ID: 384290
Sample Name: Transferencia
Cookbook: default.jbs
Time: 21:11:21
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

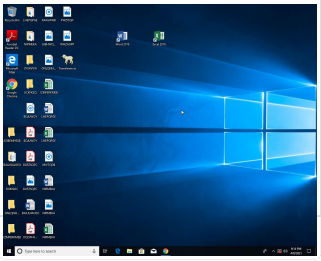
Analysis Report Transferencia

Overview

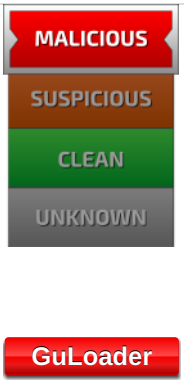
General Information

Sample Name:	Transferencia (renamed file extension from none to exe)
Analysis ID:	384290
MD5:	7c22c3e3b8726d..
SHA1:	7715be6b73e525..
SHA256:	96fb89fdc387386..
Infos:	

Most interesting Screenshot:



Detection

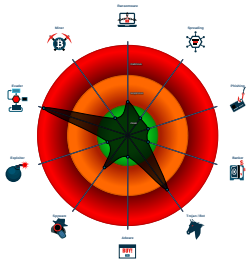


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contain functionality to detect virtua…
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- Transferencia.exe (PID: 6804 cmdline: 'C:\Users\user\Desktop\Transferencia.exe' MD5: 7C22C3E3B8726DD1B03E69C203590026)
  - RegAsm.exe (PID: 7052 cmdline: 'C:\Users\user\Desktop\Transferencia.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 7080 cmdline: 'C:\Users\user\Desktop\Transferencia.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 7096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

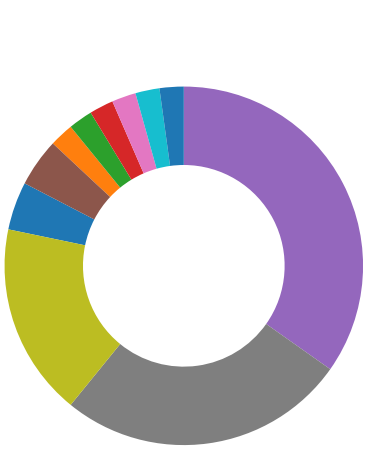
Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.902860214.0000000001370000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 7080	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contain functionality to detect virtual machines

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Found potential dummy code loops (likely to delay analysis)

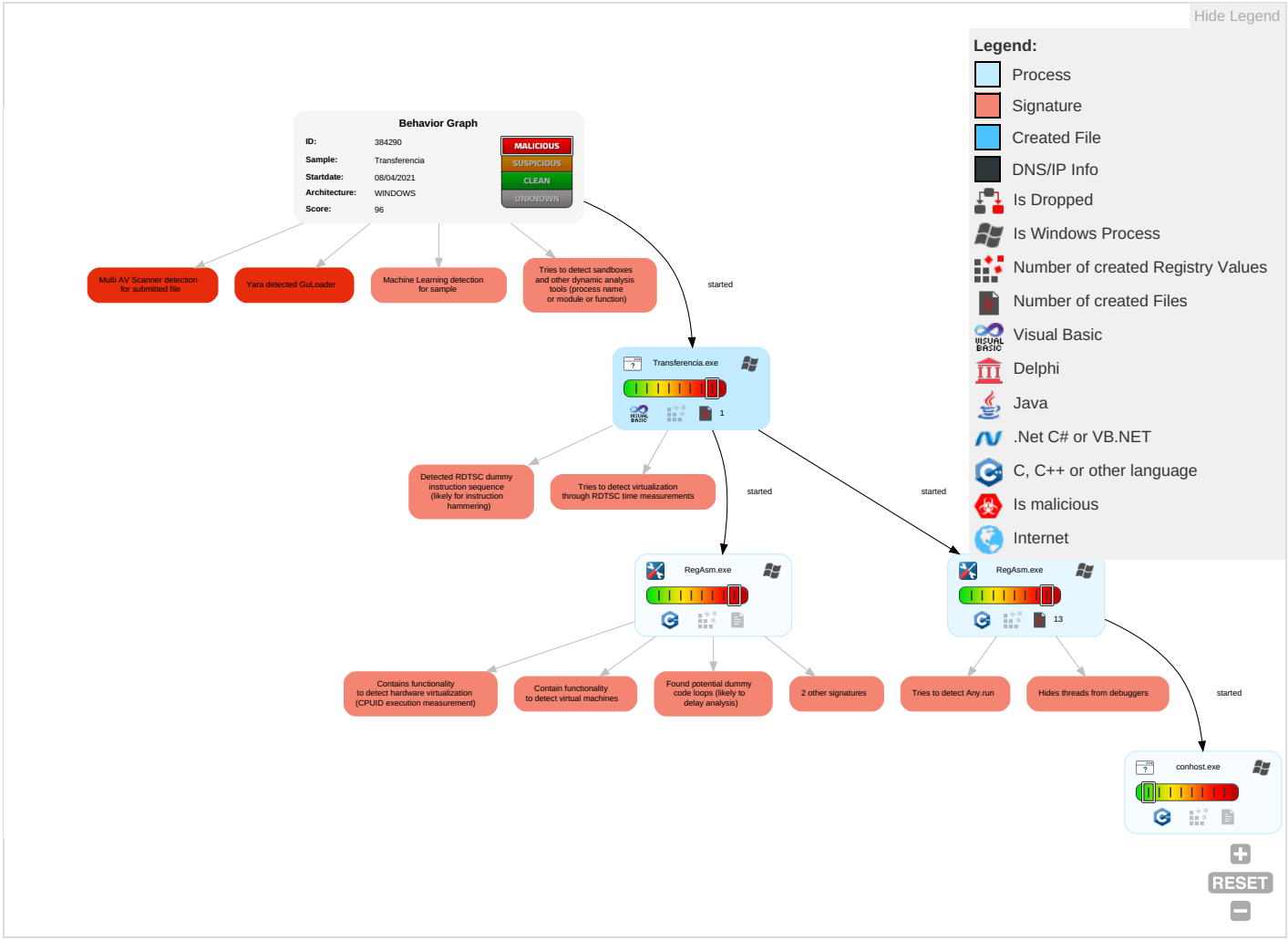
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 2	Virtualization/Sandbox Evasion 4 2 1	OS Credential Dumping	Security Software Discovery 9 2 1	Remote Services	Clipboard Data 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 4 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
Transferencia.exe	29%	Virustotal		Browse
Transferencia.exe	69%	ReversingLabs	Win32.Backdoor.Convagent	
Transferencia.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384290
Start date:	08.04.2021
Start time:	21:11:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Transferencia (renamed file extension from none to 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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winEXE@4/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.6% (good quality ratio 66.2%) • Quality average: 39.4% • Quality standard deviation: 38.2%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.42.151.234, 13.64.90.137, 13.88.21.125, 20.82.210.154, 23.10.249.26, 23.10.249.43, 40.88.32.150, 104.43.193.48, 168.61.161.212, 23.0.174.185, 23.0.174.200, 20.82.209.183, 172.217.168.14, 20.54.26.129, 23.54.113.53 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:13:39	API Interceptor	103x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.7314228952467845
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	Transferencia.exe
File size:	122880
MD5:	7c22c3e3b8726dd1b03e69c203590026
SHA1:	7715be6b73e52535d81b083a3dfd95568a729782
SHA256:	96fb89fdc3873864981ec26c355111c26c7ab5132770ead9d1d97bdfac32e566
SHA512:	bea857c957f771e3b7c24a3e9770da90766f3c8bf2af74fa79a7b2e9a372b55a1fe628dd72f0744ac1e99d63527e7292dfc47bc2e9b09e2c84030e25f519625
SSDEEP:	1536:yGouBnMJDe1Rd/tnt+5vAQlhI2k1c8VtK9ihGo:yGZBn5j+3I2gtVtK9ihG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L....{.O.....p...`.....(.....@.....

File Icon

Icon Hash:	0ccea09899191898

Static PE Info

General

Entrypoint:	0x401328
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4F8F7B90 [Thu Apr 19 02:42:24 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

General

Import Hash:	efa774b90ad6b9ab8c4fabb031ebe78d

Entrypoint Preview

Instruction
push 00413E10h
call 00007F48ACE91015h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
jl 00007F48ACE91014h
fisub dword ptr [edi]
mov bh, 3Fh
sti
inc eax
or dword ptr [edi-6Fh], 17349181h
push esi
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+53018250h], al
push 7372656Fh
aaa
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
sub bl, dl
aam 67h
dec esi
add dword ptr [ebp-6Ah], DE15A246h
inc dword ptr [edx]
sal byte ptr [ebx-5D2637B1h], 00000045h
push ecx
jc 00007F48ACE90FFAh
dec ebp
sahf
pop ds
in al, dx
dec ebx
inc esi
push esp
mov word ptr [edi+33AD4F3Ah], seg?
cdq
iretw
adc dword ptr [edi+00AA000Ch], esi
pushad
rcl dword ptr [ebx+00000000h], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov ebp, D8000129h
inc esp
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [ecx+eax*2+53h], cl
push esp
inc ebp
push eax
inc ecx
dec esp
dec esp
add byte ptr [62000701h], cl
insb
jo 00007F48ACE9108Bh
popad
jc 00007F48ACE91022h
sbb dword ptr [ecx], eax
add byte ptr [edx+00h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17614	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x4856	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xd4	.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	0x16a04	0x17000	False	0.347465183424	data	6.19151280258	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0xa88	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x4856	0x5000	False	0.4142578125	data	4.36602718987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1b2ae	0x25a8	data		
RT_ICON	0x1a206	0x10a8	data		
RT_ICON	0x1987e	0x988	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x19416	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x193d8	0x3e	data		
RT_VERSION	0x19180	0x258	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	YCIETRA
FileVersion	3.00
CompanyName	Salty
Comments	Salty
ProductName	Salty
ProductVersion	3.00
FileDescription	Salty
OriginalFilename	YCIETRA.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 21:11:55.768042088 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:11:55.780359983 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 21:11:55.883462906 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:11:55.898070097 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 21:11:58.097877979 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:11:58.110531092 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 21:11:59.033427000 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:11:59.048686028 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 21:11:59.959151983 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:11:59.971601009 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:01.150670052 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:01.163203001 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:02.185863972 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:02.198513985 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:03.113531113 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:03.126367092 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:04.205010891 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:04.218501091 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:05.546283960 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:05.560033083 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:09.546550989 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:09.559048891 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:10.521244049 CEST	53700	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 21:12:10.534894943 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:24.931571960 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:24.944093943 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:27.205535889 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:27.225574970 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:42.319421053 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:42.332051992 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:42.969063044 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:42.981756926 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:43.728193045 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:43.741270065 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:44.649430990 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:44.663150072 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:46.299026012 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:46.312469959 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:46.953691006 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:46.966485023 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:50.850680113 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:50.865803003 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:50.899362087 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:50.917721987 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:51.834000111 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:51.847381115 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 21:12:59.857206106 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:12:59.871678114 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 21:13:03.895875931 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:13:03.914320946 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 21:13:34.054303885 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:13:34.067322016 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 21:13:39.253865957 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:13:39.280627966 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 21:13:42.108520985 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:13:42.135521889 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 21:13:43.186271906 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 21:13:43.204425097 CEST	53	60875	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Transferencia.exe PID: 6804 Parent PID: 1280

General

Start time:	21:12:03
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Transferencia.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Transferencia.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	7C22C3E3B8726DD1B03E69C203590026
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 7052 Parent PID: 6804

General

Start time:	21:13:30
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Transferencia.exe'
Imagebase:	0x400000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 7080 Parent PID: 6804

General

Start time:	21:13:30
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Transferencia.exe'
Imagebase:	0xfa0000

File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000B.00000002.902860214.0000000001370000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13748B6	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7096 Parent PID: 7080

General

Start time:	21:13:31
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis