ID: 677968
Sample Name:
ofAn3uUEPe.exe
Cookbook: default.jbs
Time: 10:16:10
Date: 03/08/2022
Version: 35.0.0 Citrine

Table of Contents

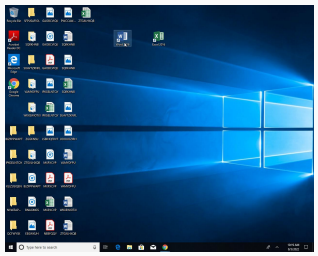
Windows Analysis Report

ofAn3uUEPe.exe

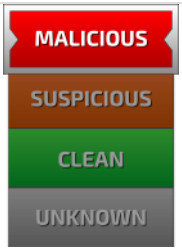
Overview

General Information

Sample Name:	ofAn3uUEPe.exe
Analysis ID:	677968
MD5:	db5723c9308cb9..
SHA1:	ee4130dcb4052d..
SHA256:	2d2bdc891614f5..
Tags:	ArkeiStealer exe
Infos:	



Detection



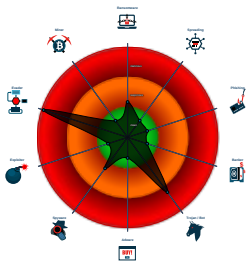
SmokeLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- 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**
- ofAn3uUEPe.exe (PID: 4496 cmdline: "C:\Users\user\Desktop\ofAn3uUEPe.exe" MD5: DB5723C9308CB986EAE4262297A51FA0)
  - ofAn3uUEPe.exe (PID: 500 cmdline: "C:\Users\user\Desktop\ofAn3uUEPe.exe" MD5: DB5723C9308CB986EAE4262297A51FA0)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- hbjebed (PID: 5008 cmdline: C:\Users\user\AppData\Roaming\hbjebed MD5: DB5723C9308CB986EAE4262297A51FA0)
  - hbjebed (PID: 4188 cmdline: C:\Users\user\AppData\Roaming\hbjebed MD5: DB5723C9308CB986EAE4262297A51FA0)
- **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
00000001.00000002.349529334.0000000001F61000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.349396035.0000000000580000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.406226962.0000000000420000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000005.00000000.328538195.0000000002701000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000012.00000002.406410596.0000000001F51000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.hbjebed.5515a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.ofAn3uUEPe.exe.6e15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
18.2.hbjebed.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.ofAn3uUEPe.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.4 - Destination IP: 34.118.39.10

Timestamp:	192.168.2.434.118.39.1049768802851815 08/03/22-10:18:21.517468
SID:	2851815
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- 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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

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

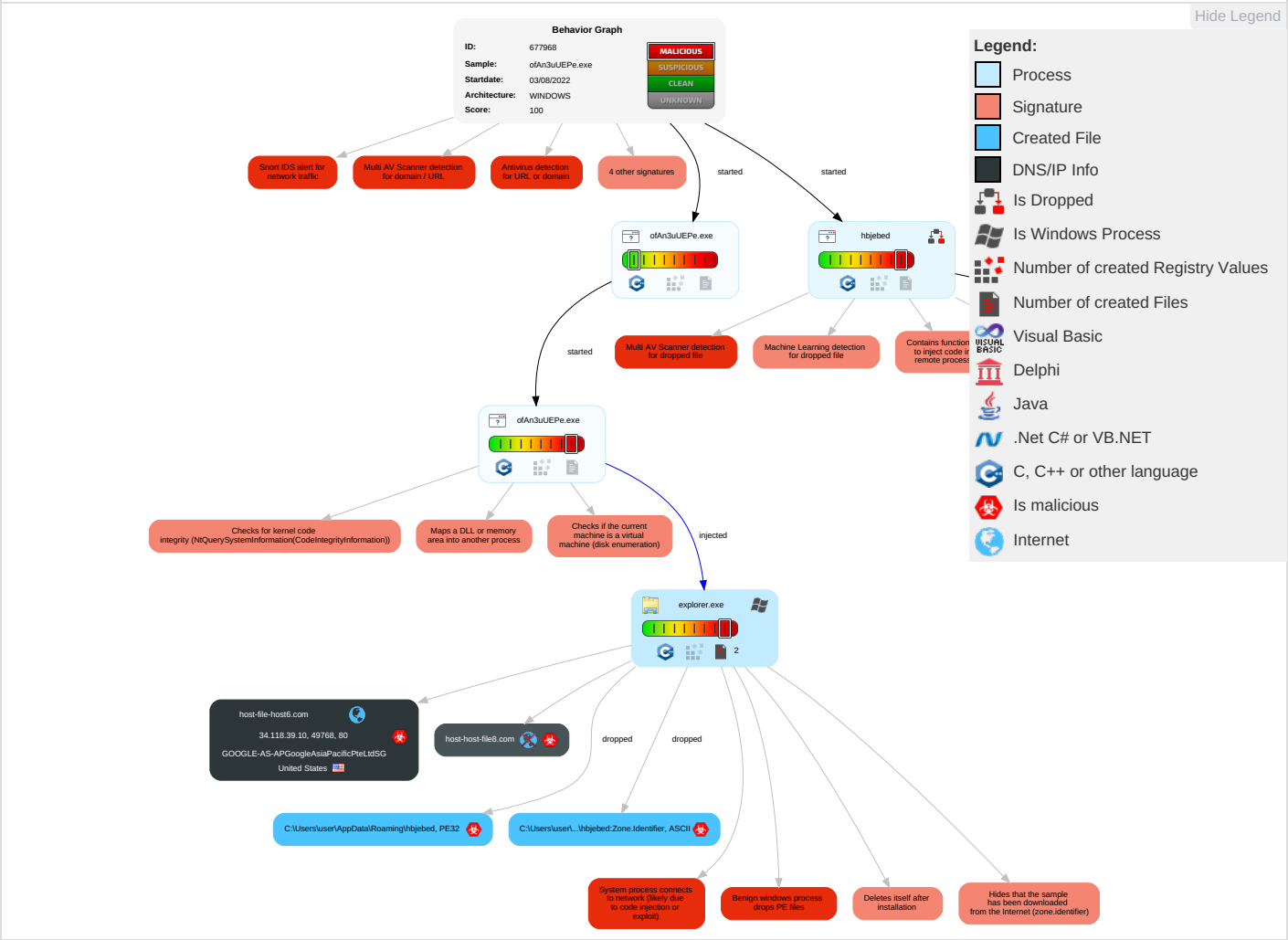
Yara detected SmokeLoader

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 3 Process Injection	1 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	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	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	5 1 3 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 5 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 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

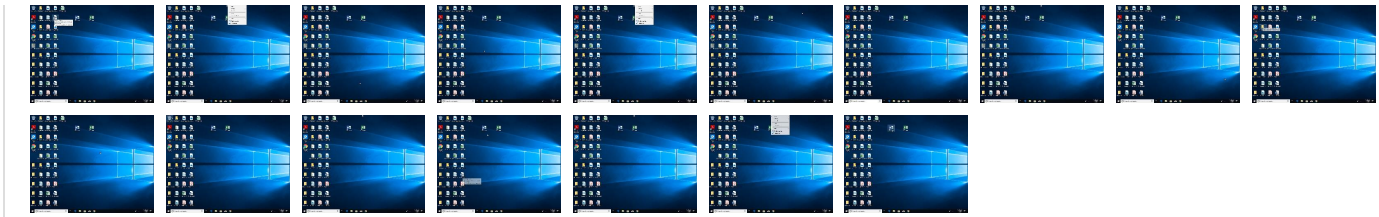
Behavior Graph



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
ofAn3uUEPe.exe	34%	Virustotal		Browse
ofAn3uUEPe.exe	48%	ReversingLabs	Win32.Ransomware.StopCrypt	
ofAn3uUEPe.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\hbjebed	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\hbjebed	34%	Virustotal		Browse
C:\Users\user\AppData\Roaming\hbjebed	48%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.ofAn3uUEPe.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.hbjebed.5515a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.ofAn3uUEPe.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.hbjebed.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.hbjebed.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.ofAn3uUEPe.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.hbjebed.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.ofAn3uUEPe.exe.6e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.ofAn3uUEPe.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.hbjebed.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dual-a-0001.dc-msedge.net	0%	Virustotal		Browse
host-file-host6.com	25%	Virustotal		Browse
host-host-file8.com	22%	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

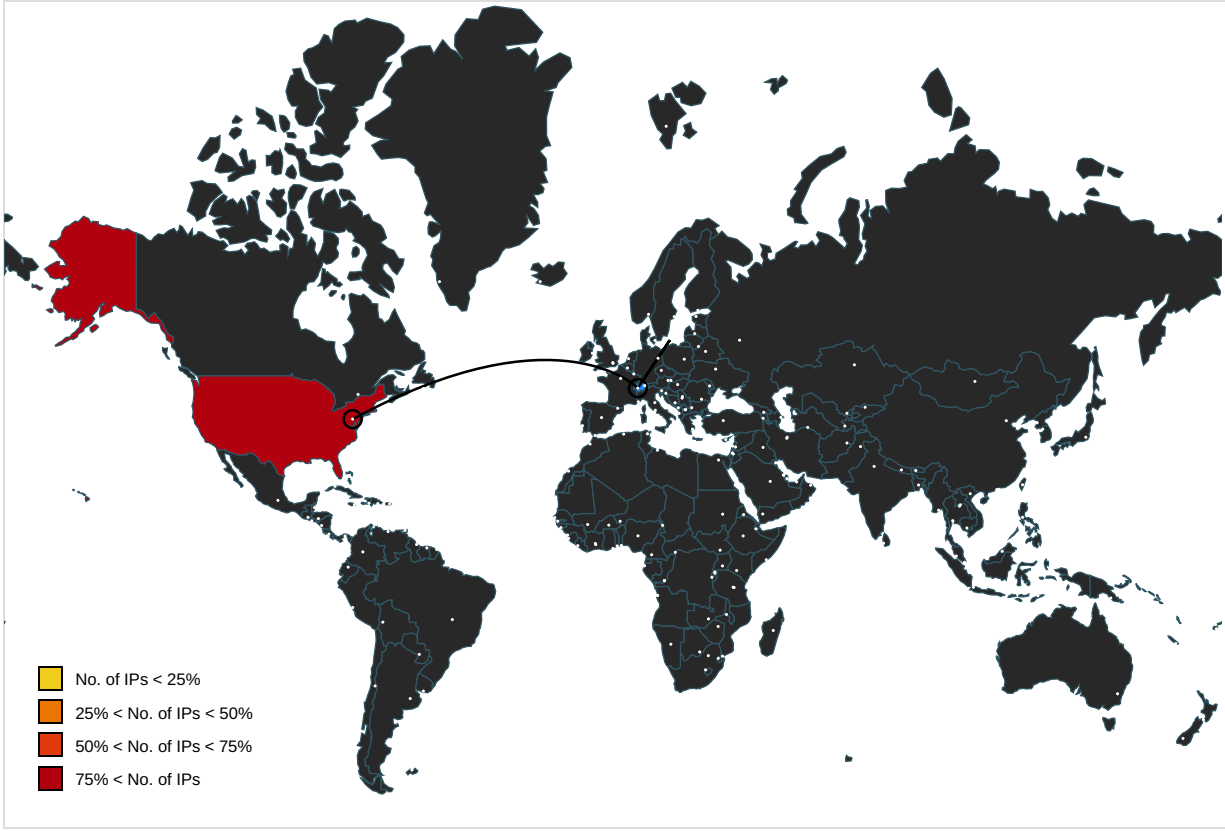
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.dc-msedge.net	131.253.33.200	true	false	• 0%, Virustotal, Browse	unknown
host-file-host6.com	34.118.39.10	true	true	• 25%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 22%, 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

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.118.39.10	host-file-host6.com	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	677968
Start date and time: 03/08/202210:16:10	2022-08-03 10:16:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ofAn3uUEPe.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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: 89.4% (good quality ratio 83.6%) • Quality average: 74.9% • Quality standard deviation: 30.7%

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 40.125.122.176, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, www-www.bing.com.trafficmanager.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
10:18:21	Task Scheduler	Run new task: Firefox Default Browser Agent B473D81467D5CBC4 path: C:\Users\user\AppData\Roaming\hbjebed

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\hbjebed

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347648
Entropy (8bit):	6.380725935353117
Encrypted:	false
SSDEEP:	6144:ewzhZWcL1leWA6JDYyHVV7Vc7JW5VtSZJYnAGiL:dhB1oWjJD7HVV76Y57AT

MD5:	DB5723C9308CB986EAE4262297A51FA0
SHA1:	EE4130DCB4052DDDCD66A5833B18661187A28F76
SHA-256:	2D2BDC891614F50E1574787D7728654C02C70EB829A04BD6411EF874F92AA1EB
SHA-512:	8FF382910DF70309BB96A95A84FABB62AC1A6ADB1D66731DEC8BCC2992A528157A3D95DDC34A44C3A94FEDF7E00D4F39BED1BCC0492FD756F4D1546CE8486E7E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 48%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1..,1..,1../.R,&../.D,...,...,4..,1..,.../.C,.../.S,0../.V,0..,Rich1..,.....PE..L...j..a.....".....`.....@....@.....0..... ..<... .....0.....h...@.....text....!....."..... ..`.data.....@.....&.....@....zuja.....:.....@....miw.....>.....@....kagivu.....B.....@....rsrc..... .....D.....@..@.....

C:\Users\user\AppData\Roaming\hbjebed: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):	6.380725935353117
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:	ofAn3uUEPe.exe
File size:	347648
MD5:	db5723c9308cb986eae4262297a51fa0
SHA1:	ee4130dcb4052dddcd66a5833b18661187a28f76
SHA256:	2d2bdc891614f50e1574787d7728654c02c70eb829a04bd6411ef874f92aa1eb
SHA512:	8ff382910df70309bb96a95a84fabb62ac1a6adb1d66731dec8bcc2992a528157a3d95ddc34a44c3a94fedf7e00d4f39bed1bcc0492fd756f4d1546ce8486e7e
SSDEEP:	6144:ewzhZWcL1leWA6JDYyHVV7Vc7JW5VtSZJYnAGiL:dhB1oWjJD7HVV76Y57AT
TLSH:	AA749D00B7A0D03DE5B311F4BA7A83A8B92D3DA1672544CF22D62AEE57346E0ED75317
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1..,1..,1../.R,&../.D,...,...,4..,1..,.../.C,.../.S,0../.V,0..,Rich1..,.....PE..L...j..a....."......

File Icon

Icon Hash:	aecaae9ecea62aa2

Static PE Info

General	
Entrypoint:	0x40b360
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:	0x61859A6A [Fri Nov 5 20:56:10 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:	7e4b40ca154bd059f7d22ed12b0ce64d

Entrypoint Preview
Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007FD014D7011Bh
call 00007FD014D65A26h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00431950h
push 0040EFF0h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [00444234h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax

Instruction
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004011F4h]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007FD014D65A38h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007FD014D65B68h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FD014D65BA4h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007FD014D713DAh
add esp, 04h
test eax, eax
jne 00007FD014D65A1Ch
push 0000001Ch
call 00007FD014D65B5Ch
add esp, 04h
call 00007FD014D6DEF4h
test eax, eax
jne 00007FD014D65A1Ch
push 00000010h

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	0x320b4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x108d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1330	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	0x8f68	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2e0	.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	0x321d2	0x32200	False	0.37546758104738154	data	5.761195119633815	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x34000	0x1a3e8	0x11400	False	0.9332540760869565	data	7.791068859484556	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.zuja	0x4f000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.miw	0x50000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.kagivu	0x51000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x52000	0x108d0	0x10a00	False	0.5499295112781954	data	5.488087902886926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x52630	0x6c8	data	Korean	North Korea
RT_ICON	0x52630	0x6c8	data	Korean	South Korea
RT_ICON	0x52cf8	0x568	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x52cf8	0x568	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x53260	0x10a8	data	Korean	North Korea
RT_ICON	0x53260	0x10a8	data	Korean	South Korea
RT_ICON	0x54308	0x988	dBase III DBT, version number 0, next free block index 40	Korean	North Korea
RT_ICON	0x54308	0x988	dBase III DBT, version number 0, next free block index 40	Korean	South Korea
RT_ICON	0x54c90	0x468	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x54c90	0x468	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x55148	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Korean	North Korea
RT_ICON	0x55148	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Korean	South Korea
RT_ICON	0x559f0	0x6c8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Korean	North Korea
RT_ICON	0x559f0	0x6c8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Korean	South Korea
RT_ICON	0x560b8	0x568	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x560b8	0x568	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x56620	0x10a8	data	Korean	North Korea
RT_ICON	0x56620	0x10a8	data	Korean	South Korea
RT_ICON	0x576c8	0x988	data	Korean	North Korea
RT_ICON	0x576c8	0x988	data	Korean	South Korea
RT_ICON	0x58050	0x468	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x58050	0x468	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x58518	0x25a8	data	Korean	North Korea
RT_ICON	0x58518	0x25a8	data	Korean	South Korea
RT_ICON	0x5aac0	0x10a8	data	Korean	North Korea
RT_ICON	0x5aac0	0x10a8	data	Korean	South Korea
RT_ICON	0x5bb90	0xea8	data	Korean	North Korea
RT_ICON	0x5bb90	0xea8	data	Korean	South Korea
RT_ICON	0x5ca38	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 8305227, next used block 8370799	Korean	North Korea
RT_ICON	0x5ca38	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 8305227, next used block 8370799	Korean	South Korea
RT_ICON	0x5d2e0	0x6c8	data	Korean	North Korea

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5d2e0	0x6c8	data	Korean	South Korea
RT_ICON	0x5d9a8	0x568	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x5d9a8	0x568	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_ICON	0x5df10	0x25a8	data	Korean	North Korea
RT_ICON	0x5df10	0x25a8	data	Korean	South Korea
RT_ICON	0x604b8	0x10a8	data	Korean	North Korea
RT_ICON	0x604b8	0x10a8	data	Korean	South Korea
RT_ICON	0x61560	0x988	data	Korean	North Korea
RT_ICON	0x61560	0x988	data	Korean	South Korea
RT_ICON	0x61ee8	0x468	GLS_BINARY_LSB_FIRST	Korean	North Korea
RT_ICON	0x61ee8	0x468	GLS_BINARY_LSB_FIRST	Korean	South Korea
RT_STRING	0x625d8	0xac	data	Korean	North Korea
RT_STRING	0x625d8	0xac	data	Korean	South Korea
RT_STRING	0x62688	0x246	data	Korean	North Korea
RT_STRING	0x62688	0x246	data	Korean	South Korea
RT_ACCELERATOR	0x62438	0x60	data	Korean	North Korea
RT_ACCELERATOR	0x62438	0x60	data	Korean	South Korea
RT_ACCELERATOR	0x623c8	0x70	data	Korean	North Korea
RT_ACCELERATOR	0x623c8	0x70	data	Korean	South Korea
RT_GROUP_ICON	0x5bb68	0x22	data	Korean	North Korea
RT_GROUP_ICON	0x5bb68	0x22	data	Korean	South Korea
RT_GROUP_ICON	0x584b8	0x5a	data	Korean	North Korea
RT_GROUP_ICON	0x584b8	0x5a	data	Korean	South Korea
RT_GROUP_ICON	0x62350	0x76	data	Korean	North Korea
RT_GROUP_ICON	0x62350	0x76	data	Korean	South Korea
RT_GROUP_ICON	0x550f8	0x4c	data	Korean	North Korea
RT_GROUP_ICON	0x550f8	0x4c	data	Korean	South Korea
RT_VERSION	0x62498	0x13c	data	Korean	North Korea
RT_VERSION	0x62498	0x13c	data	Korean	South Korea

Imports

DLL	Import
KERNEL32.dll	LocalSize, FindNextFileA, VerifyVersionInfoA, VerifyVersionInfoW, WriteConsoleInputW, EnumDateFormatsW, FindNextFileW, CopyFileExA, DnsHostnameToComputerNameW, ReadConsoleOutputCharacterW, SetConsoleActiveScreenBuffer, LockFile, GetProfileSectionW, QueryDosDeviceW, IsSystemResumeAutomatic, GetProcessPriorityBoost, GetDriveTypeW, GlobalGetAtomNameA, lstrlenA, FindNextVolumeMountPointW, TlsGetValue, SizeofResource, WriteConsoleInputA, GetConsoleTitleA, GetComputerNameExW, OpenEventA, CallNamedPipeW, GetModuleHandleW, GetSystemDirectoryA, SetCurrentDirectoryA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, MoveFileWithProgressW, GetCommandLineW, InterlockedExchange, GetConsoleTitleW, CopyFileW, CreateActCtxA, FormatMessageW, EnterCriticalSection, FindNextVolumeW, GetOverlappedResult, CreateNamedPipeW, GetSystemDefaultLangID, GetConsoleAliasesLengthW, WriteProfileSectionW, AddAtomA, InterlockedIncrement, HeapFree, _hwrite, InterlockedExchangeAdd, GetStartupInfoW, CreateMailslotA, GetCPInfoExW, GetSystemWow64DirectoryW, GetLastError, GetPrivateProfileIntA, GetConsoleAliasExesLengthW, DebugBreak, SetLastError, LoadLibraryW, GetComputerNameA, VirtualAlloc, GetOEMCP, lstrcpyA, GetConsoleAliasA, GetDiskFreeSpaceExA, TerminateProcess, EnumResourceLanguagesA, GetCPInfoExA, SetConsoleWindowInfo, GlobalGetAtomNameW, WriteConsoleA, EnumSystemLocalesA, GetPrivateProfileSectionNamesW, OpenMutexW, GetFileAttributesW, FileTimeToSystemTime, GlobalWire, GetTapeParameters, lstrcmpW, ResetEvent, LockFileEx, MoveFileA, CreateMutexA, FindResourceW, GetCommState, FormatMessageA, InterlockedCompareExchange, ConvertThreadToFiber, GetConsoleFontSize, LocalAlloc, lstrcpyW, HeapLock, GetFileAttributesA, SetCalendarInfoW, GetSystemWindowsDirectoryW, GetConsoleAliasesW, EnumDateFormatsExW, GetComputerNameW, GetPrivateProfileStructW, _hread, OpenWaitableTimerA, EnumResourceNamesW, FillConsoleOutputCharacterA, GetFullPathNameW, GetThreadPriority, MapUserPhysicalPages, WriteConsoleOutputCharacterA, OpenJobObjectW, CreateFileW, BuildCommDCBAndTimeoutsW, GetBinaryTypeW, SetCalendarInfoA, GetFileInformationByHandle, GetDefaultCommConfigW, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, GetCommandLineA, GetStartupInfoA, HeapValidate, IsBadReadPtr, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, GetCurrentProcess, IsDebuggerPresent, GetModuleHandleA, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, SetFilePointer, SetHandleCount, GetStdHandle, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, ExitProcess, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapDestroy, HeapCreate, VirtualFree, WriteFile, HeapAlloc, HeapSize, HeapReAlloc, GetACP, GetCPInfo, IsValidCodePage, FlushFileBuffers, GetConsoleCP, GetConsoleMode, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, InitializeCriticalSectionAndSpinCount, SetStdHandle, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleOutputCP, CloseHandle, CreateFileA
USER32.dll	CharUpperA, GetCursorInfo

Possible Origin

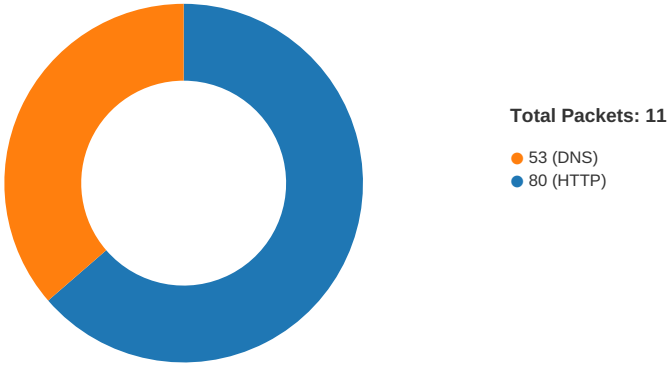
Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.434.118.39.104 9768802851815 08/03/22-10:18:21.517468	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49768	80	192.168.2.4	34.118.39.10

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 10:18:21.476331949 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:21.513225079 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 3, 2022 10:18:21.514849901 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:21.517467976 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:21.517509937 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:21.554637909 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 3, 2022 10:18:21.649977922 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 3, 2022 10:18:21.701522112 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:51.651237011 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 3, 2022 10:18:51.651437998 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:51.840192080 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 3, 2022 10:18:51.876586914 CEST	80	49768	34.118.39.10	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 10:18:21.366434097 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 3, 2022 10:18:21.473633051 CEST	53	56076	8.8.8.8	192.168.2.4
Aug 3, 2022 10:18:21.669536114 CEST	60758	53	192.168.2.4	8.8.8.8
Aug 3, 2022 10:18:22.717921019 CEST	60758	53	192.168.2.4	8.8.8.8
Aug 3, 2022 10:18:23.764383078 CEST	60758	53	192.168.2.4	8.8.8.8
Aug 3, 2022 10:18:25.720189095 CEST	53	60758	8.8.8.8	192.168.2.4
Aug 3, 2022 10:18:26.768790007 CEST	53	60758	8.8.8.8	192.168.2.4
Aug 3, 2022 10:18:27.795301914 CEST	53	60758	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 3, 2022 10:18:26.768888950 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Aug 3, 2022 10:18:27.796173096 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2022 10:18:21.366434097 CEST	192.168.2.4	8.8.8.8	0x1545	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:21.669536114 CEST	192.168.2.4	8.8.8.8	0x72d2	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:22.717921019 CEST	192.168.2.4	8.8.8.8	0x72d2	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:23.764383078 CEST	192.168.2.4	8.8.8.8	0x72d2	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2022 10:17:07.954627037 CEST	8.8.8.8	192.168.2.4	0x8fc3	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2022 10:17:07.954627037 CEST	8.8.8.8	192.168.2.4	0x8fc3	No error (0)	dual-a-0001.dc-msedge.net		131.253.33.200	A (IP address)	IN (0x0001)
Aug 3, 2022 10:17:07.954627037 CEST	8.8.8.8	192.168.2.4	0x8fc3	No error (0)	dual-a-0001.dc-msedge.net		13.107.22.200	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:21.473633051 CEST	8.8.8.8	192.168.2.4	0x1545	No error (0)	host-file-host6.com		34.118.39.10	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:25.720189095 CEST	8.8.8.8	192.168.2.4	0x72d2	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:26.768790007 CEST	8.8.8.8	192.168.2.4	0x72d2	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 10:18:27.795301914 CEST	8.8.8.8	192.168.2.4	0x72d2	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- akycjr.com
  - host-file-host6.com

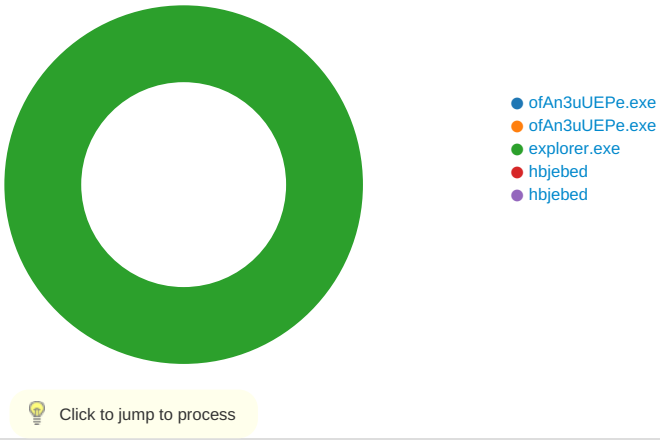
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49768	34.118.39.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2022 10:18:21.517467976 CEST	1235	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://akycjr.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 253 Host: host-file-host6.com
Aug 3, 2022 10:18:21.649977922 CEST	1236	IN	HTTP/1.1 200 OK server: nginx/1.20.1 date: Wed, 03 Aug 2022 08:18:21 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked Data Raw: 46 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: ofAn3uUEPe.exe PID: **4496**, Parent PID: **3724**

General

Target ID:	0
Start time:	10:17:15
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\ofAn3uUEPe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ofAn3uUEPe.exe"
Imagebase:	0x400000
File size:	347648 bytes
MD5 hash:	DB5723C9308CB986EAE4262297A51FA0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ofAn3uUEPe.exe PID: **500**, Parent PID: **4496**

General

Target ID:	1
Start time:	10:17:17
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\ofAn3uUEPe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ofAn3uUEPe.exe"
Imagebase:	0x400000
File size:	347648 bytes
MD5 hash:	DB5723C9308CB986EAE4262297A51FA0
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: 00000001.00000002.349529334.0000000001F61000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.349396035.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **3616**, Parent PID: **500**

General

Target ID:	5
Start time:	10:17:25
Start date:	03/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.328538195.0000000002701000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hbjebed	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	2701F42	CopyFileW
C:\Users\user\AppData\Roaming\hbjebed\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2701F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ofAn3uUEPe.exe	success or wait	1	2701F53	DeleteFileW
C:\Users\user\AppData\Roaming\hbjebed:Zone.Identifier	success or wait	1	2701F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hbjebed	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 75 fd fd 7f 31 fd fd 2c 31 fd fd 2c 31 fd fd 2c 2f fd 52 2c 26 fd fd 2c 2f fd 44 2c fd fd fd 2c 16 15 fd 2c 34 fd fd 2c 31 fd fd 2c fd fd fd 2c 2f fd 43 2c 0e fd fd 2c 2f fd 53 2c 30 fd fd 2c 2f fd 56 2c 30 fd fd 2c 52 69 63 68 31 fd fd 2c 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 6a fd fd 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 22 03 00 00 fd 02 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$u1,1,1,/R,&,/D ,,,4,1,,/C,,/S,0,/V,0,Rich1, PELja"	success or wait	3	2701F42	CopyFileW
C:\Users\user\AppData\Roaming\hbjebed: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	2701F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: hbjebed PID: **5008**, Parent PID: **960**

General

Target ID:	17
Start time:	10:18:21
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\hbjebed
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hbjebed
Imagebase:	0x400000
File size:	347648 bytes
MD5 hash:	DB5723C9308CB986EAE4262297A51FA0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 34%, Virustotal, Browse • Detection: 48%, ReversingLabs
Reputation:	low

Analysis Process: hbjebed PID: **4188**, Parent PID: **5008**

General

Target ID:	18
Start time:	10:18:24
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\hbjebed
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hbjebed

Imagebase:	0x400000
File size:	347648 bytes
MD5 hash:	DB5723C9308CB986EAE4262297A51FA0
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: 00000012.00000002.406226962.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000012.00000002.406410596.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly