	0.4851675724637681	data	4.842680156477422	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.weme	0x47000	0xbb8	0xc00	False	0.008138020833333334	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.hoseTot	0x48000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x49000	0x1a510	0x1a600	False	0.6376629146919431	data	6.2449814680641245	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0x1c12	0x1e00	False	0.3893229166666667	data	3.8827536368334243	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARD ABLE, 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

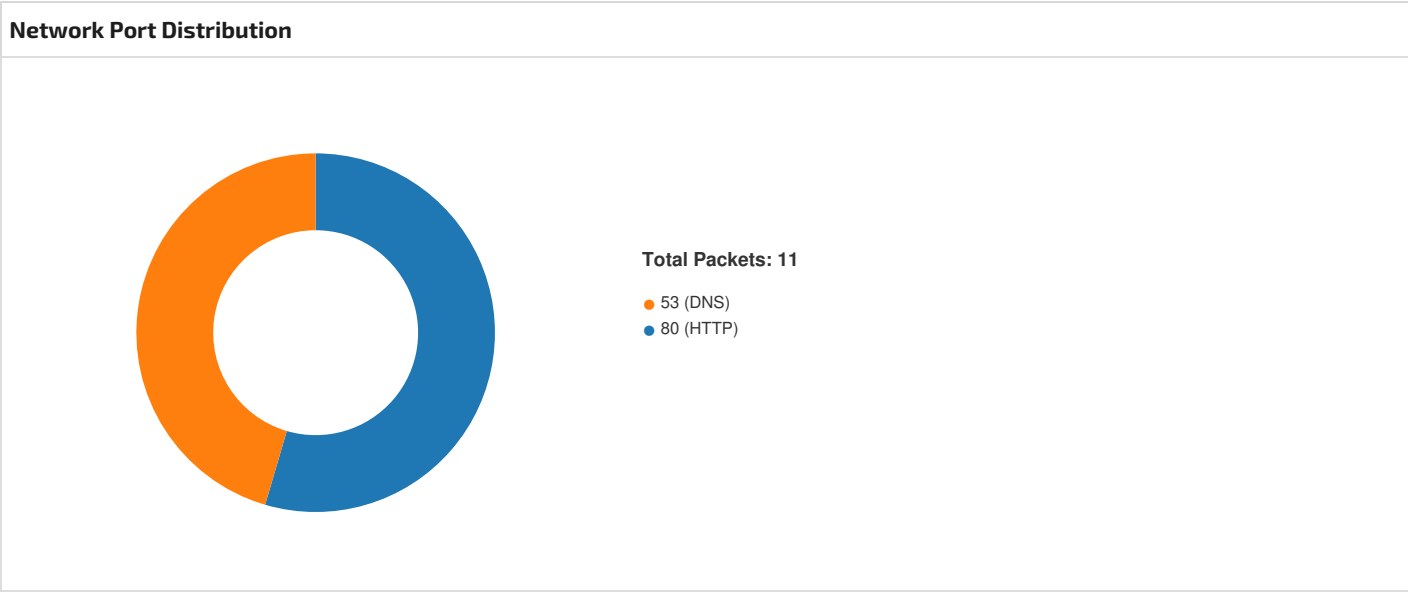
Name	RVA	Size	Type	Language	Country
RT_ICON	0x585c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Slovak	Slovakia
RT_ICON	0x58a98	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Slovak	Slovakia
RT_ICON	0x59940	0x8a8	Device independent 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
RT_ICON	0x5edf0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Slovak	Slovakia
RT_STRING	0x62fc8	0x546	data	Slovak	Slovakia
RT_ACCELERATOR	0x613d8	0x40	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x62ba8	0x22	data	Slovak	Slovakia
RT_GROUP_CURSOR	0x62db0	0x22	data	Slovak	Slovakia
RT_GROUP_ICON	0x58a30	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x4ca68	0x30	data	Slovak	Slovakia
RT_GROUP_ICON	0x52b90	0x68	data	Slovak	Slovakia
RT_GROUP_ICON	0x5f258	0x76	data	Slovak	Slovakia
RT_VERSION	0x62dd8	0x1f0	MS Windows COFF PowerPC object file	Slovak	Slovakia
None	0x61418	0xa	data	Slovak	Slovakia
None	0x61428	0xa	data	Slovak	Slovakia

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

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

Network Behavior
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.584.21.172.159 49704802851815 12/09/22- 10:55:01.226456	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49704	80	192.168.2.5	84.21.172.159



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:55:01.199026108 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.226083994 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:55:01.226320982 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.226455927 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.226455927 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.253685951 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:55:01.344106913 CET	80	49704	84.21.172.159	192.168.2.5
Dec 9, 2022 10:55:01.344264030 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.347003937 CET	49704	80	192.168.2.5	84.21.172.159
Dec 9, 2022 10:55:01.374615908 CET	80	49704	84.21.172.159	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:55:00.849432945 CET	49177	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:55:01.192933083 CET	53	49177	8.8.8.8	192.168.2.5
Dec 9, 2022 10:55:01.355135918 CET	49724	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:55:02.354784966 CET	49724	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:55:03.370491982 CET	49724	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:55:05.354854107 CET	49724	53	192.168.2.5	8.8.8.8
Dec 9, 2022 10:55:05.385504961 CET	53	49724	8.8.8.8	192.168.2.5
Dec 9, 2022 10:55:07.385929108 CET	53	49724	8.8.8.8	192.168.2.5
Dec 9, 2022 10:55:07.398686886 CET	53	49724	8.8.8.8	192.168.2.5
Dec 9, 2022 10:55:09.381998062 CET	53	49724	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 9, 2022 10:55:07.386039972 CET	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
Dec 9, 2022 10:55:09.382101059 CET	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Checksum	Code	Type
-----------	-----------	---------	----------	------	------

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:55:00.849432945 CET	192.168.2.5	8.8.8.8	0xed9c	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:01.355135918 CET	192.168.2.5	8.8.8.8	0x1589	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:02.354784966 CET	192.168.2.5	8.8.8.8	0x1589	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:03.370491982 CET	192.168.2.5	8.8.8.8	0x1589	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:05.354854107 CET	192.168.2.5	8.8.8.8	0x1589	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 10:55:01.192933083 CET	8.8.8.8	192.168.2.5	0xed9c	No error (0)	host-file-host6.com		84.21.172.159	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:05.385504961 CET	8.8.8.8	192.168.2.5	0x1589	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:07.385929108 CET	8.8.8.8	192.168.2.5	0x1589	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:07.398686886 CET	8.8.8.8	192.168.2.5	0x1589	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:55:09.381998062 CET	8.8.8.8	192.168.2.5	0x1589	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph										
- quargeql.com - host-file-host6.com										

Statistics

Behavior



file.exe

file.exe

explorer.exe

dubewge

dubewge

Click to jump to process

Analysis Process: file.exe PID: 4700, Parent PID: 3324**General**

Target ID:	0
Start time:	10:54:00
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:	391168 bytes
MD5 hash:	6B8486D9065FB3105E8C8A14C58DD0ED
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: 00000000.00000002.305126000.0000000000603000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: file.exe PID: 3340, Parent PID: 4700**General**

Target ID:	1
Start time:	10:54:05
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	391168 bytes
MD5 hash:	6B8486D9065FB3105E8C8A14C58DD0ED
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: 00000001.00000002.389552753.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_SmokeLoader_4e31426e, Description: unknown, Source: 00000001.00000002.389552753.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.389415953.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_SmokeLoader_4e31426e, Description: unknown, Source: 00000001.00000002.389415953.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3324, Parent PID: 3340**General**

Target ID:	2
Start time:	10:54:11
Start date:	09/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	- Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000000.377043487.0000000002971000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_SmokeLoader_4e31426e, Description: unknown, Source: 00000002.00000000.377043487.0000000002971000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dubewge	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	2971F42	CopyFileW
C:\Users\user\AppData\Roaming\dubewge\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	2971F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	2971F53	DeleteFileW
C:\Users\user\AppData\Roaming\dubewge:Zone.Identifier	success or wait	1	2971F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dubewge	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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 47 fd 6d 10 03 fd 03 43 03 fd 03 43 03 fd 03 43 1d fd fd 43 28 fd 03 43 1d fd fd 43 19 fd 03 43 1d fd fd 43 fd fd 03 43 24 25 78 43 06 fd 03 43 03 fd 02 43 7d fd 03 43 1d fd fd 43 02 fd 03 43 1d fd fd 43 02 fd 03 43 1d fd fd 43 02 fd 03 43 52 69 63 68 03 fd 03 43 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd 60 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 6e 01	MZ@!L!This program cannot be run in DOS mode.\$GmCCCC(CCCC C\$% xCCC)CCCCCRRichCP EL`n	success or wait	3	2971F42	CopyFileW
C:\Users\user\AppData\Roaming\dubewge: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]Zoneld=0	success or wait	1	2971F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: dubewge PID: 5576, Parent PID: 1084

General

Target ID:	5
Start time:	10:55:00
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\dubewge

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\dubewge
Imagebase:	0x400000
File size:	391168 bytes
MD5 hash:	6B8486D9065FB3105E8C8A14C58DD0ED
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.437430133.0000000000492000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: dubewge PID: 4036, Parent PID: 5576

General

Target ID:	6
Start time:	10:55:06
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\dubewge
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\dubewge
Imagebase:	0x400000
File size:	391168 bytes
MD5 hash:	6B8486D9065FB3105E8C8A14C58DD0ED
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000002.453507425.0000000000460000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.453507425.0000000000460000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000002.453701840.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.453701840.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

 No disassembly