ID: 677963
Sample Name: Qv4fcaX7ft.exe
Cookbook: default.jbs
Time: 10:06:44
Date: 03/08/2022
Version: 35.0.0 Citrine

Table of Contents

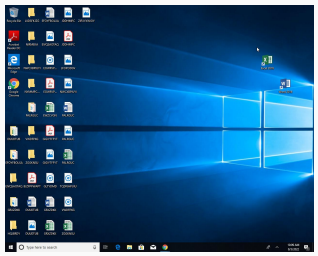
Windows Analysis Report

Qv4fcaX7ft.exe

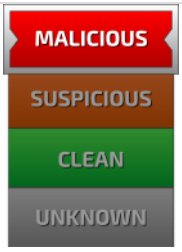
Overview

General Information

Sample Name:	Qv4fcaX7ft.exe
Analysis ID:	677963
MD5:	72ca6d61795722..
SHA1:	fbcd2b16d346c1...
SHA256:	5a3d6d5164f3d0..
Tags:	ArkeiStealer exe
Infos:	



Detection



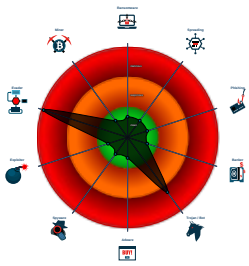
SmokeLoader

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...
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Machine Learning detection for sam...
- Injects a PE file into a foreign proce...
- Checks for kernel code integrity (NtQ...

Classification



Process Tree

- **System is w10x64**
- Qv4fcaX7ft.exe (PID: 5440 cmdline: "C:\Users\user\Desktop\Qv4fcaX7ft.exe" MD5: 72CA6D6179572214160DA9198D4DD496)
  - Qv4fcaX7ft.exe (PID: 3868 cmdline: "C:\Users\user\Desktop\Qv4fcaX7ft.exe" MD5: 72CA6D6179572214160DA9198D4DD496)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- switbwt (PID: 4844 cmdline: C:\Users\user\AppData\Roaming\switbwt MD5: 72CA6D6179572214160DA9198D4DD496)
  - switbwt (PID: 3868 cmdline: C:\Users\user\AppData\Roaming\switbwt MD5: 72CA6D6179572214160DA9198D4DD496)
- **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
00000006.00000000.495364437.0000000002E21000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.520149531.0000000002301000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.588777858.0000000000420000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.519610356.0000000000500000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000010.00000002.588984126.0000000001F61000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Qv4fcaX7ft.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.2.switbwt.24c15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
16.2.switbwt.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.Qv4fcaX7ft.exe.26215a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

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

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

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

Sample uses process hollowing technique

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

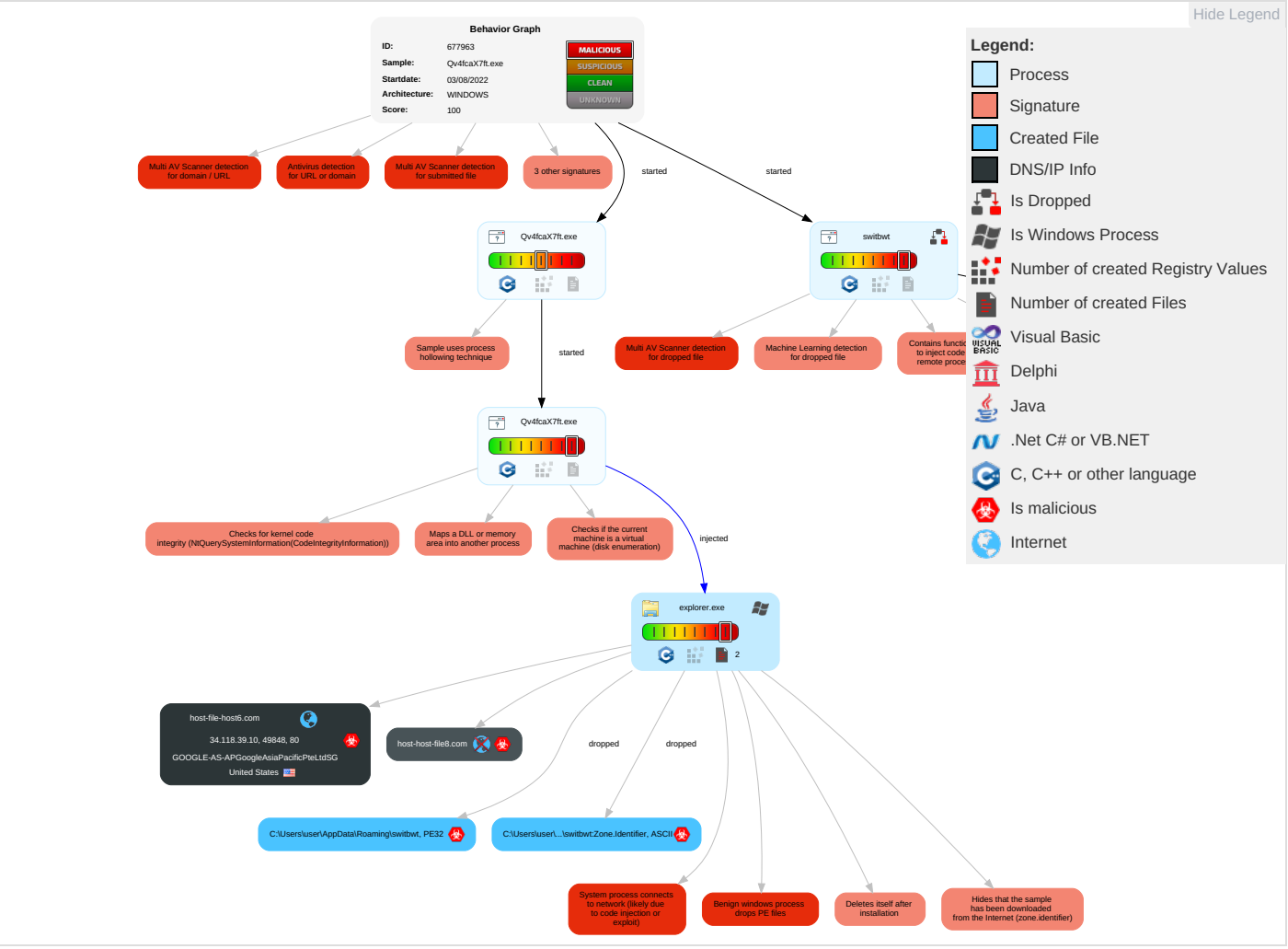
Yara detected SmokeLoader

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 Shared Modules	1 DLL Side-Loading	6 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	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	3 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)	6 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
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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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
Qv4fcaX7ft.exe	41%	Virustotal		Browse
Qv4fcaX7ft.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Qv4fcaX7ft.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.switbwt.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.Qv4fcaX7ft.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.switbwt.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.Qv4fcaX7ft.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Qv4fcaX7ft.exe.26215a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.switbwt.24c15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.switbwt.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Qv4fcaX7ft.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
16.0.switbwt.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.Qv4fcaX7ft.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.switbwt.400000.5.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://host-file-host6.com/	0%	URL Reputation	safe	
http://host-host-file8.com/	100%	URL Reputation	malware	

Domains and IPs

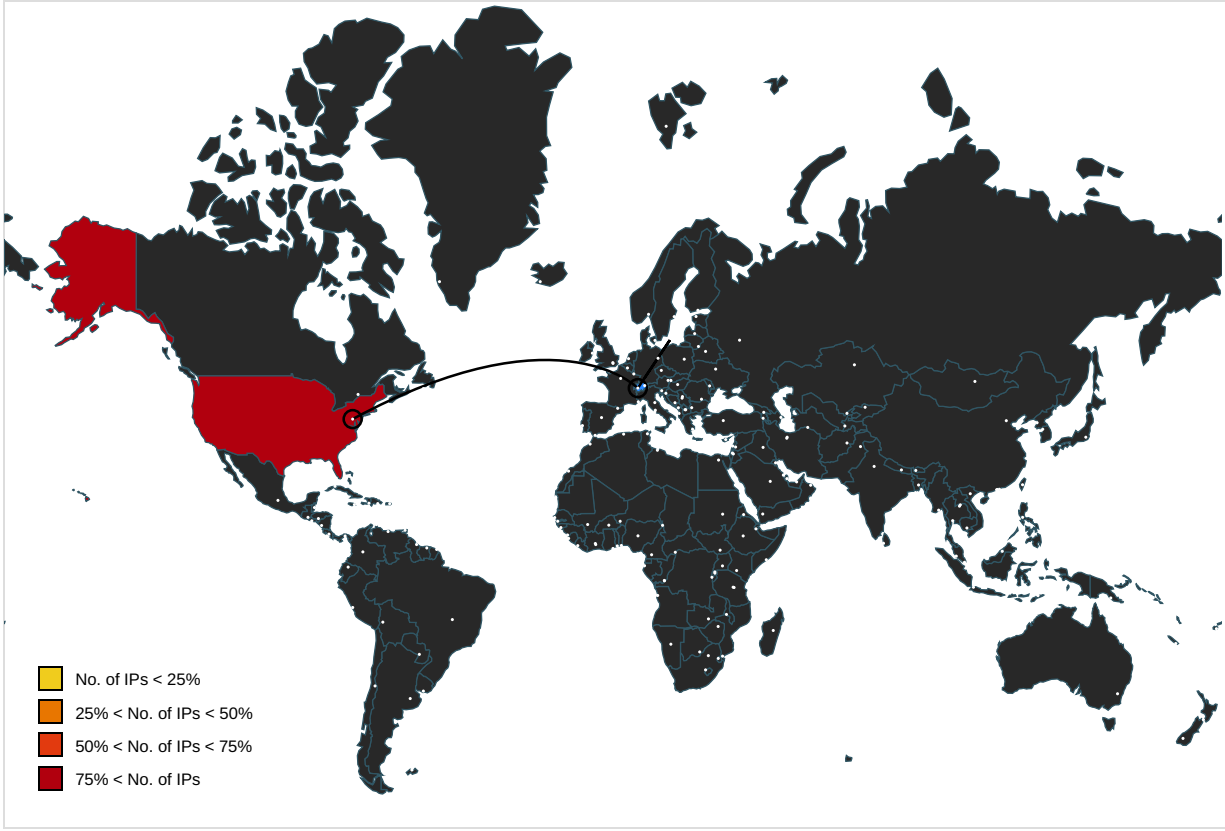
Contacted Domains

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

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:	677963
Start date and time: 03/08/202210:06:44	2022-08-03 10:06:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Qv4fcaX7ft.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:	21
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: 75%
HDC Information:	• Successful, ratio: 98.8% (good quality ratio 83.7%) • Quality average: 45.5% • Quality standard deviation: 27.3%

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, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target Qv4fcaX7ft.exe, PID 5440 because there are no executed function
- 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
10:08:52	Task Scheduler	Run new task: Firefox Default Browser Agent 273031370DC24B60 path: C:\Users\user\AppData\Roaming\switbwt

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\switbwt

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	185344
Entropy (8bit):	7.048410877691765
Encrypted:	false

SSDEEP:	3072:2YCYERsUNdM7FUSkqwICGcieDdIkQ0fE5BrvJPFya/bd/wyCGxqWoVim4eY:2YNlUA7mSkFKe5lJ0furjya/bZhqLO
MD5:	72CA6D6179572214160DA9198D4DD496
SHA1:	FBCD2B16D346C156F6083B0367B751DF0A8D6503
SHA-256:	5A3D6D5164F3D0A89F158B542C683752BA6071799D1B375D0B74A643C2CF7618
SHA-512:	8930448F089D464A52C1A84C817112B45BFD895790C32F33B2F56E4E57B8B5EBB30533422E5BD3E8DB9A7D8A3CE6E42F2CB0AE464C55DFD6C57BBDEE3A74F0C9
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....;I`.....(...B.....c.....@....@.....,..<.....w..... .....p6..@..... .....text...'.....(..... ..`.data....:...@...0...,.....@....rsrc....w.....x...\.....@..@..... ....

C:\Users\user\AppData\Roaming\switbwt: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):	7.048410877691765
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:	Qv4fcaX7ft.exe
File size:	185344
MD5:	72ca6d6179572214160da9198d4dd496
SHA1:	fbcd2b16d346c156f6083b0367b751df0a8d6503
SHA256:	5a3d6d5164f3d0a89f158b542c683752ba6071799d1b375d0b74a643c2cf7618
SHA512:	8930448f089d464a52c1a84c817112b45bfd895790c32f33b2f56e4e57b8b5ebb30533422e5bd3e8db9a7d8a3ce6e42f2cb0ae464c55dfd6c57bbdee3a74f0c9
SSDEEP:	3072:2YCYERsUNdM7FUSkqwICGcieDdIkQ0fE5BrvJPFya/bd/wyCGxqWoVim4eY:2YNlUA7mSkFKe5lJ0furjya/bZhqLO
TLSH:	4A04BE2133E1C072E5F75A705B7897F06A7FB932677886CB7764023E1E612C16A38356
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....;I`.....(.

File Icon

Icon Hash:	8a909989ca8ed2f2

Static PE Info

General	
Entrypoint:	0x416317
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:	0x60493B02 [Wed Mar 10 21:32:50 2021 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:	7b8da7d62de49809359b378ca66a56f3

Entrypoint Preview
Instruction
call 00007F41ACA377C9h
jmp 00007F41ACA3118Eh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
call 00007F41ACA3133Ch
xchg cl, ch
jmp 00007F41ACA31324h
call 00007F41ACA31333h
fxch st(0), st(1)
jmp 00007F41ACA3131Bh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007F41ACA31311h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007F41ACA31306h
fldpi
fsubrp st(1), st(0)

Instruction
or ch, ch
je 00007F41ACA31304h
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 00007F41ACA31307h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007F41ACA3798Fh
fstp st(0)
fld tbyte ptr [004024BAh]
ret
fstp st(0)
or cl, cl
je 00007F41ACA3130Dh
fstp st(0)
fldpi
or ch, ch
je 00007F41ACA31304h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007F41ACA312F9h
fchs
ret
fstp st(0)
jmp 00007F41ACA37965h
fstp st(0)
mov cl, ch
jmp 00007F41ACA31302h
call 00007F41ACA312CEh
jmp 00007F41ACA37970h
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	0x22c1c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20a8000	0x7780	.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	0x3670	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1dc	.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	0x2270e	0x22800	False	0.7573171422101449	data	7.418736880149773	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	0x7780	0x7800	False	0.68251953125	data	6.285235139121841	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x20ae4e0	0xe	data		
RT_ICON	0x20a8370	0xea8	data	Kannada	Kanada
RT_ICON	0x20a9218	0x8a8	data	Kannada	Kanada
RT_ICON	0x20a9ac0	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20aa028	0x25a8	data	Kannada	Kanada
RT_ICON	0x20ac5d0	0x10a8	data	Kannada	Kanada
RT_ICON	0x20ad678	0x988	data	Kannada	Kanada
RT_ICON	0x20ae000	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_STRING	0x20ae688	0x67a	data	French	Switzerland
RT_STRING	0x20aed08	0x566	data	French	Switzerland
RT_STRING	0x20af270	0x510	data	French	Switzerland
RT_GROUP_ICON	0x20ae468	0x68	data	Kannada	Kanada
RT_VERSION	0x20ae4f0	0x194	data		
None	0x20ae4d0	0xa	data		

Imports

DLL	Import

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

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 11

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 10:08:52.568114996 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:08:52.605123043 CEST	80	49848	34.118.39.10	192.168.2.5
Aug 3, 2022 10:08:52.605232954 CEST	49848	80	192.168.2.5	34.118.39.10

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 10:08:52.605427027 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:08:52.605448008 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:08:52.641733885 CEST	80	49848	34.118.39.10	192.168.2.5
Aug 3, 2022 10:08:52.641779900 CEST	80	49848	34.118.39.10	192.168.2.5
Aug 3, 2022 10:08:52.732853889 CEST	80	49848	34.118.39.10	192.168.2.5
Aug 3, 2022 10:08:52.777544975 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:09:22.733890057 CEST	80	49848	34.118.39.10	192.168.2.5
Aug 3, 2022 10:09:22.734090090 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:09:22.734146118 CEST	49848	80	192.168.2.5	34.118.39.10
Aug 3, 2022 10:09:22.770313978 CEST	80	49848	34.118.39.10	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 10:08:52.258240938 CEST	50588	53	192.168.2.5	8.8.8.8
Aug 3, 2022 10:08:52.552293062 CEST	53	50588	8.8.8.8	192.168.2.5
Aug 3, 2022 10:08:52.836795092 CEST	60470	53	192.168.2.5	8.8.8.8
Aug 3, 2022 10:08:53.872087002 CEST	60470	53	192.168.2.5	8.8.8.8
Aug 3, 2022 10:08:54.934542894 CEST	60470	53	192.168.2.5	8.8.8.8
Aug 3, 2022 10:08:56.892152071 CEST	53	60470	8.8.8.8	192.168.2.5
Aug 3, 2022 10:08:57.904903889 CEST	53	60470	8.8.8.8	192.168.2.5
Aug 3, 2022 10:08:58.967468977 CEST	53	60470	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 3, 2022 10:08:57.905052900 CEST	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
Aug 3, 2022 10:08:58.967550039 CEST	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2022 10:08:52.258240938 CEST	192.168.2.5	8.8.8.8	0x6edb	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:52.836795092 CEST	192.168.2.5	8.8.8.8	0x9275	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:53.872087002 CEST	192.168.2.5	8.8.8.8	0x9275	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:54.934542894 CEST	192.168.2.5	8.8.8.8	0x9275	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2022 10:08:52.552293062 CEST	8.8.8.8	192.168.2.5	0x6edb	No error (0)	host-file-host6.com		34.118.39.10	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:56.892152071 CEST	8.8.8.8	192.168.2.5	0x9275	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:57.904903889 CEST	8.8.8.8	192.168.2.5	0x9275	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 10:08:58.967468977 CEST	8.8.8.8	192.168.2.5	0x9275	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ocgywdvooe.com
  - host-file-host6.com

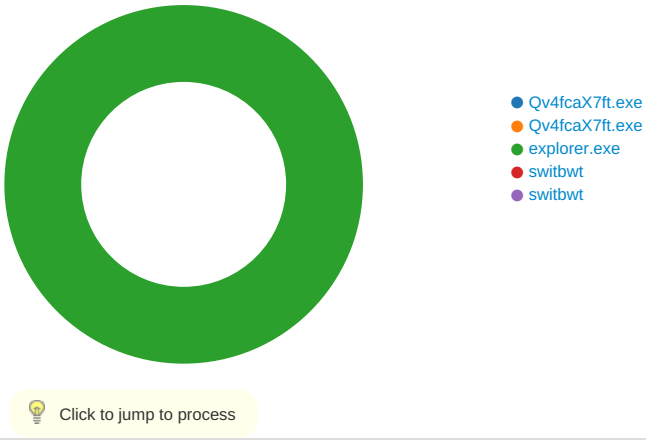
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49848	34.118.39.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2022 10:08:52.605427027 CEST	8448	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ocgywdvooe.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 250 Host: host-file-host6.com
Aug 3, 2022 10:08:52.732853889 CEST	8449	IN	HTTP/1.1 200 OK server: nginx/1.20.1 date: Wed, 03 Aug 2022 08:08:52 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: Qv4fcaX7ft.exe PID: **5440**, Parent PID: **5656**

General

Target ID:	0
Start time:	10:07:47
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\Qv4fcaX7ft.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Qv4fcaX7ft.exe"
Imagebase:	0x400000
File size:	185344 bytes
MD5 hash:	72CA6D6179572214160DA9198D4DD496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: Qv4fcaX7ft.exe PID: **3868**, Parent PID: **5440**

General

Target ID:	1
Start time:	10:07:51
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\Qv4fcaX7ft.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Qv4fcaX7ft.exe"
Imagebase:	0x400000
File size:	185344 bytes
MD5 hash:	72CA6D6179572214160DA9198D4DD496
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: 00000001.00000002.520149531.0000000002301000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.519610356.0000000000500000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **684**, Parent PID: **3868**

General

Target ID:	6
Start time:	10:07:59
Start date:	03/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
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: 00000006.00000000.495364437.0000000002E21000.00000020.80000000.00040000.00000000.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\switbwt	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	2E21F42	CopyFileW
C:\Users\user\AppData\Roaming\switbwt\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2E21F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Qv4fcaX7ft.exe	success or wait	1	2E21F53	DeleteFileW
C:\Users\user\AppData\Roaming\switbwt:Zone.Identifier	success or wait	1	2E21F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\switbwt	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 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 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 50 45 00 00 4c 01 03 00 02 3b 49 60 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 28 02	MZ@!L!This program cannot be run in DOS mode.$mKKK$\$8BNKmJ$JRichKPEL;I`(	success or wait	2	2E21F42	CopyFileW
C:\Users\user\AppData\Roaming\switbwt: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	2E21F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: switbwt PID: **4844**, Parent PID: **1040**

General

Target ID:	14
Start time:	10:08:52
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\switbwt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\switbwt
Imagebase:	0x400000
File size:	185344 bytes
MD5 hash:	72CA6D6179572214160DA9198D4DD496
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: switbwt PID: **3868**, Parent PID: **4844**

General

Target ID:	16
Start time:	10:09:01
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\switbwt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\switbwt
Imagebase:	0x400000

File size:	185344 bytes
MD5 hash:	72CA6D6179572214160DA9198D4DD496
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: 00000010.00000002.588777858.0000000000420000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000010.00000002.588984126.0000000001F61000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly