ID: 678224
Sample Name: 4cqJ4Jjd5j.exe
Cookbook: default.jbs
Time: 17:50:29
Date: 03/08/2022
Version: 35.0.0 Citrine

Table of Contents

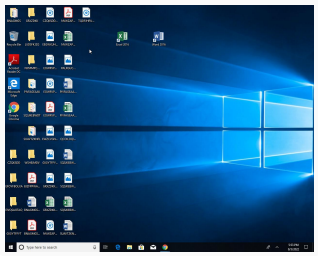
Windows Analysis Report

4cqJ4Jjd5j.exe

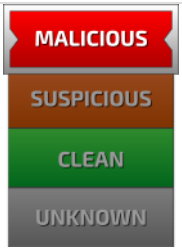
Overview

General Information

Sample Name:	4cqJ4Jjd5j.exe
Analysis ID:	678224
MD5:	c529659ad79b58..
SHA1:	aad399bd653192.
SHA256:	269200ba6acb85..
Tags:	ArkeiStealer exe
Infos:	



Detection



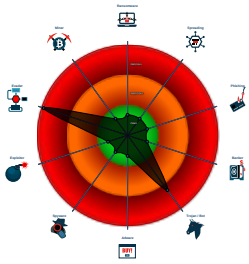
SmokeLoader

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…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Checks for kernel code integrity (NtQ…

Classification



Process Tree

- **System is w10x64**
- 4cqJ4Jjd5j.exe (PID: 1276 cmdline: "C:\Users\user\Desktop\4cqJ4Jjd5j.exe" MD5: C529659AD79B58EB83D1732B6CC88FF5)
  - 4cqJ4Jjd5j.exe (PID: 5848 cmdline: "C:\Users\user\Desktop\4cqJ4Jjd5j.exe" MD5: C529659AD79B58EB83D1732B6CC88FF5)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- brgfgda (PID: 5392 cmdline: C:\Users\user\AppData\Roaming\brgfgda MD5: C529659AD79B58EB83D1732B6CC88FF5)
  - brgfgda (PID: 4916 cmdline: C:\Users\user\AppData\Roaming\brgfgda MD5: C529659AD79B58EB83D1732B6CC88FF5)
- **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
00000012.00000002.416720371.00000000006C1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.350531051.0000000000540000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.416678230.0000000000680000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.350835390.0000000002431000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000005.00000000.331229772.0000000002941000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.brgfgda.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
18.0.brgfgda.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.4cqJ4Jjd5j.exe.25015a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
16.2.brgfgda.25d15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
18.0.brgfgda.400000.6.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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

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

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

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

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

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected SmokeLoader

Remote Access Functionality

Yara detected SmokeLoader

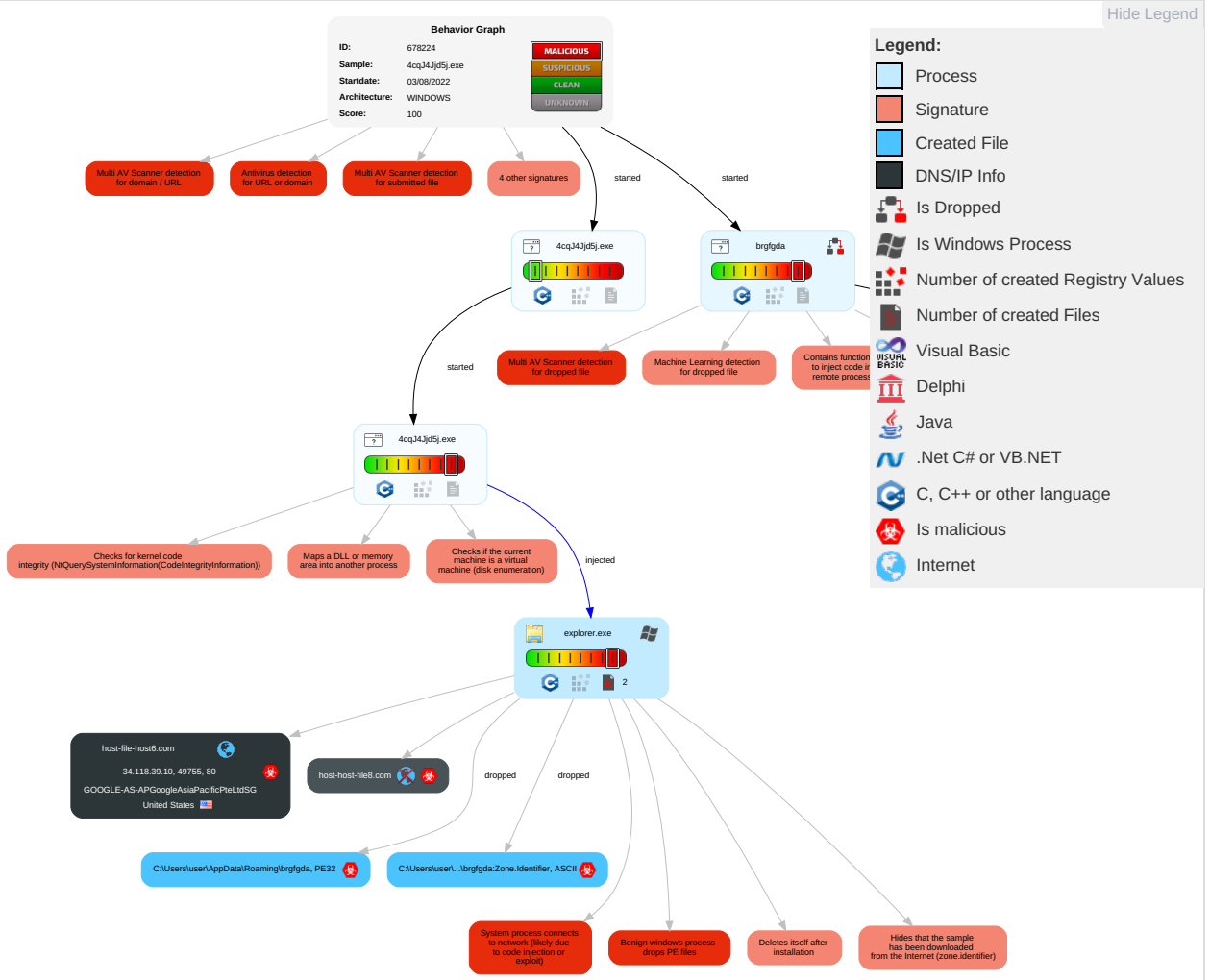
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	5 1 2 Process Injection	1 1 Masqueradi ng	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 Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	1 DLL Side-Loading	1 2 Virtualizatio n/Sandbox Evasion	LSASS Memory	4 1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 2 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 2 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra phy	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 Impersonati on	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 Communic ation		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.commo n	Rc.commo n	3 Software Packing	Cached Domain Credentials	4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic ation	Jamming or Denial of Service		Abuse Accessibilit y Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

Hide Legend



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
4cqJ4Jjd5j.exe	39%	Virustotal		Browse
4cqJ4Jjd5j.exe	44%	ReversingLabs	Win32.Trojan.Vigorf	
4cqJ4Jjd5j.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\brgfgda	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\brgfgda	39%	Virustotal		Browse
C:\Users\user\AppData\Roaming\brgfgda	44%	ReversingLabs	Win32.Trojan.Vigorf	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.0.brgfgda.400000.2.unpack	100%	Avira	TR/Patched.Gen		Download File
18.0.brgfgda.400000.1.unpack	100%	Avira	TR/Patched.Gen		Download File
18.0.brgfgda.400000.3.unpack	100%	Avira	TR/Patched.Gen		Download File
18.0.brgfgda.400000.0.unpack	100%	Avira	TR/Patched.Gen		Download File
18.0.brgfgda.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.4cqJ4Jjd5j.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
18.2.brgfgda.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.4cqJ4Jjd5j.exe.25015a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.4cqJ4Jjd5j.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.brgfgda.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.4cqJ4Jjd5j.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.4cqJ4Jjd5j.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.brgfgda.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.brgfgda.25d15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.brgfgda.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
1.0.4cqJ4Jjd5j.exe.400000.4.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

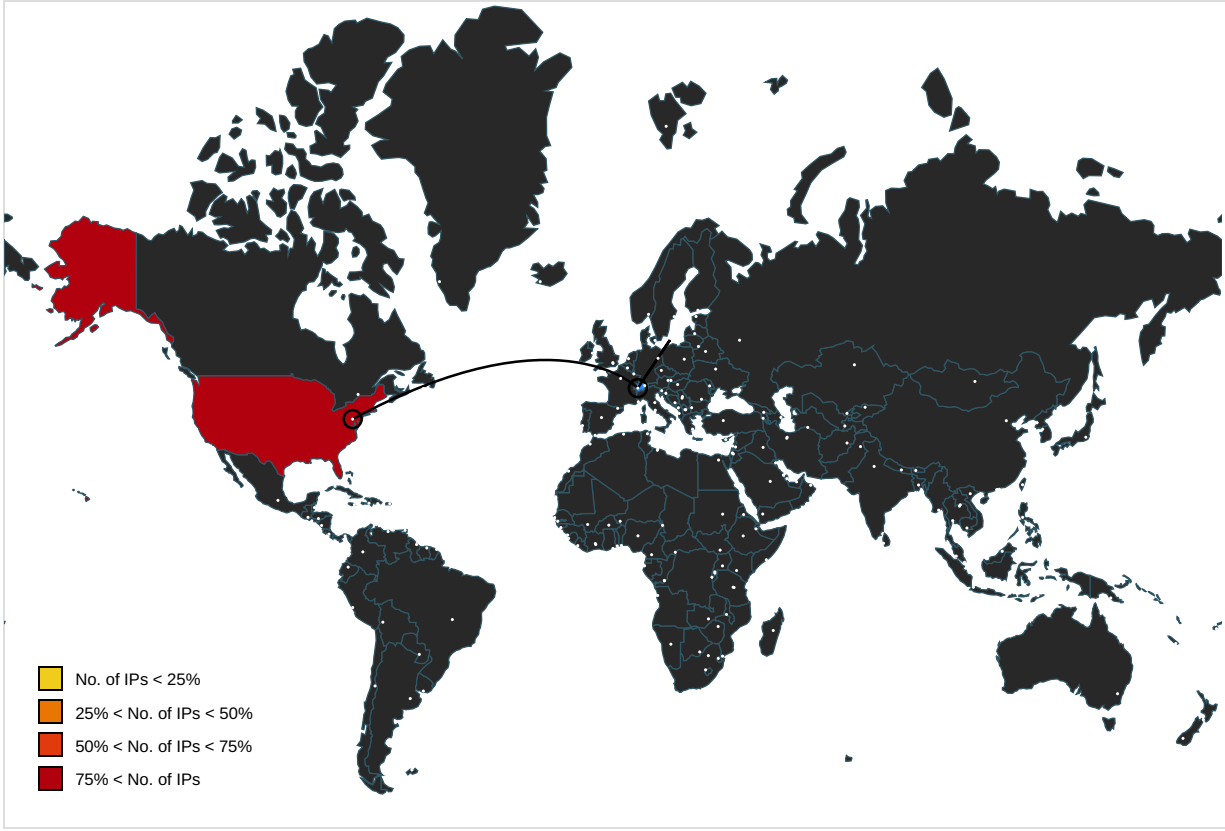
Contacted Domains

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:	678224
Start date and time: 03/08/202217:50:29	2022-08-03 17:50:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4cqJ4Jjd5j.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:	26
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: 27.2%

HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14, 52.242.101.226, 20.223.24.244, 20.54.89.106, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target 4cqJ4Jjd5j.exe, PID 1276 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
17:52:36	Task Scheduler	Run new task: Firefox Default Browser Agent 173C074F5A931F0F path: C:\Users\user\AppData\Roaming\brgfgda

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\brgfgda

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	7.056602649646931
Encrypted:	false

SSDEEP:	3072:C196SvSbCDBMY3ue3PFUt76X9JflruFeKQvd4xkESjMWD/Y:CVcmhfW6X9OihQvDF
MD5:	C529659AD79B58EB83D1732B6CC88FF5
SHA1:	AAD399BD653192EC0ECDEAC5C1A4CBF43AFB19B6
SHA-256:	269200BA6ACB859B712185EBDAD2B0000333E42D194E05D12D86EB3590125AED
SHA-512:	6E81A8A8803746E0C10B8A18EC7A1061EFC8BD6EABBBBAB4E02B0A01B21C360B1A73FB93B0A8D40961F309AE915F214A03F0E6A49024E6A000DE24FB906CA3D6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 39%, Browse • Antivirus: ReversingLabs, Detection: 44%
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....".....B.....gg.....@....@.....8.....l0..<.....Pv..... .....6..@.... .....text...@+.....,..... ..`.data....:...@...0...0.....@....rsrc...Pv.....x...`.....@..@..... ....

C:\Users\user\AppData\Roaming\brgfgda: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):	7.056602649646931
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:	4cqJ4Jjd5j.exe
File size:	186368
MD5:	c529659ad79b58eb83d1732b6cc88ff5
SHA1:	aad399bd653192ec0ecdeac5c1a4cbf43afb19b6
SHA256:	269200ba6acb859b712185ebdad2b0000333e42d194e05d12d86eb3590125aed
SHA512:	6e81a8a8803746e0c10b8a18ec7a1061efc8bd6eabbbbab4e02b0a01b21c360b1a73fb93b0a8d40961f309ae915f214a03f0e6a49024e6a000de24fb906ca3d6
SSDEEP:	3072:C196SvSbCDBMY3ue3PFUt76X9JflruFeKQvd4xkESjMWD/Y:CVcmhfW6X9OihQvDF
TLSH:	4A04AD2133E1C072D4B729309B75DAE15B3AB922E7B45B8B7760072A1F712C1BA38757
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.....".`.....

File Icon

Icon Hash:	8a9199c9ca8cd2f2

Static PE Info

General

Entrypoint:	0x416767
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x602286F3 [Tue Feb 9 12:58:27 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:	19d26450af6fae284e6a28f691d90382

Entrypoint Preview

Instruction
call 00007F36C4BD02B9h
jmp 00007F36C4BC9C7Eh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
call 00007F36C4BC9E2Ch
xchg cl, ch
jmp 00007F36C4BC9E14h
call 00007F36C4BC9E23h
fxch st(0), st(1)
jmp 00007F36C4BC9E0Bh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007F36C4BC9E01h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007F36C4BC9DF6h
fldpi

Instruction
fsubrp st(1), st(0)
or ch, ch
je 00007F36C4BC9DF4h
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 00007F36C4BC9DF7h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007F36C4BD047Fh
fstp st(0)
fld tbyte ptr [004024CAh]
ret
fstp st(0)
or cl, cl
je 00007F36C4BC9DFDh
fstp st(0)
fldpi
or ch, ch
je 00007F36C4BC9DF4h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007F36C4BC9DE9h
fchs
ret
fstp st(0)
jmp 00007F36C4BD0455h
fstp st(0)
mov cl, ch
jmp 00007F36C4BC9DF2h
call 00007F36C4BC9DBEh
jmp 00007F36C4BD0460h
int3
int3
int3
int3
int3
int3

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2306c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20a8000	0x7650	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3680	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x22b40	0x22c00	False	0.7597726506294964	data	7.423882781109827	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x24000	0x2083ad0	0x3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x20a8000	0x7650	0x7800	False	0.6784505208333333	data	6.280404502514193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

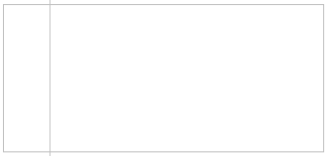
Name	RVA	Size	Type	Language	Country
RT_ICON	0x20a8300	0xea8	data	Kannada	Kanada
RT_ICON	0x20a91a8	0x8a8	data	Kannada	Kanada
RT_ICON	0x20a9a50	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20a9fb8	0x25a8	data	Kannada	Kanada
RT_ICON	0x20ac560	0x10a8	data	Kannada	Kanada
RT_ICON	0x20ad608	0x988	data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

Imports

DLL	Import

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

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 11

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 17:52:36.203840017 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:52:36.240654945 CEST	80	49755	34.118.39.10	192.168.2.3
Aug 3, 2022 17:52:36.242068052 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:52:36.242321968 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:52:36.243194103 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:52:36.279036045 CEST	80	49755	34.118.39.10	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 17:52:36.279752016 CEST	80	49755	34.118.39.10	192.168.2.3
Aug 3, 2022 17:52:36.375181913 CEST	80	49755	34.118.39.10	192.168.2.3
Aug 3, 2022 17:52:36.429420948 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:53:06.376564026 CEST	80	49755	34.118.39.10	192.168.2.3
Aug 3, 2022 17:53:06.376753092 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:53:06.418031931 CEST	49755	80	192.168.2.3	34.118.39.10
Aug 3, 2022 17:53:06.454641104 CEST	80	49755	34.118.39.10	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 3, 2022 17:52:35.903945923 CEST	58116	53	192.168.2.3	8.8.8.8
Aug 3, 2022 17:52:36.197936058 CEST	53	58116	8.8.8.8	192.168.2.3
Aug 3, 2022 17:52:36.391638994 CEST	57421	53	192.168.2.3	8.8.8.8
Aug 3, 2022 17:52:37.441411972 CEST	57421	53	192.168.2.3	8.8.8.8
Aug 3, 2022 17:52:38.492662907 CEST	57421	53	192.168.2.3	8.8.8.8
Aug 3, 2022 17:52:40.417336941 CEST	53	57421	8.8.8.8	192.168.2.3
Aug 3, 2022 17:52:41.465724945 CEST	53	57421	8.8.8.8	192.168.2.3
Aug 3, 2022 17:52:42.518218040 CEST	53	57421	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 3, 2022 17:52:41.465881109 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Aug 3, 2022 17:52:42.518362045 CEST	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
Aug 3, 2022 17:52:35.903945923 CEST	192.168.2.3	8.8.8.8	0xe7f1	Standard query (0)	host-file-host6.com	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:36.391638994 CEST	192.168.2.3	8.8.8.8	0xad13	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:37.441411972 CEST	192.168.2.3	8.8.8.8	0xad13	Standard query (0)	host-host-file8.com	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:38.492662907 CEST	192.168.2.3	8.8.8.8	0xad13	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 17:52:36.197936058 CEST	8.8.8.8	192.168.2.3	0xe7f1	No error (0)	host-file-host6.com		34.118.39.10	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:40.417336941 CEST	8.8.8.8	192.168.2.3	0xad13	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:41.465724945 CEST	8.8.8.8	192.168.2.3	0xad13	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2022 17:52:42.518218040 CEST	8.8.8.8	192.168.2.3	0xad13	Server failure (2)	host-host-file8.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- armtrksuct.net
  - host-file-host6.com

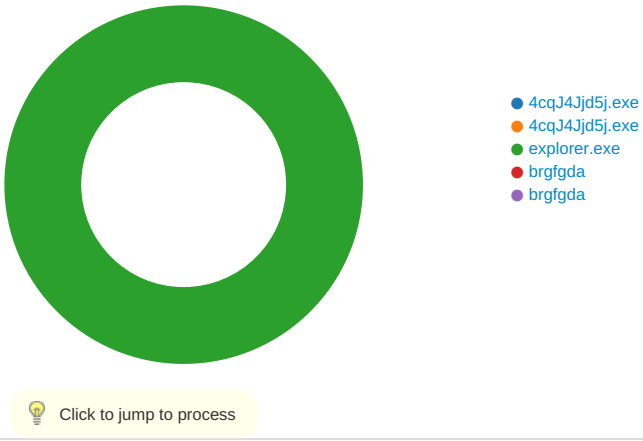
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49755	34.118.39.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2022 17:52:36.242321968 CEST	1197	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://armtrksuct.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 343 Host: host-file-host6.com
Aug 3, 2022 17:52:36.375181913 CEST	1198	IN	HTTP/1.1 200 OK server: nginx/1.20.1 date: Wed, 03 Aug 2022 15:52:36 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: 4cqJ4Jjd5j.exe PID: 1276, Parent PID: 5352

General

Target ID:	0
Start time:	17:51:31
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\4cqJ4Jjd5j.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4cqJ4Jjd5j.exe"
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C529659AD79B58EB83D1732B6CC88FF5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 4cqJ4Jjd5j.exe PID: **5848**, Parent PID: **1276**

General

Target ID:	1
Start time:	17:51:34
Start date:	03/08/2022
Path:	C:\Users\user\Desktop\4cqJ4Jjd5j.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4cqJ4Jjd5j.exe"
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C529659AD79B58EB83D1732B6CC88FF5
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: 00000001.00000002.350531051.0000000000540000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.350835390.0000000002431000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5848**

General

Target ID:	5
Start time:	17:51:43
Start date:	03/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
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: 00000005.00000000.331229772.0000000002941000.00000020.80000000.00040000.00000000.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\brgfgda	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	2941F42	CopyFileW
C:\Users\user\AppData\Roaming\brgfgda\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2941F42	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4cqJ4Jjd5j.exe	success or wait	1	2941F53	DeleteFileW
C:\Users\user\AppData\Roaming\brgfgda:Zone.Identifier	success or wait	1	2941F9E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\brgfgda	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 0f fd 6d fd 4b fd 03 fd 4b fd 03 fd 4b fd 03 fd 24 fd fd fd 5c fd 03 fd 24 fd fd fd 38 fd 03 fd 42 fd fd fd 4e fd 03 fd 4b fd 02 fd fd fd 03 fd 24 fd fd fd 6d fd 03 fd 24 fd fd fd 4a fd 03 fd 24 fd fd fd 4a fd 03 fd 52 69 63 68 4b fd 03 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 22 60 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$mKKK$\$8BNK$ mJJRichKPEL"`	success or wait	2	2941F42	CopyFileW
C:\Users\user\AppData\Roaming\brgfgda: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	2941F42	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: brgfgda PID: **5392**, Parent PID: **848**

General

Target ID:	16
Start time:	17:52:36
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\brgfgda
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\brgfgda
Imagebase:	0x400000
File size:	186368 bytes
MD5 hash:	C529659AD79B58EB83D1732B6CC88FF5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, Virustotal, Browse • Detection: 44%, ReversingLabs
Reputation:	low

Analysis Process: brgfgda PID: **4916**, Parent PID: **5392**

General

Target ID:	18
Start time:	17:52:40
Start date:	03/08/2022
Path:	C:\Users\user\AppData\Roaming\brgfgda
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\brgfgda
Imagebase:	0x400000

File size:	186368 bytes
MD5 hash:	C529659AD79B58EB83D1732B6CC88FF5
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: 00000012.00000002.416720371.00000000006C1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000012.00000002.416678230.0000000000680000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly