ID: 678081
Sample Name: 6s1js8BzrC.exe
Cookbook: default.jbs
Time: 14:51:07
Date: 03/08/2022
Version: 35.0.0 Citrine

Table of Contents

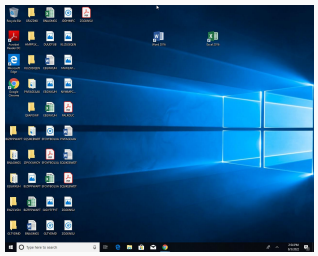
Windows Analysis Report

6s1js8BzrC.exe

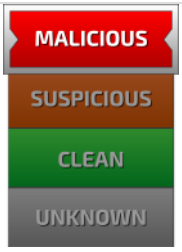
Overview

General Information

Sample Name:	6s1js8BzrC.exe
Analysis ID:	678081
MD5:	c9948059cdc5e0..
SHA1:	0c00b2242c8648..
SHA256:	80f503f4fd7e84b..
Tags:	ArkeiStealer exe
Infos:	



Detection



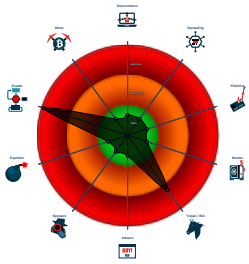
SmokeLoader

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…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- 6s1js8BzrC.exe (PID: 1056 cmdline: "C:\Users\user\Desktop\6s1js8BzrC.exe" MD5: C9948059CDC5E0AEF9C193D605C7F659)
  - 6s1js8BzrC.exe (PID: 504 cmdline: "C:\Users\user\Desktop\6s1js8BzrC.exe" MD5: C9948059CDC5E0AEF9C193D605C7F659)
    - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- twtgjvf (PID: 2912 cmdline: C:\Users\user\AppData\Roaming\twtgjvf MD5: C9948059CDC5E0AEF9C193D605C7F659)
  - twtgjvf (PID: 2756 cmdline: C:\Users\user\AppData\Roaming\twtgjvf MD5: C9948059CDC5E0AEF9C193D605C7F659)
- **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
00000007.00000002.503883541.00000000004A0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000002.00000002.445865427.0000000002051000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.445757308.0000000002030000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000007.00000002.503917126.00000000005B1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000003.00000000.423194052.0000000004D61000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.6s1js8BzrC.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.6s1js8BzrC.exe.24c15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
7.2.twtgjvf.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.2.twtgjvf.24c15a0.1.raw.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: 192.168.2.6 - Destination IP: 34.118.39.10

Timestamp:	192.168.2.634.118.39.1049722802851815 08/03/22-14:53:10.081323
SID:	2851815
Source Port:	49722
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

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

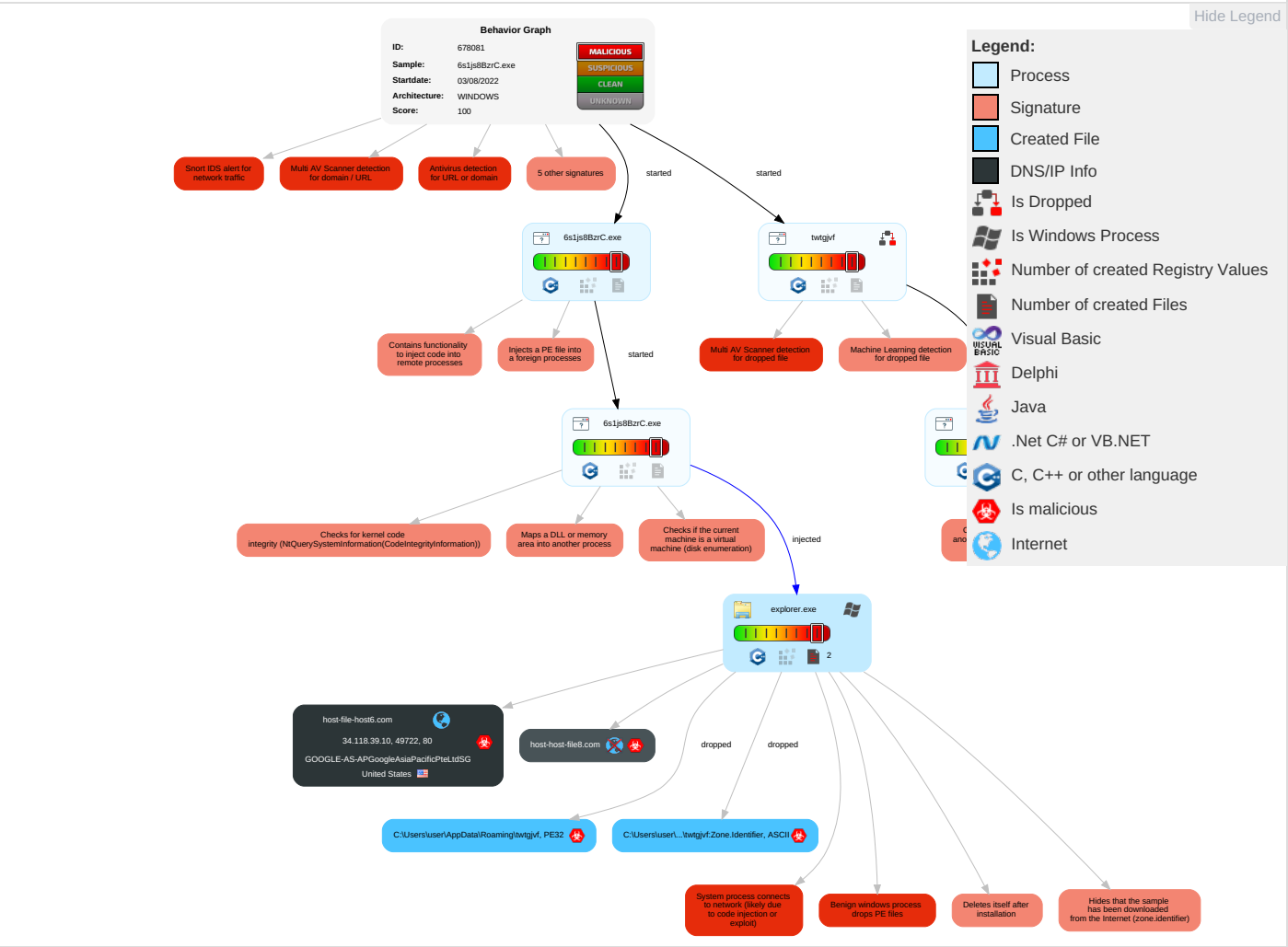
Yara detected SmokeLoader

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	1 Exploitation for Client Execution	1 DLL Side-Loading	5 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	4 1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 2 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	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	2 Obfuscated Files or Information	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 Software Packing	Cached Domain Credentials	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 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
6s1js8BzrC.exe	41%	Virustotal		Browse
6s1js8BzrC.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\twtgjvf	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\twtgjvf	41%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.6s1js8BzrC.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.6s1js8BzrC.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.twtgjvf.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.6s1js8BzrC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.twtgjvf.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.6s1js8BzrC.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
2.0.6s1js8BzrC.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.twtgjvf.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.twtgjvf.24c15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.twtgjvf.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
7.2.twtgjvf.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.6s1js8BzrC.exe.24c15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
host-file-host6.com	25%	Virustotal		Browse
host-host-file8.com	22%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
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	• 25%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 22%, Virustotal, Browse	unknown

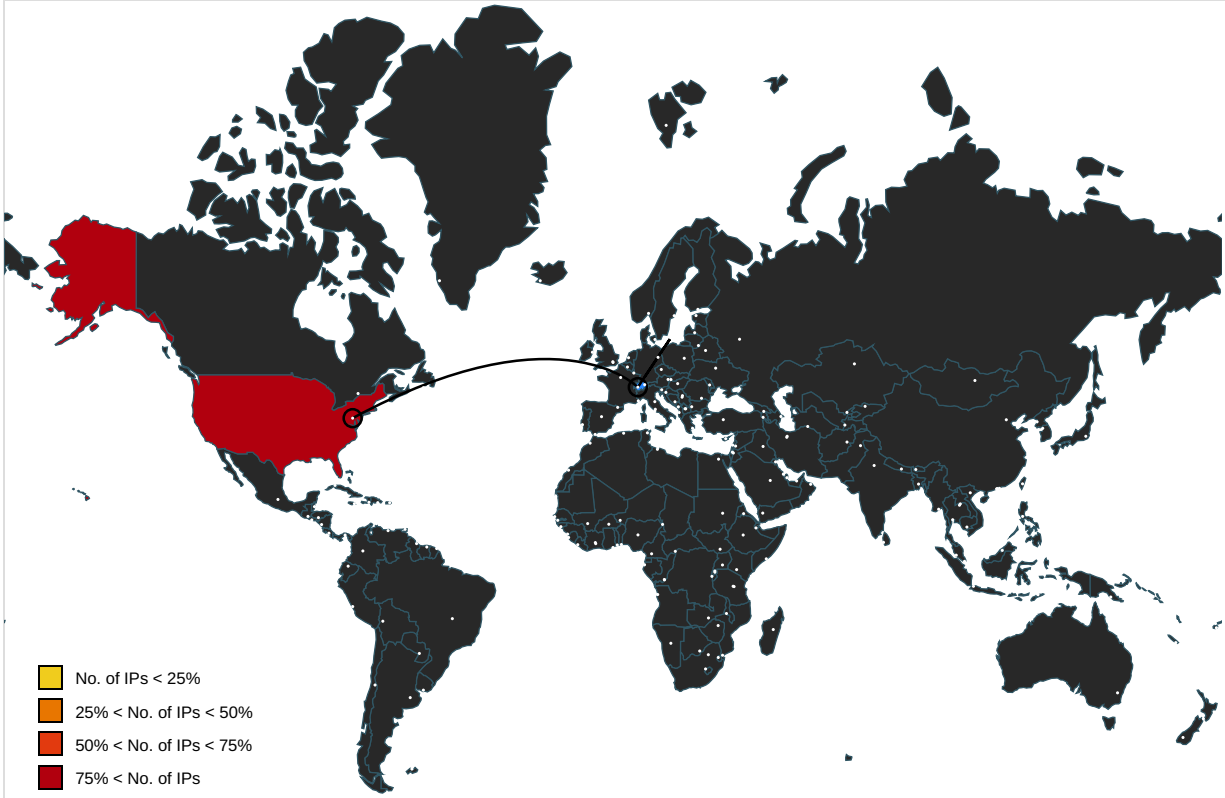
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.mi	explorer.exe, 00000003.00000000.412067253.000000000807C000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.438079821.000000000807C000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.395202609.000000000807C000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	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:	678081
Start date and time: 03/08/202214:51:07	2022-08-03 14:51:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6s1js8BzrC.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:	9
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: 71.1% (good quality ratio 60.3%) • Quality average: 45.5% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 79% • 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, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:53:09	Task Scheduler	Run new task: Firefox Default Browser Agent 3106851CBFE21B54 path: C:\Users\user\AppData\Roaming\twtgjvf

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\twtgjvf

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	7.053101995036968
Encrypted:	false
SSDEEP:	3072:O1CItAzXunlpY2Tw4gST76X9JfIruFeKQvd4xlYCjwm3Y:OgSllDwNS/6X9OihQvqb8m

MD5:	C9948059CDC5E0AEF9C193D605C7F659
SHA1:	0C00B2242C86487E305D53AEA8894100BDA41035
SHA-256:	80F503F4FD7E84B614FC5A50888629178996402D10E245193136C0AEE909B87B
SHA-512:	916CEFA7ECE9599A4AEA3B2E909B8F0537324203B4E5E5F4BD429F9A95DDA9DCA1D877F39F8FB5313F66D10EC66317DCEBD39ACD5BDEA465C8FB2CE016AC809D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 41%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.K...K...K...$...\...$...8...B...N...K.....$...m...$...J...$...J... RichK.....PE..L....Z.a.....,...B.....gg.....@....@.....D.....l0..<.....Pv..... .....6..@... .....text...@+.....,..... ..`.data....:...@...0...0.....@....rsrc...Pv.....x...`.....@..@..... ....

C:\Users\user\AppData\Roaming\twtgjvf: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):	7.053101995036968
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:	6s1js8BzrC.exe
File size:	186368
MD5:	c9948059cdc5e0aef9c193d605c7f659
SHA1:	0c00b2242c86487e305d53aea8894100bda41035
SHA256:	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b
SHA512:	916cefa7ece9599a4aea3b2e909b8f0537324203b4e5e5f4bd429f9a95dda9dca1d877f39f8fb5313f66d10ec66317dcebd39acd5bdea465c8fb2ce016ac809d
SSDEEP:	3072:O1CItAzXunlpY2Tw4gST76X9JfIruFeKQvd4xlYCjwm3Y:OgSllDwNS/6X9OihQvqb8m
TLSH:	7704BE2137E0CC32D1E7693058B4C6B16A7FBD626BB8998F37A4362E1F617C15A34316
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.K...K...K...$...\...$...8...B...N...K.....$...m...$...J...$...J...RichK.....PE..L....Z.a.....

File Icon

Icon Hash:	8a9099a9ca8ed2f2

Static PE Info

General

Entrypoint:	0x416767
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:	0x61D55A8E [Wed Jan 5 08:45:02 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	19d26450af6fae284e6a28f691d90382

Entrypoint Preview

Instruction
call 00007F9AC0B4F589h
jmp 00007F9AC0B48F4Eh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
call 00007F9AC0B490FCh
xchg cl, ch
jmp 00007F9AC0B490E4h
call 00007F9AC0B490F3h
fxch st(0), st(1)
jmp 00007F9AC0B490DBh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007F9AC0B490D1h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007F9AC0B490C6h
fldpi
fsubrp st(1), st(0)
or ch, ch
je 00007F9AC0B490C4h

Instruction
fchs
ret
fabs
fld st(0), st(0)
fld st(0), st(0)
fld1
fsubrp st(1), st(0)
fxch st(0), st(1)
fld1
faddp st(1), st(0)
fmulp st(1), st(0)
ftst
wait
fstsw word ptr [ebp-000000A0h]
wait
test byte ptr [ebp-0000009Fh], 00000001h
jne 00007F9AC0B490C7h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007F9AC0B4F74Fh
fstp st(0)
fld tbyte ptr [004024CAh]
ret
fstp st(0)
or cl, cl
je 00007F9AC0B490CDh
fstp st(0)
fldpi
or ch, ch
je 00007F9AC0B490C4h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007F9AC0B490B9h
fchs
ret
fstp st(0)
jmp 00007F9AC0B4F725h
fstp st(0)
mov cl, ch
jmp 00007F9AC0B490C2h
call 00007F9AC0B4908Eh
jmp 00007F9AC0B4F730h
int3
int3
int3
int3
int3
int3

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2306c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20a8000	0x7650	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x3680	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x22b40	0x22c00	False	0.7594916254496403	data	7.427480094498362	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x24000	0x2083ad0	0x3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x20a8000	0x7650	0x7800	False	0.6780924479166667	data	6.264422446606695	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

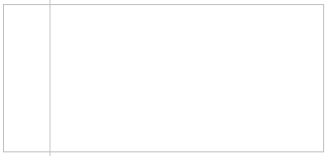
Name	RVA	Size	Type	Language	Country
RT_ICON	0x20a8300	0xea8	data	Kannada	Kanada
RT_ICON	0x20a91a8	0x8a8	data	Kannada	Kanada
RT_ICON	0x20a9a50	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20a9fb8	0x25a8	data	Kannada	Kanada
RT_ICON	0x20ac560	0x10a8	data	Kannada	Kanada
RT_ICON	0x20ad608	0x988	data	Kannada	Kanada
RT_ICON	0x20adf90	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_STRING	0x20ae608	0x67a	data	French	Switzerland
RT_STRING	0x20aec88	0x566	data	French	Switzerland
RT_STRING	0x20af1f0	0x45e	data	French	Switzerland
RT_GROUP_ICON	0x20ae3f8	0x68	data	Kannada	Kanada
RT_VERSION	0x20ae470	0x194	data		
None	0x20ae460	0xa	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	FoldStringA, GetLocalTime, InterlockedDecrement, GetLocaleInfoA, InterlockedCompareExchange, _hwrite, CancelWaitableTimer, GetSystemDirectoryA, CreateEventW, ReadConsoleA, VerifyVersionInfoA, BuildCommDCBA, GetConsoleAliasExesLengthA, SetSystemTimeAdjustment, PeekConsoleInputA, EnumDateFormatsA, CreateFileW, RegisterWaitForSingleObjectEx, LoadLibraryA, WaitNamedPipeA, GetEnvironmentStrings, FindResourceExA, VirtualProtect, GetFirmwareEnvironmentVariableW, GetModuleFileNameW, BeginUpdateResourceW, EnumCalendarInfoExW, WriteConsoleOutputCharacterW, WriteConsoleA, LoadLibraryW, DeleteFileW, LocalAlloc, GetProcAddress, GetModuleHandleW, GetUserDefaultLCID, FindFirstChangeNotificationW, HeapUnlock, GetCalendarInfoW, SetConsoleTitleA, GetBinaryTypeW, GetComputerNameExA, FindNextFileA, OpenJobObjectA, HeapValidate, _lclose, GetComputerNameW, SetFileShortNameW, TlsSetValue, SetCalendarInfoW, SetComputerNameW, CreateDirectoryExA, InitializeCriticalSectionAndSpinCount, FindFirstChangeNotificationA, GetVolumePathNameW, GetProcessHandleCount, GetThreadLocale, GetSystemDefaultLangID, GetCurrentProcess, ReadFile, GetStringTypeW, HeapSize, GetDiskFreeSpaceA, HeapReAlloc, RaiseException, RtlUnwind, MultiByteToWideChar, GetCommandLineW, HeapSetInformation, GetStartupInfoW, EncodePointer, HeapAlloc, GetLastError, HeapFree, IsProcessorFeaturePresent, SetFilePointer, EnterCriticalSection, LeaveCriticalSection, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, DecodePointer, TerminateProcess, TlsAlloc, TlsGetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, ExitProcess, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, WriteFile, GetStdHandle, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetStdHandle, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, Sleep, LCMapStringW, WriteConsoleW
USER32.dll	ClientToScreen

Possible Origin

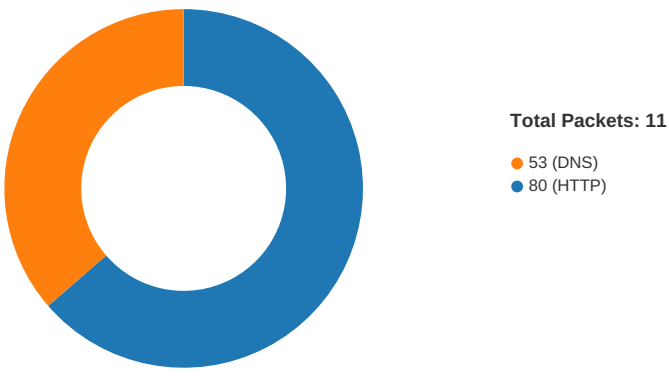
Language of compilation system	Country where language is spoken	Map
Kannada	Kanada	
French	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.634.118.39.104 9722802851815 08/03/22-14:53:10.081323	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49722	80	192.168.2.6	34.118.39.10

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 14:53:10.044868946 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:10.081063032 CEST	80	49722	34.118.39.10	192.168.2.6
Aug 3, 2022 14:53:10.081182957 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:10.081322908 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:10.081337929 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:10.117552042 CEST	80	49722	34.118.39.10	192.168.2.6
Aug 3, 2022 14:53:10.206475973 CEST	80	49722	34.118.39.10	192.168.2.6
Aug 3, 2022 14:53:10.254339933 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:40.206978083 CEST	80	49722	34.118.39.10	192.168.2.6
Aug 3, 2022 14:53:40.207204103 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:40.207360983 CEST	49722	80	192.168.2.6	34.118.39.10
Aug 3, 2022 14:53:40.243535995 CEST	80	49722	34.118.39.10	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 14:53:10.025039911 CEST	49507	53	192.168.2.6	8.8.8.8
Aug 3, 2022 14:53:10.042541981 CEST	53	49507	8.8.8.8	192.168.2.6
Aug 3, 2022 14:53:10.226603985 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 3, 2022 14:53:11.254611015 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 3, 2022 14:53:12.254663944 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 3, 2022 14:53:14.259399891 CEST	53	55201	8.8.8.8	192.168.2.6
Aug 3, 2022 14:53:15.294389963 CEST	53	55201	8.8.8.8	192.168.2.6
Aug 3, 2022 14:53:17.272901058 CEST	53	55201	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 3, 2022 14:53:15.295216084 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 3, 2022 14:53:17.272984982 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2022 14:53:10.025039911 CEST	192.168.2.6	8.8.8.8	0xab68	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:10.226603985 CEST	192.168.2.6	8.8.8.8	0x9e47	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:11.254611015 CEST	192.168.2.6	8.8.8.8	0x9e47	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:12.254663944 CEST	192.168.2.6	8.8.8.8	0x9e47	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 14:53:10.042541981 CEST	8.8.8.8	192.168.2.6	0xab68	No error (0)	host-file-host6.com		34.118.39.10	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:14.259399891 CEST	8.8.8.8	192.168.2.6	0x9e47	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:15.294389963 CEST	8.8.8.8	192.168.2.6	0x9e47	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 14:53:17.272901058 CEST	8.8.8.8	192.168.2.6	0x9e47	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- foxtykohl.net
  - host-file-host6.com

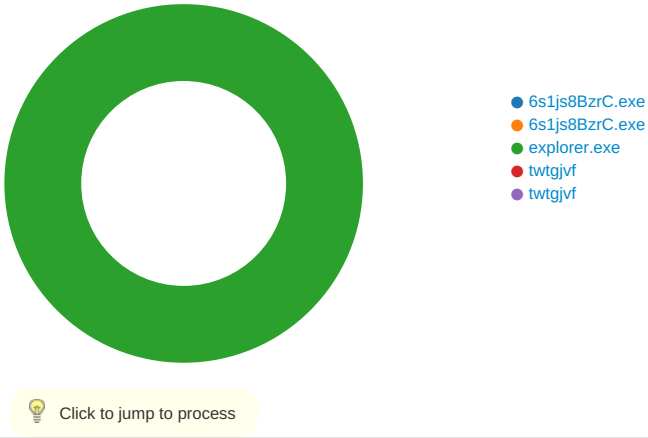
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49722	34.118.39.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2022 14:53:10.081322908 CEST	110	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://foxtykohl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 121 Host: host-file-host6.com
Aug 3, 2022 14:53:10.206475973 CEST	110	IN	HTTP/1.1 200 OK server: nginx/1.20.1 date: Wed, 03 Aug 2022 12:53:10 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: 6s1js8BzrC.exe PID: **1056**, Parent PID: **4232**

General

Target ID:	0
Start time:	14:52:11
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\6s1js8BzrC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\6s1js8BzrC.exe"
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C9948059CDC5E0AEF9C193D605C7F659
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 6s1js8BzrC.exe PID: **504**, Parent PID: **1056**

General

Target ID:	2
Start time:	14:52:15
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\6s1js8BzrC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\6s1js8BzrC.exe"
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C9948059CDC5E0AEF9C193D605C7F659
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: 00000002.00000002.445865427.0000000002051000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.445757308.0000000002030000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **3688**, Parent PID: **504**

General

Target ID:	3
Start time:	14:52:23
Start date:	03/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
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: 00000003.00000000.423194052.0000000004D61000.00000020.80000000.00040000.00000000.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\twtgjvf	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	4D61F42	CopyFileW
C:\Users\user\AppData\Roaming\twtgjvf\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	4D61F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\6s1js8BzrC.exe	success or wait	1	4D61F53	DeleteFileW
C:\Users\user\AppData\Roaming\twtgjvf:Zone.Identifier	success or wait	1	4D61F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\twtgjvf	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 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 0f fd 6d fd 4b fd 03 fd 4b fd 03 fd 4b fd 03 fd 24 fd fd fd 5c fd 03 fd 24 fd fd fd 38 fd 03 fd 42 fd fd fd 4e fd 03 fd 4b fd 02 fd fd fd 03 fd 24 fd fd fd 6d fd 03 fd 24 fd fd fd 4a fd 03 fd 24 fd fd fd 4a fd 03 fd 52 69 63 68 4b fd 03 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 5a fd 61 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$mKKK$\$8BNK$ mJJRichKPELZa	success or wait	2	4D61F42	CopyFileW
C:\Users\user\AppData\Roaming\twtgjvf: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	4D61F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: twtgjvf PID: **2912**, Parent PID: **696**

General

Target ID:	6
Start time:	14:53:10
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\twtgjvf
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\twtgjvf
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C9948059CDC5E0AEF9C193D605C7F659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, Virustotal, Browse
Reputation:	low

Analysis Process: twtgjvf PID: **2756**, Parent PID: **2912**

General

Target ID:	7
Start time:	14:53:13
Start date:	03/08/2022

Path:	C:\Users\user\AppData\Roaming\twtgjvf
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\twtgjvf
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C9948059CDC5E0AEF9C193D605C7F659
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: 00000007.00000002.503883541.00000000004A0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000007.00000002.503917126.00000000005B1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly