ID: 678602
Sample Name: 04ZQ5etz9i.exe
Cookbook: default.jbs
Time: 09:36:11
Date: 04/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report 04ZQ5etz9i.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
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\jtdteff 11
C:\Users\user\AppData\Roaming\jtdteff: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 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
ICMP Packets 18
DNS Queries 18
DNS Answers 18
HTTP Request Dependency Graph 18

HTTP Packets 18
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: 04ZQ5etz9i.exePID: 1888, Parent PID: 6016 19
General 19
Analysis Process: 04ZQ5etz9i.exePID: 3908, Parent PID: 1888 19
General 19
Analysis Process: explorer.exePID: 3616, Parent PID: 3908 20
General 20
File Activities 20
File Created 20
File Deleted 20
File Written 20
Analysis Process: jtdteffPID: 5348, Parent PID: 960 21
General 21
Analysis Process: jtdteffPID: 388, Parent PID: 5348 21
General 21
Disassembly 22

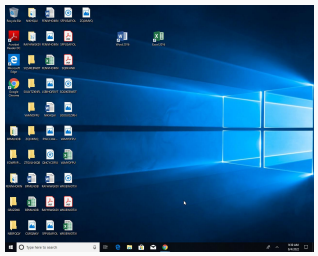
Windows Analysis Report

04ZQ5etz9i.exe

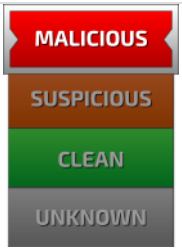
Overview

General Information

Sample Name:	04ZQ5etz9i.exe
Analysis ID:	678602
MD5:	785d9d53c4b721..
SHA1:	751b17ab9fae89..
SHA256:	6716b20272e1b5.
Tags:	ArkeiStealer exe
Infos:	



Detection



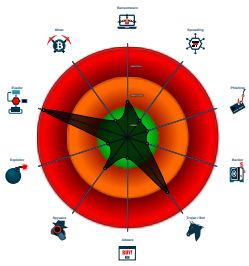
SmokeLoader

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**
- 04ZQ5etz9i.exe (PID: 1888 cmdline: "C:\Users\user\Desktop\04ZQ5etz9i.exe" MD5: 785D9D53C4B721385E9E5F51A4846791)
  - 04ZQ5etz9i.exe (PID: 3908 cmdline: "C:\Users\user\Desktop\04ZQ5etz9i.exe" MD5: 785D9D53C4B721385E9E5F51A4846791)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- jtdteff (PID: 5348 cmdline: C:\Users\user\AppData\Roaming\jtdteff MD5: 785D9D53C4B721385E9E5F51A4846791)
  - jtdteff (PID: 388 cmdline: C:\Users\user\AppData\Roaming\jtdteff MD5: 785D9D53C4B721385E9E5F51A4846791)
- **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
00000015.00000002.369606256.0000000000580000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000015.00000002.369606256.0000000000580000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x6f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0

Source	Rule	Description	Author	Strings
00000001.00000002.315316799.00000000005A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.315316799.00000000005A1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000014.00000002.357473381.0000000000766000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x506e:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.04ZQ5etz9i.exe.4815a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.0.04ZQ5etz9i.exe.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.0.04ZQ5etz9i.exe.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.0.04ZQ5etz9i.exe.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.04ZQ5etz9i.exe.400000.0.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

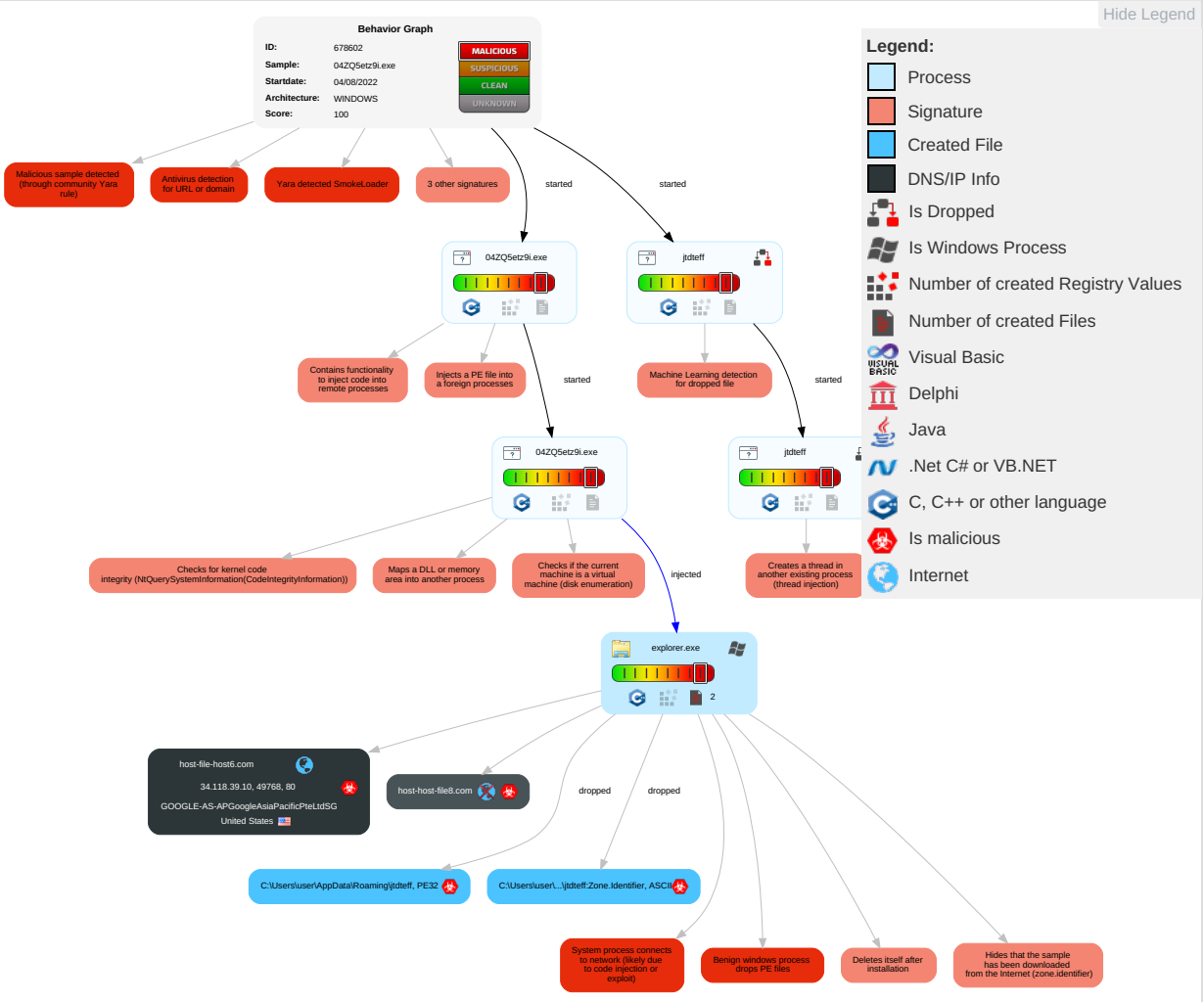
Yara detected SmokeLoader

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 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
04ZQ5etz9i.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.04ZQ5etz9i.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1228923		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.04ZQ5etz9i.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.04ZQ5etz9i.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1228923		Download File
21.0.jtdteff.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.jtdteff.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.04ZQ5etz9i.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.04ZQ5etz9i.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.04ZQ5etz9i.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.04ZQ5etz9i.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1228923		Download File
1.0.04ZQ5etz9i.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1228923		Download File
0.2.04ZQ5etz9i.exe.4815a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.jtdteff.6f15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.jtdteff.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.jtdteff.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://host-file-host6.com/	0%	URL Reputation	safe	
http://host-host-file8.com/	100%	URL Reputation	malware	

Domains and IPs

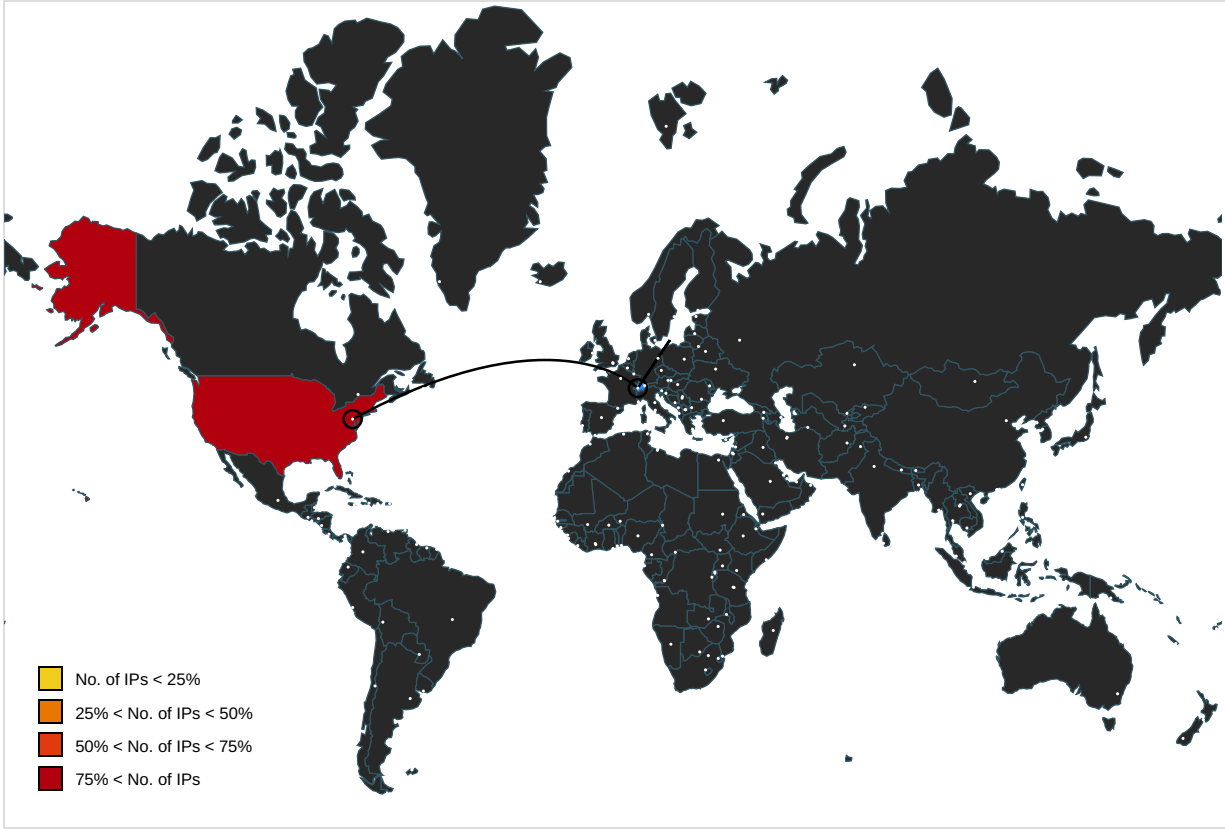
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	34.118.39.10	true	true		unknown
host-host-file8.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://host-file-host6.com/	true	• URL Reputation: safe	unknown
http://host-host-file8.com/	true	• URL Reputation: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	678602
Start date and time: 04/08/202209:36:11	2022-08-04 09:36:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	04ZQ5etz9i.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:	30
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: 83.7% (good quality ratio 78.1%) • Quality average: 74.7% • Quality standard deviation: 30.8%

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, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
09:38:08	Task Scheduler	Run new task: Firefox Default Browser Agent 14075C06E1FEED28 path: C:\Users\user\AppData\Roaming\jtdteff

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\jtdteff

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346624
Entropy (8bit):	6.355322829319774
Encrypted:	false
SSDEEP:	6144:kbielRAT0GZkAMOHG/HBCssiXE8du+9W0U:kmehKkZOHGfBCsG29W
MD5:	785D9D53C4B721385E9E5F51A4846791
SHA1:	751B17AB9FAE896ED414F42DACD885BD75A83F46
SHA-256:	6716B20272E1B5EC3A6D86F9144AF69E1615EFDAB035E130B654757B36E8B84F

SHA-512:	C96CF6B70332FBFB0F0E55674843082A1AF5F88447D0E8FAA7351CF59B54080139F91745DAE07558C168802690628D86D0CEFEC97B50F3F0A05F6792BE923581
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1..,1..,1../.2,&../.$,..,.%..,4..,1..,../.#,.../.3,0..,/.6,0..,Rich1.,..... ..PE..L....r#`.....".....@....@.....0.....T..... ..<... .....@..... .text...Z .....".....  ..`.data.....@.....&.....@....cuheb.....4.....@....rilez.....6.....@....kibu.....:.....@....vitid.....>..... .....@....rsrc..... .....@.....@..@.....

C:\Users\user\AppData\Roaming\jtdteff: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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 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):	6.355322829319774
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	04ZQ5etz9i.exe
File size:	346624
MD5:	785d9d53c4b721385e9e5f51a4846791
SHA1:	751b17ab9fae896ed414f42dacd885bd75a83f46
SHA256:	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f
SHA512:	c96cf6b70332fbfb0f0e55674843082a1af5f88447d0e8faa7351cf59b54080139f91745dae07558c168802690628d86d0cefec97b50f3f0a05f6792be923581
SSDEEP:	6144:kbielRAT0GZkAMOHG/HBCssiXE8du+9W0U:kmehKkZOHGfBCsG29W
TLSH:	0574AE40BBA0D43DE1F312F4B97A83A8B52D7EA15B7410CB52D62AEE56346E0EC75307
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1..,1..,1../.2,&../.$,...,.%.,4..,1..,.../.#,.../.3,0../.6,0..,Rich1..,.....PE..L....r#`.....".

File Icon

Icon Hash:	aedaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x40b2a0
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6023728D [Wed Feb 10 05:43:41 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:	9da6af138aaaf087a1ce609a65e93d9a

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007FE788C6911Bh
call 00007FE788C5EA26h
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 004318A0h
push 0040EF30h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [00443BD4h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
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

Instruction
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004011D0h]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007FE788C5EA38h
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 00007FE788C5EB68h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FE788C5EBA4h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007FE788C6A3EAh
add esp, 04h
test eax, eax
jne 00007FE788C5EA1Ch
push 0000001Ch
call 00007FE788C5EB5Ch
add esp, 04h
call 00007FE788C66EF4h
test eax, eax
jne 00007FE788C5EA1Ch
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	0x32004	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	0x1310	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	0x8f18	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2bc	.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	0x3205a	0x32200	False	0.3747418562967581	data	5.747276658789658	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x34000	0x19d88	0x10e00	False	0.9295717592592593	data	7.777144287546035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.cuheb	0x4e000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rilez	0x4f000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.kibu	0x50000	0x400	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.vitid	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	0.5496211231203008	data	5.486118535451178	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
RT_ICON	0x5d2e0	0x6c8	data	Korean	South Korea

Name	RVA	Size	Type	Language	Country
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	lstrcatA, LocalSize, 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, LeaveCriticalSection, FindNextVolumeW, GetOverlappedResult, CreateNamedPipeW, GetSystemDefaultLangID, GetConsoleAliasesLengthW, WriteProfileSectionW, AddAtomA, InterlockedIncrement, HeapSize, _hwrite, InterlockedExchangeAdd, GetStartupInfoW, CreateMailslotA, IsDBCSLeadByte, GetSystemWow64DirectoryW, GetLastError, GetPrivateProfileIntA, GetConsoleAliasExesLengthW, DebugBreak, SetLastError, LoadLibraryW, GetComputerNameA, VirtualAlloc, GetOEMCP, lstrcpyA, GetConsoleAliasW, GetDiskFreeSpaceExW, TerminateProcess, EnumResourceLanguagesA, GetCPInfoExW, SetConsoleWindowInfo, GlobalGetAtomNameW, WriteConsoleA, EnumSystemLocalesA, FileTimeToSystemTime, ResetEvent, LockFileEx, MoveFileA, CreateMutexA, FindResourceW, SetCommState, InterlockedCompareExchange, ConvertThreadToFiber, GetConsoleFontSize, LocalAlloc, lstrcpyW, HeapLock, GetFileAttributesA, SetCalendarInfoW, GetSystemWindowsDirectoryW, GetConsoleAliasesW, EnumDateFormatsExW, GetComputerNameW, GetPrivateProfileStructW, OpenWaitableTimerA, EnumResourceNamesW, FillConsoleOutputCharacterA, GetFullPathNameW, GetThreadPriority, MapUserPhysicalPages, WriteConsoleOutputCharacterA, OpenJobObjectA, CreateFileW, BuildCommDCBAndTimeoutsW, SetCalendarInfoA, GetFileInformationByHandle, GetDefaultCommConfigW, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, 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, HeapFree, VirtualFree, WriteFile, HeapAlloc, 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

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

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 4, 2022 09:38:07.691579103 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:07.728035927 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 4, 2022 09:38:07.728180885 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:07.728344917 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:07.728353024 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:07.764966965 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 4, 2022 09:38:07.858201027 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 4, 2022 09:38:08.059257984 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:37.858741045 CEST	80	49768	34.118.39.10	192.168.2.4
Aug 4, 2022 09:38:37.858876944 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:37.858978033 CEST	49768	80	192.168.2.4	34.118.39.10
Aug 4, 2022 09:38:37.895512104 CEST	80	49768	34.118.39.10	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 4, 2022 09:38:07.363244057 CEST	64277	53	192.168.2.4	8.8.8.8
Aug 4, 2022 09:38:07.655704975 CEST	53	64277	8.8.8.8	192.168.2.4
Aug 4, 2022 09:38:07.868459940 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 4, 2022 09:38:08.871870041 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 4, 2022 09:38:09.872922897 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 4, 2022 09:38:11.895647049 CEST	53	56076	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 4, 2022 09:38:12.898232937 CEST	53	56076	8.8.8.8	192.168.2.4
Aug 4, 2022 09:38:14.069996119 CEST	53	56076	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 4, 2022 09:38:12.898369074 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Aug 4, 2022 09:38:14.070182085 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 4, 2022 09:38:07.363244057 CEST	192.168.2.4	8.8.8.8	0xb1b8	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:07.868459940 CEST	192.168.2.4	8.8.8.8	0x8843	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:08.871870041 CEST	192.168.2.4	8.8.8.8	0x8843	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:09.872922897 CEST	192.168.2.4	8.8.8.8	0x8843	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 4, 2022 09:38:07.655704975 CEST	8.8.8.8	192.168.2.4	0xb1b8	No error (0)	host-file-host6.com		34.118.39.10	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:11.895647049 CEST	8.8.8.8	192.168.2.4	0x8843	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:12.898232937 CEST	8.8.8.8	192.168.2.4	0x8843	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 4, 2022 09:38:14.069996119 CEST	8.8.8.8	192.168.2.4	0x8843	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nwvsnnm.org
  - host-file-host6.com

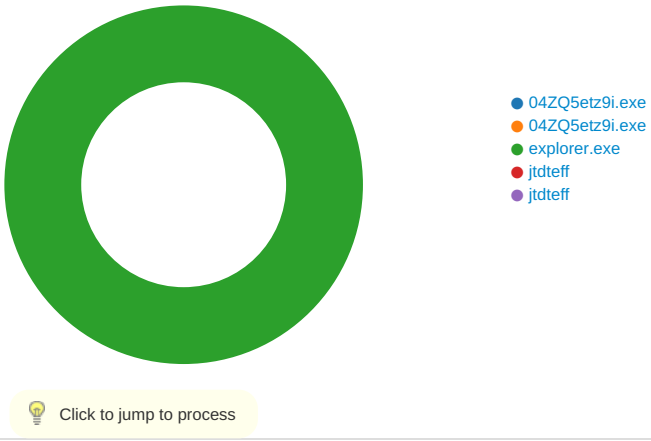
HTTP Packets

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 4, 2022 09:38:07.728344917 CEST	1155	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nwvsnnm.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 247 Host: host-file-host6.com
Aug 4, 2022 09:38:07.858201027 CEST	1155	IN	HTTP/1.1 200 OK server: nginx/1.20.1 date: Thu, 04 Aug 2022 07:38:07 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: 04ZQ5etz9i.exe PID: 1888, Parent PID: 6016

General

Target ID:	0
Start time:	09:37:12
Start date:	04/08/2022
Path:	C:\Users\user\Desktop\04ZQ5etz9i.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\04ZQ5etz9i.exe"
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	785D9D53C4B721385E9E5F51A4846791
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: 00000000.00000002.235932667.00000000006B6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: 04ZQ5etz9i.exe PID: 3908, Parent PID: 1888

General

Target ID:	1
Start time:	09:37:14
Start date:	04/08/2022
Path:	C:\Users\user\Desktop\04ZQ5etz9i.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\04ZQ5etz9i.exe"
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	785D9D53C4B721385E9E5F51A4846791
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: 00000001.00000002.315316799.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.315316799.00000000005A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.315100572.00000000004F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.315100572.00000000004F0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3616**, Parent PID: **3908**

General

Target ID:	5
Start time:	09:37:21
Start date:	04/08/2022
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: 00000005.00000000.288381644.00000000024D1000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000005.00000000.288381644.00000000024D1000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jtdteff	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	24D1F42	CopyFileW
C:\Users\user\AppData\Roaming\jtdteff\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	24D1F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\04ZQ5etz9i.exe	success or wait	1	24D1F53	DeleteFileW
C:\Users\user\AppData\Roaming\jtdteff:Zone.Identifier	success or wait	1	24D1F9E	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\jtdteff	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 2c 31 fd 2c 31 fd 2c 2f fd 32 2c 26 fd 2c 2f fd 24 2c fd fd 2c 16 25 fd 2c 34 fd 2c 31 fd 2c fd fd 2c 2f fd 23 2c 0e fd 2c 2f fd 33 2c 30 fd 2c 2f fd 36 2c 30 fd 2c 52 69 63 68 31 fd 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 fd 72 23 60 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 22 03	MZ@!L!This program cannot be run in DOS mode.$u1,1,1,/2,&,/$,,%,4,1,,/#,,/3,0,/6,0,Rich 1,PELr#`"	success or wait	3	24D1F42	CopyFileW
C:\Users\user\AppData\Roaming\jtdteff: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	24D1F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: jtdteff PID: **5348**, Parent PID: **960**

General

Target ID:	20
Start time:	09:38:08
Start date:	04/08/2022
Path:	C:\Users\user\AppData\Roaming\jtdteff
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jtdteff
Imagebase:	0x400000
File size:	346624 bytes
MD5 hash:	785D9D53C4B721385E9E5F51A4846791
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: 00000014.00000002.357473381.0000000000766000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: jtdteff PID: **388**, Parent PID: **5348**

General

Target ID:	21
Start time:	09:38:11
Start date:	04/08/2022
Path:	C:\Users\user\AppData\Roaming\jtdteff
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jtdteff
Imagebase:	0x400000

File size:	346624 bytes
MD5 hash:	785D9D53C4B721385E9E5F51A4846791
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: 00000015.00000002.369606256.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000015.00000002.369606256.0000000000580000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000015.00000002.369783218.0000000002091000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000015.00000002.369783218.0000000002091000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly