ID: 877010
Sample Name:
86NKwZGvwn.exe
Cookbook: default.jbs
Time: 14:26:09
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

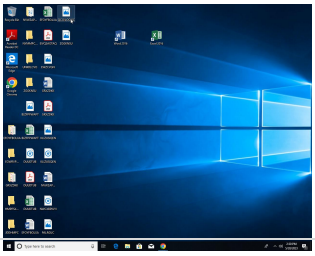
Windows Analysis Report

86NKwZGvwn.exe

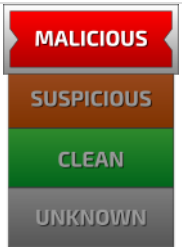
Overview

General Information

Sample Name:	86NKwZGvwn.exe
Original Sample Name:	40dcb3614c66…
Analysis ID:	877010
MD5:	40dcb3614c66…
SHA1:	4c25245ddbea…
SHA256:	069b749dc167…
Tags:	exe RecordBreaker
Infos:	



Detection



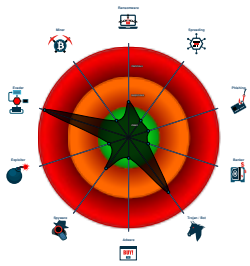
SmokeLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- 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…

Classification



Process Tree

- **System is w10x64**
- 86NKwZGvwn.exe (PID: 5764 cmdline: C:\Users\user\Desktop\86NKwZGvwn.exe MD5: 40DCB3614C663E7EF659044A6514D446)
  - 86NKwZGvwn.exe (PID: 5732 cmdline: C:\Users\user\Desktop\86NKwZGvwn.exe MD5: 40DCB3614C663E7EF659044A6514D446)
    - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- evcgwtu (PID: 6696 cmdline: C:\Users\user\AppData\Roaming\evcgwtu MD5: 40DCB3614C663E7EF659044A6514D446)
  - evcgwtu (PID: 6688 cmdline: C:\Users\user\AppData\Roaming\evcgwtu MD5: 40DCB3614C663E7EF659044A6514D446)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
SmokeLoader	The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.	• SMOKY SPIDER	http://security.neurolabs.club/2019/08/smokeloaders-hardcoded-domains-sneaky.htmlhttp://security.neurolabs.club/2019/10/dynamic-imports-and-working-around.htmlhttp://security.neurolabs.club/2020/04/diffing-malware-samples-using-bindiff.htmlhttp://security.neurolabs.club/2020/06/unpacking-smokeloader-and.htmlhttps://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader

Malware Configuration

Threatname: SmokeLoader


```
{
  "Version": 2020,
  "C2 list": [
    "http://host-file-host6.com/",
    "http://host-host-file8.com/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.528146469.0000000000808000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x7581:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000002.570702599.00000000006A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.570702599.00000000006A1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x2f4:$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
00000001.00000002.570658568.0000000000530000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.570658568.0000000000530000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x6f4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.86NKwZGvwn.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
6.2.evcgwtu.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
5.2.evcgwtu.22a15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.86NKwZGvwn.exe.7315a0.1.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

Found malware configuration

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)

Data Obfuscation

Detected unpacking (changes PE section rights)

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

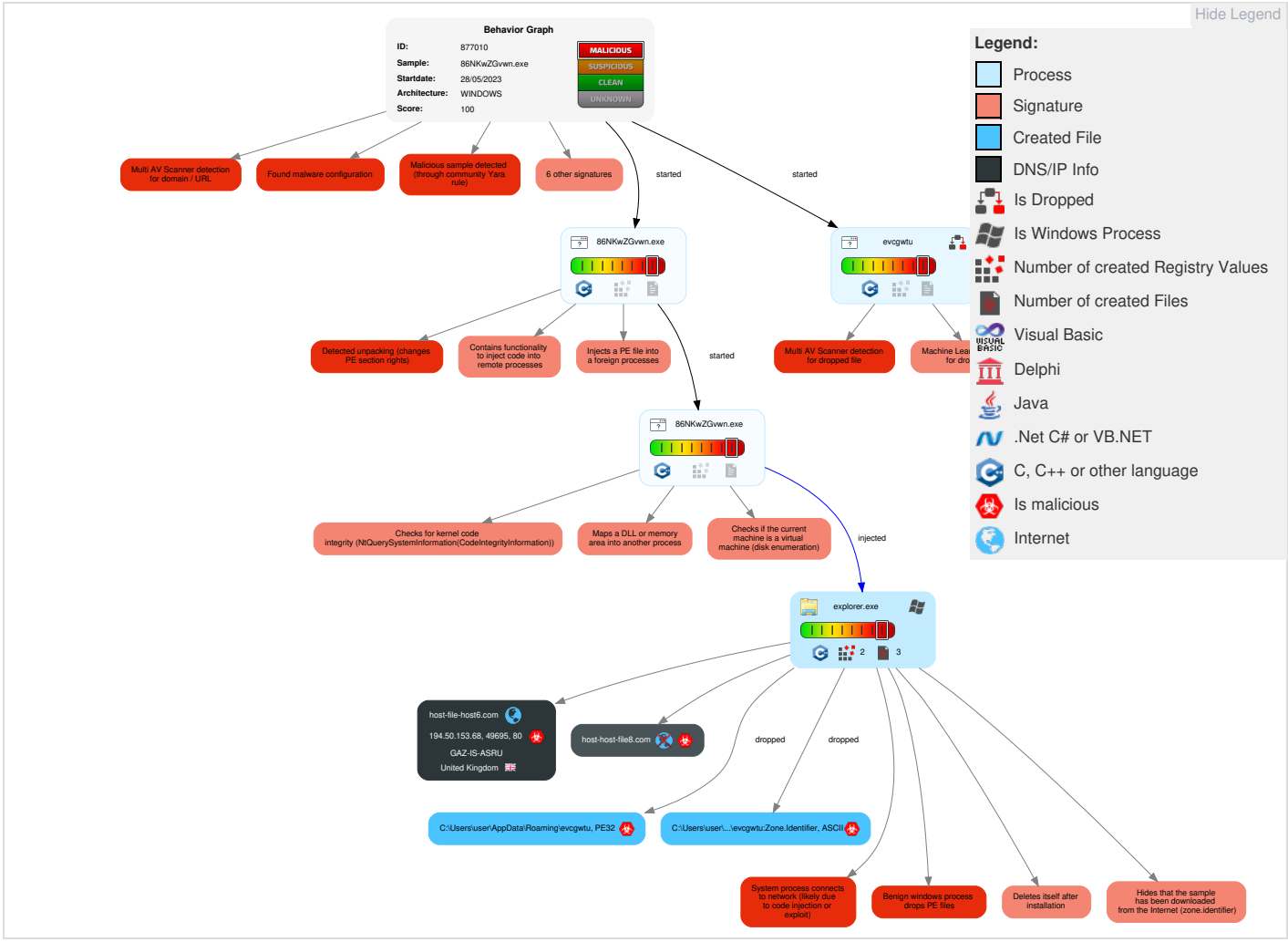
Remote Access Functionality

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	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Virtualization/Sandbox Evasion	LSASS Memory	4 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	5 1 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	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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 2 Software Packing	DCSync	1 File and Directory Discovery	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	1 4 System Information Discovery	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

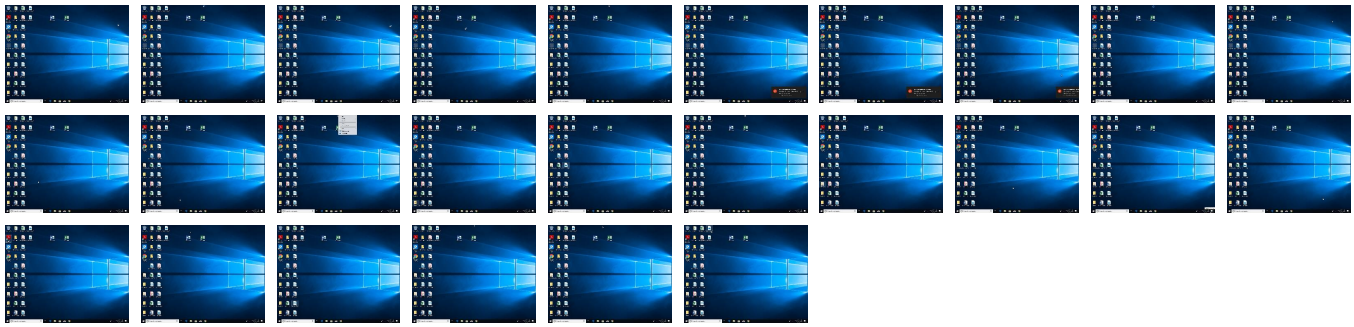
Behavior Graph



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
86NKwZGvwn.exe	38%	ReversingLabs		
86NKwZGvwn.exe	38%	Virustotal		Browse
86NKwZGvwn.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\evcgwtu	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\evcgwtu	38%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	0%	URL Reputation	safe	
http://host-file-host6.com/	0%	URL Reputation	safe	
http://host-host-file8.com/	100%	URL Reputation	malware	
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host6.com	194.50.153.68	true	true	• 22%, Virustotal, Browse	unknown
host-host-file8.com	unknown	unknown	true		unknown

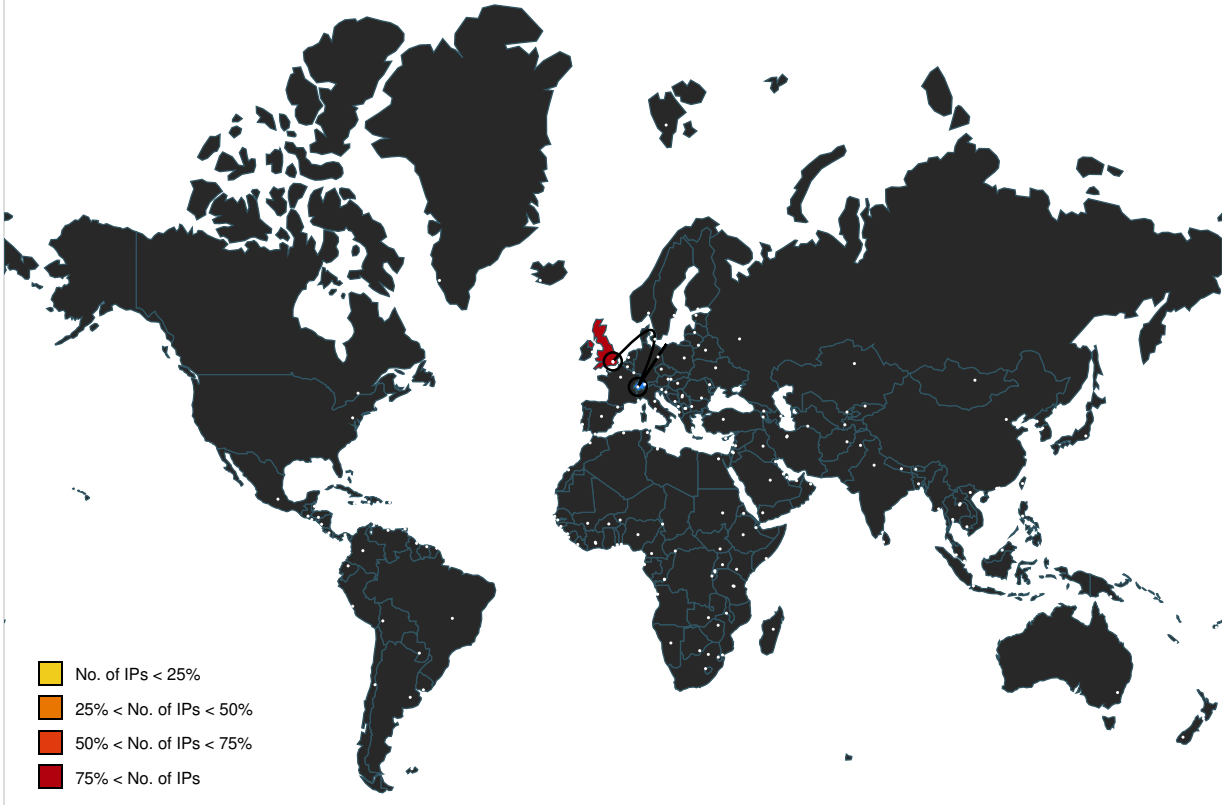
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	explorer.exe, 00000002.00000000.5697225107.00007FF883839000.00000002.00000001.01000000.00000007.sdmp	false	• URL Reputation: safe	unknown
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	explorer.exe, 00000002.00000000.5697225107.00007FF883839000.00000002.00000001.01000000.00000007.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.50.153.68	host-file-host6.com	United Kingdom		198526	GAZ-IS-ASRU	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877010
Start date and time:	2023-05-28 14:26:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	6
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
Sample file name:	86NKwZGvwn.exe
Original Sample Name:	40dcb3614c663e7ef659044a6514d446.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/2@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 89.1% (good quality ratio 81.3%) • Quality average: 69.6% • Quality standard deviation: 32.5%
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): audiodg.exe, WMIADAP.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:27:41	Task Scheduler	Run new task: Firefox Default Browser Agent 8C147AAD391B03BE path: C:\Users\user\AppData\Roaming\evcgwtu
14:27:41	API Interceptor	558x Sleep call for process: explorer.exe modified

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\evcgwtu

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	289792
Entropy (8bit):	6.556546845015486
Encrypted:	false
SSDEEP:	3072:5NifDzAVBXaRLmIuLQO4Rfl0NlusQ8+kdMEuj8hxdd5gWw9KDD5Qj:afDzA6Rceflq3Q/kWEu4GZYDDej
MD5:	40DCB3614C663E7EF659044A6514D446
SHA1:	4C25245DDBEA2D5FB5330CE333D313A4973E5B98
SHA-256:	069B749DC167BAE6560EA3F73A461184F0380F6AE3FFCFC095488063DA4F9554
SHA-512:	06520E1BB1C3F06428738BA5F10DD0445BC2FEDAA461E5D53F2A5727718F88B138DAFC08658D3598B317A06C97BD26B543B8685F52F948952384939A715ECFD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&.v.b...b...b...\|.....\|.....\|..H...EXc.k...b.....\|..c...\|..c...\|..c...Richb.... .....PE..L.....b.....~...&&.....IJ.....@.....(.....I~.....d.....&.....(..... .....P1..@..... .....text...R}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc..,3....(..4...8.....@..B..... ....

C:\Users\user\AppData\Roaming\evcgwtu: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):	6.556546845015486
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:	86NKwZGvwn.exe
File size:	289792
MD5:	40dcb3614c663e7ef659044a6514d446
SHA1:	4c25245ddbea2d5fb5330ce333d313a4973e5b98
SHA256:	069b749dc167bae6560ea3f73a461184f0380f6ae3ffcfc095488063da4f9554
SHA512:	06520e1bb1c3f06428738ba5f10dd0445bc2fedaa461e5d53f2a5727718f88b138dafc08658d3598b317a06c97bd26b543b8685f52f948952384939a715ecfd4
SSDEEP:	3072:5NifDzAVBXaRLmIuLQO4Rfl0NlusQ8+kdMEuj8hxdd5gWw9KDD5Qj:afDzA6Rceflq3Q/kWEu4GZYDDej
TLSH:	FB54185392E17D54E9764B729F2FC7F87A1EF2508E5977A912189E2F04B03B2C263702
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&.v.b...b...b...|.....|.....|...H...EXc.k...b.....|...c...|...c...|...c...Richb.....PE..L.....b.....~.

File Icon

Icon Hash:	455145455155691d

Static PE Info

General

Entrypoint:	0x404a49
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x62E7B3D1 [Mon Aug 1 11:06:57 2022 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:	937554e81340ac479b370382e43a74d4

Entrypoint Preview

Instruction
call 00007F5790DA6B23h
jmp 00007F5790DA21BDh
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F5790DA2366h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F5790DA2390h
test ecx, 00000003h
jne 00007F5790DA2331h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F5790DA232Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F5790DA2374h
test ah, ah
je 00007F5790DA2366h
test eax, 00FF0000h
je 00007F5790DA2355h
test eax, FF000000h
je 00007F5790DA2344h
jmp 00007F5790DA230Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi

Instruction
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [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	0x282a8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f000	0x197f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x289000	0xde4	.reloc
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	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d0	.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	0x27d52	0x27e00	False	0.7870910070532915	data	7.5850231403020265	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x29000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26f000	0x197f8	0x19800	False	0.3793370863970588	data	4.201292392897118	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x289000	0x332c	0x3400	False	0.22874098557692307	data	2.527933420000788	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x26f730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2705d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x270e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x273428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2744d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x274988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x275830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2760d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x276640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x278be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x279c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x27a618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x27aae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x27b990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27c238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x27c900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x27ce68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x27f410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2804b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x280988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x281830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2820d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x282640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x284be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x285c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x286618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x286d20	0x5c4	data		
RT_STRING	0x2872e8	0x710	data		
RT_STRING	0x2879f8	0x558	data		
RT_STRING	0x287f50	0x29c	data		
RT_STRING	0x2881f0	0x606	data		
RT_GROUP_ICON	0x286a80	0x68	data		
RT_GROUP_ICON	0x274938	0x4c	data		
RT_GROUP_ICON	0x280920	0x68	data		
RT_GROUP_ICON	0x27aa80	0x68	data		
RT_VERSION	0x286ae8	0x238	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleHandleW, VirtualFree, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, AttachConsole, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	EnumFontsW, GetCharABCWidthsFloatA, GetCharWidthW
ADVAPI32.dll	MapGenericMask

Network Behavior

Network Port Distribution

Total Packets: 10

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:27:41.523880005 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.549113035 CEST	80	49695	194.50.153.68	192.168.2.4
May 28, 2023 14:27:41.549222946 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.549535036 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.549597979 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.574449062 CEST	80	49695	194.50.153.68	192.168.2.4
May 28, 2023 14:27:41.672564983 CEST	80	49695	194.50.153.68	192.168.2.4
May 28, 2023 14:27:41.672703028 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.673958063 CEST	49695	80	192.168.2.4	194.50.153.68
May 28, 2023 14:27:41.698729992 CEST	80	49695	194.50.153.68	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:27:41.495443106 CEST	52239	53	192.168.2.4	8.8.8.8
May 28, 2023 14:27:41.516335011 CEST	53	52239	8.8.8.8	192.168.2.4
May 28, 2023 14:27:41.683769941 CEST	56807	53	192.168.2.4	8.8.8.8
May 28, 2023 14:27:42.720056057 CEST	56807	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 14:27:43.720438957 CEST	56807	53	192.168.2.4	8.8.8.8
May 28, 2023 14:27:45.723534107 CEST	53	56807	8.8.8.8	192.168.2.4
May 28, 2023 14:27:46.765328884 CEST	53	56807	8.8.8.8	192.168.2.4
May 28, 2023 14:27:47.753593922 CEST	53	56807	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 28, 2023 14:27:46.765438080 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
May 28, 2023 14:27:47.753828049 CEST	192.168.2.4	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 14:27:41.495443106 CEST	192.168.2.4	8.8.8.8	0x71e2	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:41.683769941 CEST	192.168.2.4	8.8.8.8	0x2ad8	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:42.720056057 CEST	192.168.2.4	8.8.8.8	0x2ad8	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:43.720438957 CEST	192.168.2.4	8.8.8.8	0x2ad8	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)	false

DNS Answers

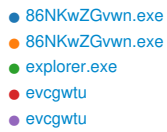
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 14:27:41.516335011 CEST	8.8.8.8	192.168.2.4	0x71e2	No error (0)	host-file-host6.com		194.50.153.68	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:45.723534107 CEST	8.8.8.8	192.168.2.4	0x2ad8	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:46.765328884 CEST	8.8.8.8	192.168.2.4	0x2ad8	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false
May 28, 2023 14:27:47.753593922 CEST	8.8.8.8	192.168.2.4	0x2ad8	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- tclyyrvk.com
  - host-file-host6.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 86NKwZGvwn.exe PID: **5764**, Parent PID: **3528**

General	
Target ID:	0
Start time:	14:26:59
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\86NKwZGvwn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\86NKwZGvwn.exe
Imagebase:	0x400000
File size:	289792 bytes
MD5 hash:	40DCB3614C663E7EF659044A6514D446
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: 00000000.00000002.528146469.0000000000808000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: 86NKwZGvwn.exe PID: **5732**, Parent PID: **5764**

General	
Target ID:	1
Start time:	14:26:59
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\86NKwZGvwn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\86NKwZGvwn.exe
Imagebase:	0x400000
File size:	289792 bytes
MD5 hash:	40DCB3614C663E7EF659044A6514D446
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: 00000001.00000002.570702599.00000000006A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.570702599.00000000006A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.570658568.0000000000530000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000002.570658568.0000000000530000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3528**, Parent PID: **5732**

General

Target ID:	2
Start time:	14:27:04
Start date:	28/05/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\evcgwtu	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	2A41F42	CopyFileW
C:\Users\user\AppData\Roaming\evcgwtu\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2A41F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\86NKwZGvwn.exe	success or wait	1	2A41F53	DeleteFileW
C:\Users\user\AppData\Roaming\evcgwtu:Zone.Identifier	success or wait	1	2A41F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\evcgwtu	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd 76 fd 62 fd 18 fd 62 fd 18 fd 62 fd 18 fd 7c 0d fd 7f fd 18 fd 7c 1b fd 18 fd 18 fd 7c 1c fd 48 fd 18 fd 45 58 63 fd 6b fd 18 fd 62 fd 19 fd fd 18 fd 7c 12 fd 63 fd 18 fd 7c 0c fd 63 fd 18 fd 7c 09 fd 63 fd 18 fd 52 69 63 68 62 fd 18 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 73 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 7e 02	MZ@!L!This program cannot be run in DOS mode.$&vbbb|||HEXckb |c|c|cRichbPELb~	success or wait	3	2A41F42	CopyFileW
C:\Users\user\AppData\Roaming\evcgwtu: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	2A41F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: evcgwtu

PID: **6696**, Parent PID: **1088**

General

Target ID:	5
Start time:	14:27:41
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\evcgwtu
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\evcgwtu
Imagebase:	0x400000
File size:	289792 bytes
MD5 hash:	40DCB3614C663E7EF659044A6514D446
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: 00000005.00000002.618725202.00000000008D8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

Analysis Process: evcgwtu

PID: **6688**, Parent PID: **6696**

General	
Target ID:	6
Start time:	14:27:41
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\evcgwtu
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\evcgwtu
Imagebase:	0x400000
File size:	289792 bytes
MD5 hash:	40DCB3614C663E7EF659044A6514D446
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: 00000006.00000002.629532527.0000000001F30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.629532527.0000000001F30000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000002.629561581.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000006.00000002.629561581.0000000001F51000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly