ID: 736951
Sample Name: P2SMn3jloH.exe
Cookbook: default.jbs
Time: 12:24:08
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

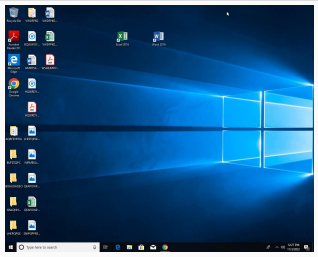
Windows Analysis Report

P2SMn3jloH.exe

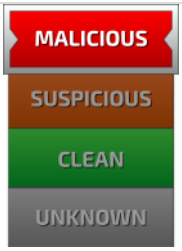
Overview

General Information

Sample Name:	P2SMn3jloH.exe
Analysis ID:	736951
MD5:	0779f7b34e9079..
SHA1:	31f2cf1dc970fdf...
SHA256:	5c7ff5f2993bdb6..
Tags:	exe SnakeKeylogger
Infos:	



Detection



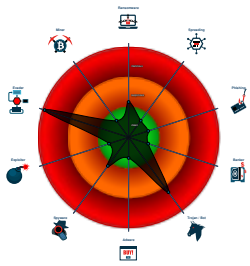
SmokeLoader

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

Signatures

- Multi AV Scanner detection for subm...
- Benign windows process drops PE f...
- Malicious sample detected (through...
- 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...
- 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**
- P2SMn3jloH.exe (PID: 4020 cmdline: C:\Users\user\Desktop\P2SMn3jloH.exe MD5: 0779F7B34E9079944427B8260B49C205)
  - P2SMn3jloH.exe (PID: 3420 cmdline: C:\Users\user\Desktop\P2SMn3jloH.exe MD5: 0779F7B34E9079944427B8260B49C205)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- utisvaa (PID: 1280 cmdline: C:\Users\user\AppData\Roaming\utisvaa MD5: 0779F7B34E9079944427B8260B49C205)
  - utisvaa (PID: 5332 cmdline: C:\Users\user\AppData\Roaming\utisvaa MD5: 0779F7B34E9079944427B8260B49C205)
- **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
0000000D.00000002.409013280.0000000001F51000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000D.00000002.409013280.0000000001F51000.00000004.10000000.00040000.00000000.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

Source	Rule	Description	Author	Strings
0000000C.00000002.395157811.00000000006D8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x5218:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000002.350515025.0000000001F51000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.350515025.0000000001F51000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$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
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.P2SMn3jloH.exe.21b15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
1.2.P2SMn3jloH.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.0.utisvaa.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.0.utisvaa.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.0.utisvaa.400000.5.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

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)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

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

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected SmokeLoader

Remote Access Functionality

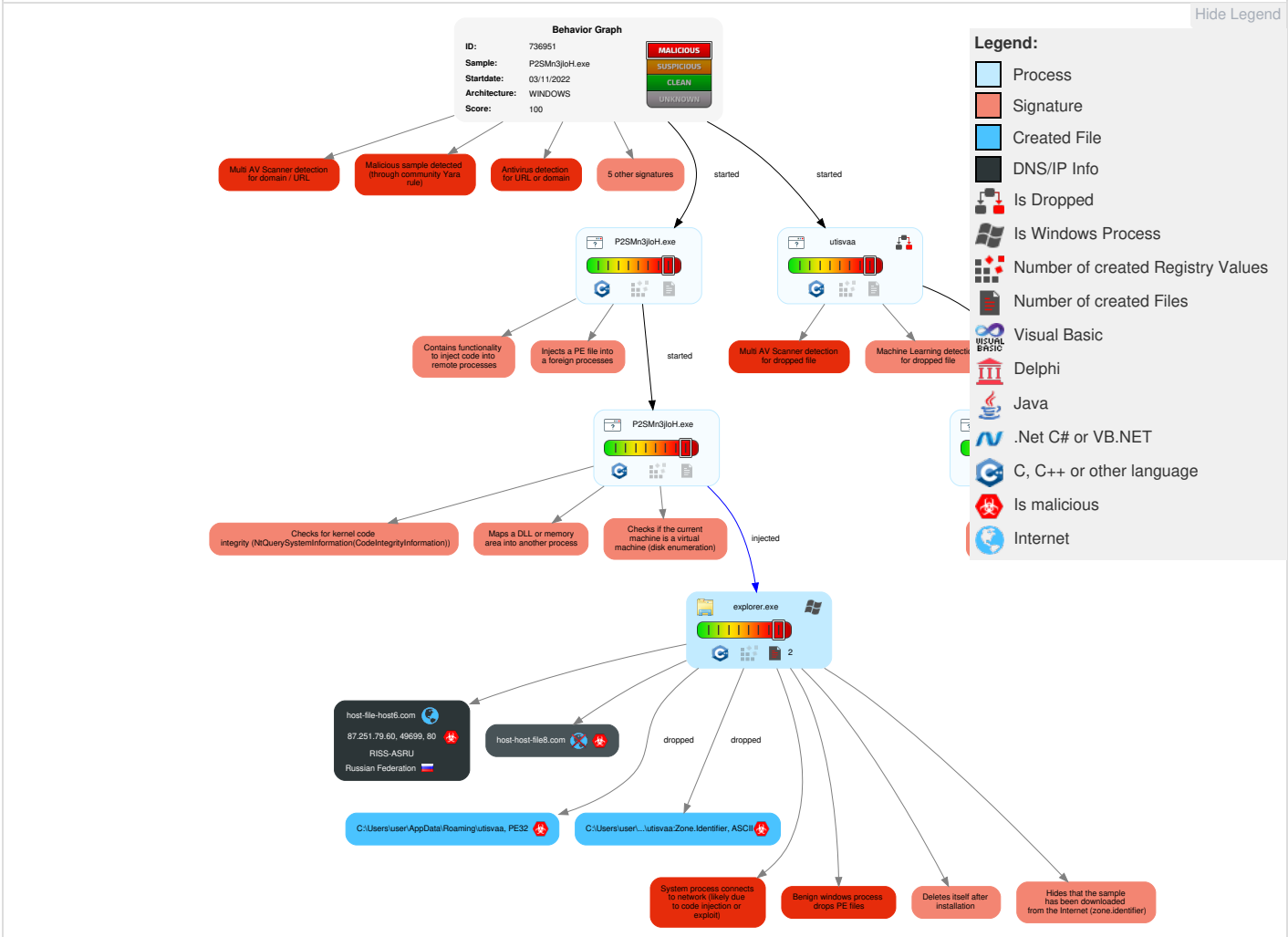
Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	5 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	4 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 6 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

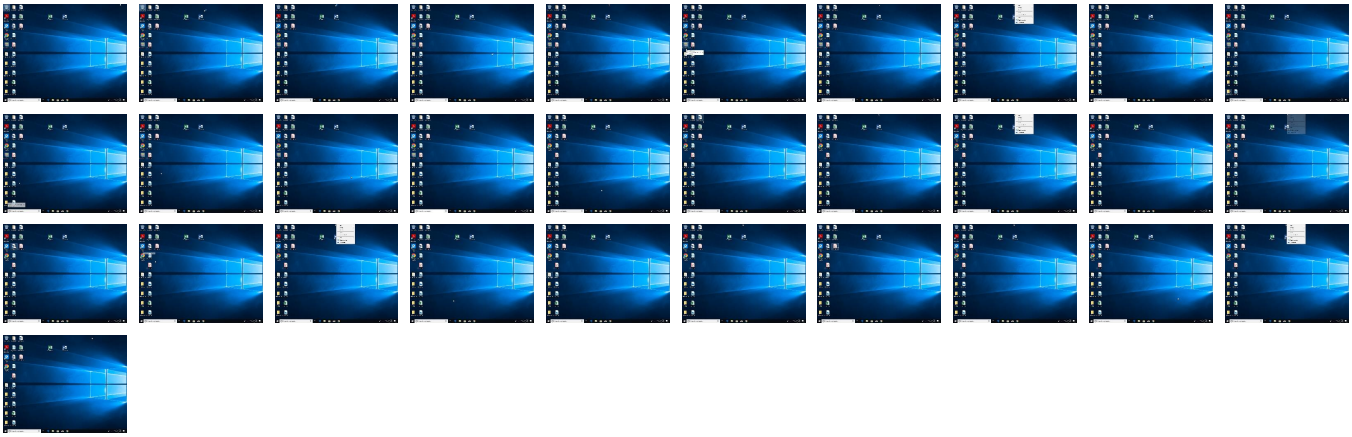
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
P2SMn3jloH.exe	46%	ReversingLabs	Win32.Trojan.Generic	

Source	Detection	Scanner	Label	Link
P2SMn3jloH.exe	35%	Virustotal		Browse
P2SMn3jloH.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\utisvaa	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\utisvaa	46%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Roaming\utisvaa	35%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.utisvaa.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.P2SMn3jloH.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.utisvaa.21a15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.P2SMn3jloH.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.P2SMn3jloH.exe.21b15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.P2SMn3jloH.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.P2SMn3jloH.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.utisvaa.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.utisvaa.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
host-file-host6.com	18%	Virustotal		Browse
host-host-file8.com	17%	Virustotal		Browse

URLs

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

Domains and IPs

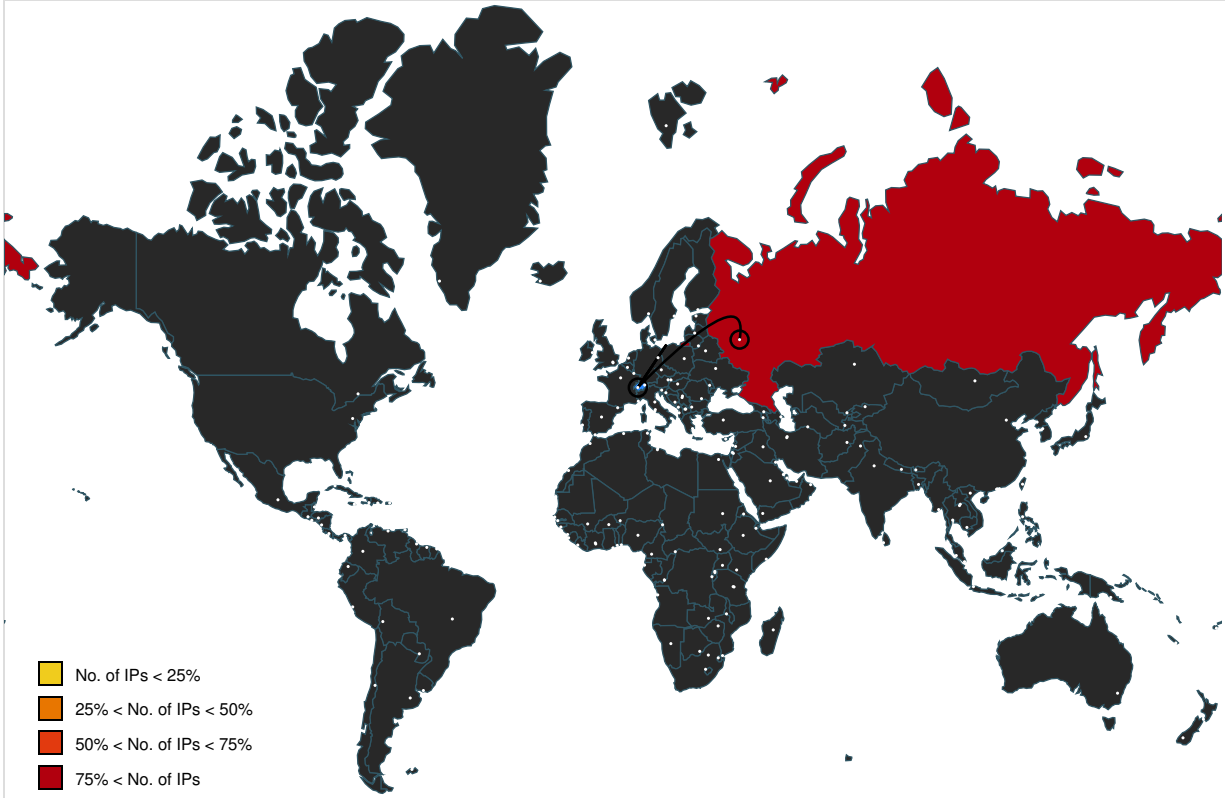
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	87.251.79.60	true	true	• 18%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true	• 17%, 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
87.251.79.60	host-file-host6.com	Russian Federation		20803	RISS-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736951
Start date and time:	2022-11-03 12:24:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P2SMn3jloH.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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: 93.8% (good quality ratio 87.2%) • Quality average: 75.4% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
12:26:08	Task Scheduler	Run new task: Firefox Default Browser Agent 18B1406226926BB9 path: C:\Users\user\AppData\Roaming\utisvaa

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\utisvaa

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	215552
Entropy (8bit):	6.969285988131741
Encrypted:	false

SSDEEP:	3072:zmRA4EwqbftQPtRLITsLxmE6pf5ADM8VGQqf/r4nnFxtHglCFBQx:zmyHbFeRRILgEFl8sfTuxtHMOq
MD5:	0779F7B34E9079944427B8260B49C205
SHA1:	31F2CF1DC970FDFAF51B9AAB2C9E0B9715FB53EC
SHA-256:	5C7FF5F2993BDB60D15A567DFAEF41DCD30875D6629F2775ACDB190E01DCEF87
SHA-512:	E22E6186F82A3EB329874C246A9D64CC45EDE3A6EE93447DCDC3E93CB0C52A40B9CFB36E0350E1CDC1487D47BB94D3478B49376C2DE5C64A82DA545C2C976B3E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46% • Antivirus: Virustotal, Detection: 35%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.^.".^.".^.".@...C.".@.....".y.Y.Y.".^.#...".@...I.".@..._.".@..._.".Rich^."..... .....PE..L...#H.a..... .....@.....D.....P.....C.....HC..@..... ... .text...J..... ..`.data.....@....rsrc....C.....D.....@..@..... ....

C:\Users\user\AppData\Roaming\utisvaa: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):	6.969285988131741
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:	P2SMn3jloH.exe
File size:	215552
MD5:	0779f7b34e9079944427b8260b49c205
SHA1:	31f2cf1dc970fdfaf51b9aab2c9e0b9715fb53ec
SHA256:	5c7ff5f2993bdb60d15a567dfaef41dcd30875d6629f2775acdb190e01dcef87
SHA512:	e22e6186f82a3eb329874c246a9d64cc45ede3a6ee93447dcdc3e93cb0c52a40b9cfb36e0350e1cdc1487d47bb94d3478b49376c2de5c64a82da545c2c976b3e
SSDEEP:	3072:zmRA4EwqbftQPtRLITsLxmE6pf5ADM8VGQqf/r4nnFxtHglCFBQx:zmyHbFeRRILgEFl8sfTuxtHMOq
TLSH:	D424CF233AD0C073E27E92758815D7B55A7BB87405365A8B3BE8567C8F313D2AE2434B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.^.".^.".^.".@...C.".@.....".y.Y.Y.".^.#...".@...I.".@..._.".@..._.".Rich^."..... .....PE..L...#H.a..... .....

File Icon

Icon Hash:	aaf8c8eaa2e4a0c1

Static PE Info

General

Entrypoint:	0x4094f6
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:	0x61884823 [Sun Nov 7 21:41:55 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:	8fb85d04360d27123c3a8e1c2ffb7f7e

Entrypoint Preview

Instruction
call 00007F1E44C53682h
jmp 00007F1E44C4B66Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007F1E44C4B804h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007F1E44C4B7F9h
push eax
call 00007F1E44C4ACC2h
pop ecx
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F1E44C4B855h
call 00007F1E44C50160h
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [004312D8h]
je 00007F1E44C4B804h
mov ecx, dword ptr [004311F0h]
test dword ptr [eax+70h], ecx
jne 00007F1E44C4B7F9h

Instruction
call 00007F1E44C4CA01h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [004310F8h]
je 00007F1E44C4B808h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [004311F0h]
test dword ptr [eax+70h], ecx
jne 00007F1E44C4B7FAh
call 00007F1E44C538B9h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007F1E44C4B806h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007F1E44C4B7FCh
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 14h
mov eax, dword ptr [004307FCh]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push esi
xor ebx, ebx

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	0x1e7e4	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18b000	0x4310	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	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	0x4348	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x220	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x1e44a	0x1e600	False	0.5128600823045267	data	6.400320083175456	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x20000	0x16ade4	0x11c00	False	0.8920417033450704	data	7.6284485167398906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x18b000	0x4310	0x4400	False	0.6488970588235294	data	6.048423243299262	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RIWEZOZAC	0x18e700	0x55f	ASCII text, with very long lines (1375), with no line terminators	Romanian	Romania
RT_ICON	0x18b330	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Romanian	Romania
RT_ICON	0x18bbd8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Romanian	Romania
RT_ICON	0x18c2a0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Romanian	Romania
RT_ICON	0x18c808	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Romanian	Romania
RT_ICON	0x18d8b0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Romanian	Romania
RT_ICON	0x18e238	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Romanian	Romania
RT_STRING	0x18ee08	0xb6	data	Romanian	Romania
RT_STRING	0x18eec0	0x2ae	data	Romanian	Romania
RT_STRING	0x18f170	0x19c	data	Romanian	Romania
RT_ACCELERATOR	0x18ec60	0x58	data	Romanian	Romania
RT_GROUP_ICON	0x18e6a0	0x5a	data	Romanian	Romania
RT_VERSION	0x18ecb8	0x14c	Intel 80386 COFF executable, no relocation info, not stripped, 52 sections, symbol offset=0x5f0053, 4522070 symbols, optional header size 82, created Sat Mar 7 05:34:56 1970		

Imports

DLL	Import
KERNEL32.dll	LocalSize, InterlockedExchange, GetTickCount, CopyFileExA, GetConsoleAliasExesLengthW, EnumSystemCodePagesA, TlsGetValue, MoveFileWithProgressA, VerifyVersionInfoW, LocalUnlock, DebugBreak, GlobalGetAtomNameA, MapViewOfFileEx, GetWindowsDirectoryA, GetModuleHandleA, lstrlenW, GlobalDeleteAtom, SizeofResource, WriteConsoleInputA, CopyFileW, SetWaitableTimer, GetVersionExA, FindResourceW, OpenEventA, SearchPathA, GetThreadPriority, CallNamedPipeA, GetProcAddress, GlobalAlloc, SetFileTime, GetConsoleAliasesLengthA, GetComputerNameA, GetSystemWindowsDirectoryA, GetMailslotInfo, GetTapeParameters, OpenJobObjectW, GetPrivateProfileIntA, ReadConsoleInputW, _lread, LockFile, GetPrivateProfileStructW, GetDiskFreeSpaceExW, DefineDosDeviceW, GetACP, SetProcessAffinityMask, GlobalFindAtomW, InterlockedDecrement, VerifyVersionInfoA, CreateActCtxW, FindNextVolumeA, GetComputerNameW, CancelDeviceWakeupRequest, EnumCalendarInfoA, InterlockedCompareExchange, GetPrivateProfileStructA, EnumCalendarInfoW, EnterCriticalSection, InterlockedIncrement, GetNamedPipeHandleStateW, AreFileApisANSI, LoadLibraryA, SetLastError, WriteConsoleW, GetVolumeInformationA, OpenFileMappingA, LoadLibraryW, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, RtlUnwind, RaiseException, GetLastError, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapReAlloc, HeapAlloc, MoveFileA, DeleteFileA, GetStartupInfoW, LCMapStringA, WideCharToMultiByte, MultiByteToWideChar, LCMapStringW, GetCPInfo, GetModuleHandleW, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, HeapCreate, VirtualFree, VirtualAlloc, HeapSize, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, SetHandleCount, GetFileType, GetStartupInfoA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, GetStringTypeW, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, SetFilePointer, GetConsoleCP, GetConsoleMode, GetLocaleInfoW, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, CloseHandle, CreateFileA
GDI32.dll	GetCharWidthA
ADVAPI32.dll	SetThreadToken

Possible Origin

Language of compilation system	Country where language is spoken	Map
Romanian	Romania	

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:26:08.621563911 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:08.715183020 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:08.715354919 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:08.715487957 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:08.715517044 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:08.810715914 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:09.114351034 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:09.205801010 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:09.238164902 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:09.240447044 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:09.551862001 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:09.559798956 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:09.559859037 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:09.727560043 CET	80	49699	87.251.79.60	192.168.2.3
Nov 3, 2022 12:26:09.727715015 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:10.161276102 CET	49699	80	192.168.2.3	87.251.79.60
Nov 3, 2022 12:26:10.251888990 CET	80	49699	87.251.79.60	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:26:08.155019999 CET	49977	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:26:08.616261959 CET	53	49977	8.8.8.8	192.168.2.3
Nov 3, 2022 12:26:09.253171921 CET	57840	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:26:10.239569902 CET	57840	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:26:11.279532909 CET	57840	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:26:13.280474901 CET	53	57840	8.8.8.8	192.168.2.3
Nov 3, 2022 12:26:14.267415047 CET	53	57840	8.8.8.8	192.168.2.3
Nov 3, 2022 12:26:16.298055887 CET	53	57840	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 3, 2022 12:26:14.267613888 CET	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Nov 3, 2022 12:26:16.298300982 CET	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:26:08.155019999 CET	192.168.2.3	8.8.8.8	0x2a3b	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:09.253171921 CET	192.168.2.3	8.8.8.8	0x6e7e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:10.239569902 CET	192.168.2.3	8.8.8.8	0x6e7e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:11.279532909 CET	192.168.2.3	8.8.8.8	0x6e7e	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

DNS Answers

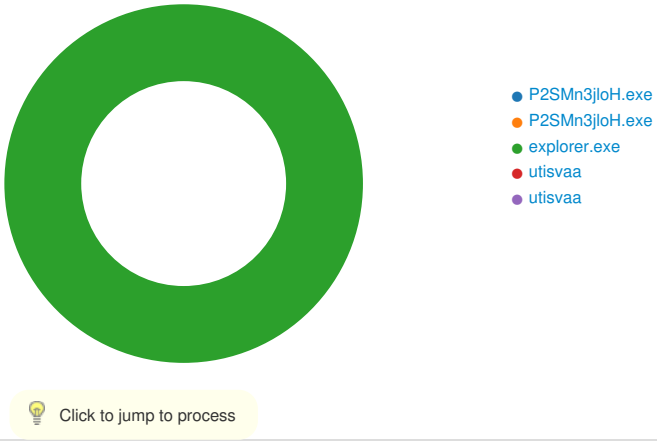
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:26:08.616261959 CET	8.8.8.8	192.168.2.3	0x2a3b	No error (0)	host-file-host6.com		87.251.79.60	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:13.280474901 CET	8.8.8.8	192.168.2.3	0x6e7e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:14.267415047 CET	8.8.8.8	192.168.2.3	0x6e7e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:16.298055887 CET	8.8.8.8	192.168.2.3	0x6e7e	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- dcihclar.com
  - host-file-host6.com

Statistics

Behavior



System Behavior

Analysis Process: P2SMn3jloH.exe PID: **4020**, Parent PID: **3452**

General	
Target ID:	0
Start time:	12:25:04
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\P2SMn3jloH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P2SMn3jloH.exe
Imagebase:	0x400000
File size:	215552 bytes
MD5 hash:	0779F7B34E9079944427B8260B49C205
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: 00000000.00000002.254069978.00000000005E9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: P2SMn3jloH.exe PID: **3420**, Parent PID: **4020**

General	
Target ID:	1
Start time:	12:25:05
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\P2SMn3jloH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P2SMn3jloH.exe
Imagebase:	0x400000
File size:	215552 bytes
MD5 hash:	0779F7B34E9079944427B8260B49C205
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: 00000001.00000002.350515025.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.350515025.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.350312010.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.350312010.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **3420**

General	
Target ID:	2
Start time:	12:25:11
Start date:	03/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000000.338679207.00000000057B1000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000002.00000000.338679207.00000000057B1000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\utisvaa	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	57B1F42	CopyFileW
C:\Users\user\AppData\Roaming\utisvaa\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	57B1F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\P2SMn3jloH.exe	success or wait	1	57B1F53	DeleteFileW
C:\Users\user\AppData\Roaming\utisvaa:Zone.Identifier	success or wait	1	57B1F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\utisvaa	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 1a fd 4c fd 5e fd 22 fd 5e fd 22 fd 5e fd 22 fd 40 fd fd fd 43 fd 22 fd 40 fd fd fd fd 22 fd 79 0b 59 fd 59 fd 22 fd 5e fd 23 fd fd fd 22 fd 40 fd fd fd 6c fd 22 fd 40 fd fd fd 5f fd 22 fd 40 fd fd fd 5f fd 22 fd 52 69 63 68 5e fd 22 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 23 48 fd 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 01 00 00 20 17 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$L^"^"^"@C"@"yY Y"^#"@l"@_"@_"Rich^"P EL#Ha	success or wait	2	57B1F42	CopyFileW
C:\Users\user\AppData\Roaming\utisvaa: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	57B1F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: utisvaa PID: **1280**, Parent PID: **1080**

General

Target ID:	12
Start time:	12:26:08
Start date:	03/11/2022
Path:	C:\Users\user\AppData\Roaming\utisvaa
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\utisvaa
Imagebase:	0x400000
File size:	215552 bytes
MD5 hash:	0779F7B34E9079944427B8260B49C205
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.395157811.00000000006D8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, ReversingLabs • Detection: 35%, Virustotal, Browse
Reputation:	low

Analysis Process: utisvaa PID: 5332, Parent PID: 1280

General

Target ID:	13
Start time:	12:26:11
Start date:	03/11/2022
Path:	C:\Users\user\AppData\Roaming\utisvaa
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\utisvaa
Imagebase:	0x400000
File size:	215552 bytes
MD5 hash:	0779F7B34E9079944427B8260B49C205
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.409013280.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000D.00000002.409013280.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.408977758.0000000001F30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000D.00000002.408977758.0000000001F30000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly