ID: 395283
Sample Name: transferencia
Cookbook: default.jbs
Time: 11:36:59
Date: 22/04/2021
Version: 31.0.0 Emerald

Table of Contents

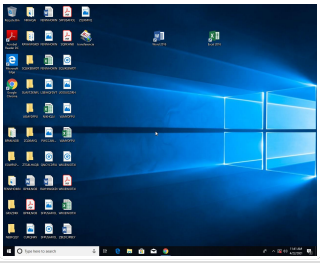
Analysis Report transferencia

Overview

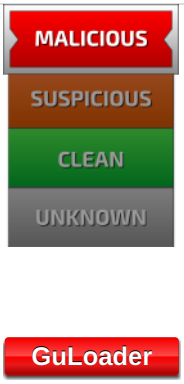
General Information

Sample Name:	transferencia (renamed file extension from none to exe)
Analysis ID:	395283
MD5:	718116c2cc15e5..
SHA1:	d14a54807e58e6..
SHA256:	573a35a2e7644c..
Infos:	

Most interesting Screenshot:



Detection

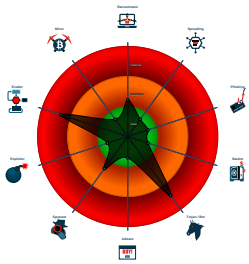


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …
- Contains functionality to read the PEB

Classification



Startup

- **System is w10x64**
- transferencia.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\transferencia.exe' MD5: 718116C2CC15E564DB71B3BDA3F966E5)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1UJvRluFmYD39H3TjOMIaVwZTdLhauoPu",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```

Yara Overview

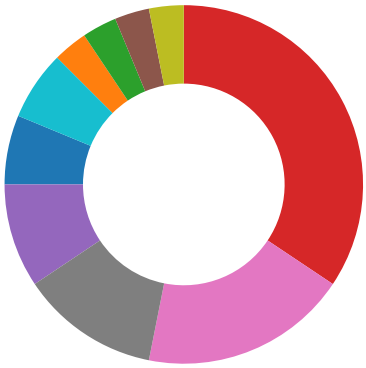
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.852343064.000000000230 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: transferencia.exe PID: 6424	JoeSecurity_VB6Downloader Generic	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: transferencia.exe PID: 6424	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

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:

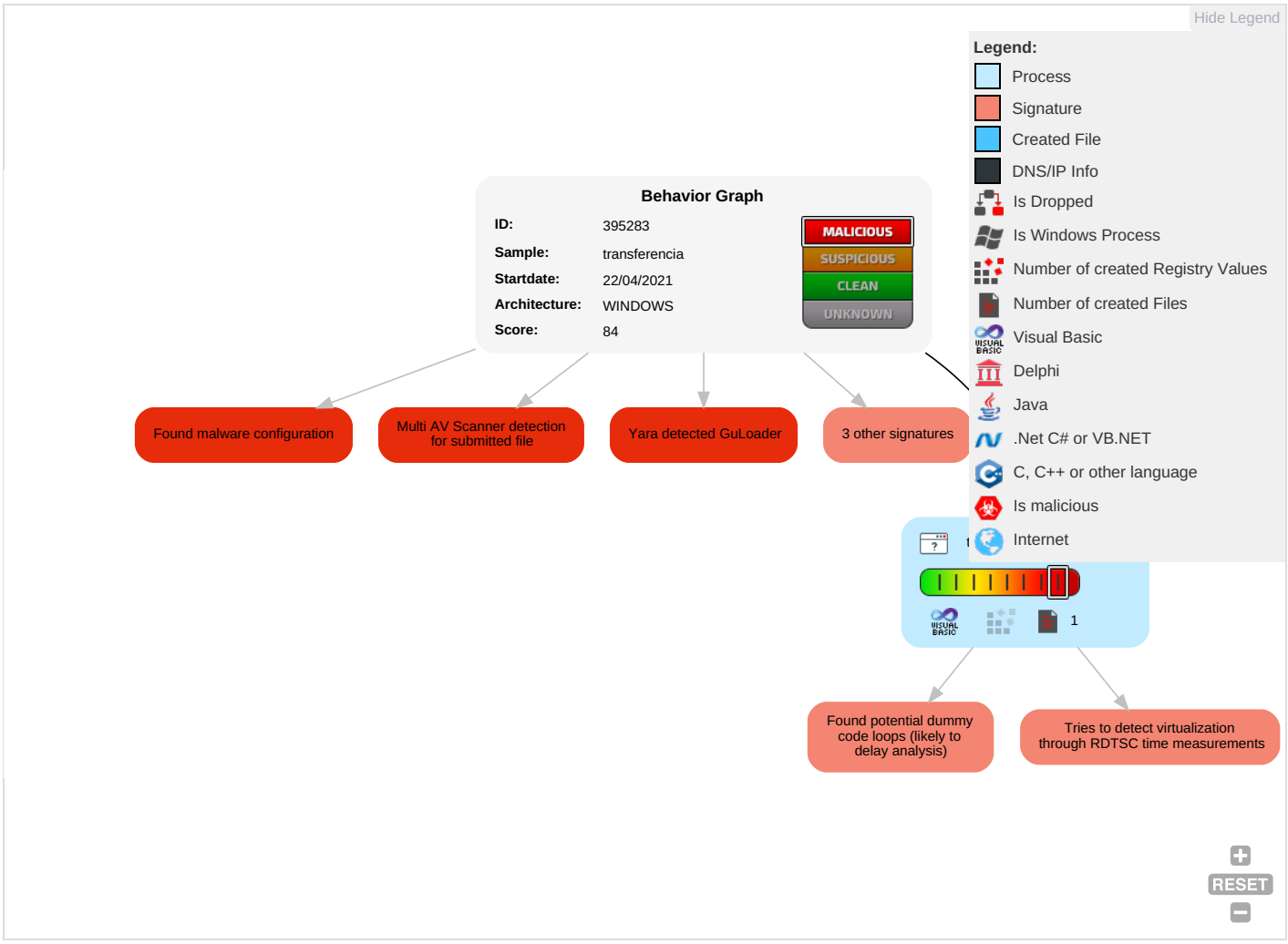
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

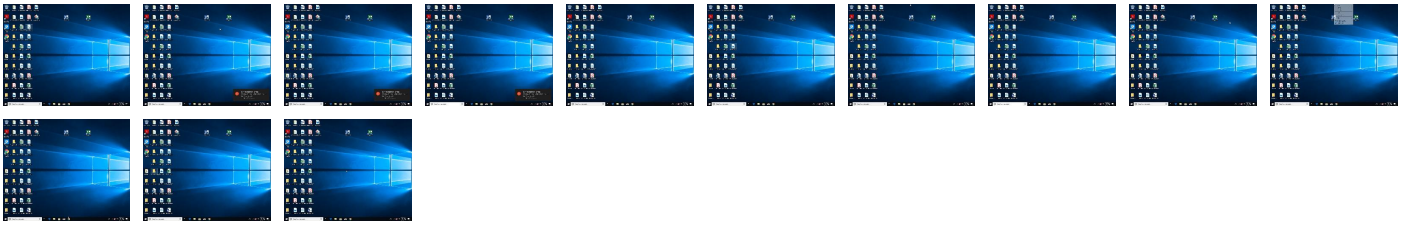
Behavior Graph



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	46%	Virustotal		Browse
transferencia.exe	34%	ReversingLabs	Win32.Trojan.Vebzenpak	

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:	395283
Start date:	22.04.2021
Start time:	11:36:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.9% (good quality ratio 12.1%) • Quality average: 27.7% • Quality standard deviation: 36.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe

Simulations

Behavior and APIs

No simulations

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):	5.800047430460185
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:	86016
MD5:	718116c2cc15e564db71b3bda3f966e5
SHA1:	d14a54807e58e625dc18c6210c08bc553e474d41
SHA256:	573a35a2e7644c067c6ce60c344fbe291be24d85e6cecbee256a37e1219f7a83
SHA512:	84afb3f7d8e1ae4e8431fc755dfc1e434988f2fbfa8b2805715fa5467b9d8e7fae17f40fcd3e82d25bfe6bae8baa28676d3663926ca88536993c3da7b22541ee
SSDEEP:	1536:an2G5PW5XCqdsfBj5Sin0y/AODB80Hn2G5P:j5XCqK9r/AOx

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...e..K.....0..... ....@.....

File Icon

Icon Hash:	b370e4d6f0c44880

Static PE Info

General

Entrypoint:	0x4013ec
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:	0x4BC9A565 [Sat Apr 17 12:11:17 2010 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
Import Hash:	5d12f87c2526f1462e3e55521a60ec88

Entrypoint Preview

Instruction
push 0040C7A0h
call 00007FED9CA44425h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebx], dl
out BAh, eax
inc edx
hlt
mov bh, 97h
inc esp
mov ah, F2h
mov dh, 3Bh
pop edi
inc edi
dec edx
test dword ptr [eax], 00000000h
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebp+6Dh], al

Instruction
bound ebp, dword ptr [ecx+74h]
je 00007FED9CA44497h
jc 00007FED9CA4449Bh
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 bh, bh
int3
xor dword ptr [eax], eax
and al, E5h
push edi
out dx, al
mov cl, dh
pop ebx
daa
inc esi
xchg dh, ch
cmpsd
pop eax
jns 00007FED9CA4445Eh
mov ch, 06h
cmp ah, byte ptr [ebx]
cmp ch, bl
test cl, ah
outsb
dec esi
mov byte ptr [FC9C23C8h], al
xor al, 3Ah
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
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
add byte ptr [eax], al
pop eax
mov dl, 00h
add byte ptr [edx], cl
or eax, 09000000h
add byte ptr [ecx+78h], dl
imul ebp, dword ptr [ebx+72h], 00656C73h
or eax, 49000401h
popad
popad
add byte ptr [ecx], bl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x118c4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x13000	0x100c	.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	0x12c	.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	0x10de4	0x11000	False	0.37357823989	data	6.53865304618	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0xad0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x13000	0x100c	0x2000	False	0.205810546875	data	2.60682974307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x13364	0xca8	data		
RT_GROUP_ICON	0x13350	0x14	data		
RT_VERSION	0x130f0	0x260	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaAryConstruct2, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, __vbaStrComp, __vbaStrToAnsi, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

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

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: transferencia.exe PID: 6424 Parent PID: 5996

General

Start time:	11:37:50
Start date:	22/04/2021
Path:	C:\Users\user\Desktop\transferencia.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\transferencia.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	718116C2CC15E564DB71B3BDA3F966E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.852343064.0000000002300000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis