



ID: 624276
Sample Name:
Transferencia.exe
Cookbook: default.jbs
Time: 13:17:05
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Transferencia.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: GuLoader 3
Yara Signatures 3
Memory Dumps 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Networking 4
Data Obfuscation 4
Malware Analysis System Evasion 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
C:\Users\user\AppData\Local\Temp\Dadoes.thi 8
C:\Users\user\AppData\Local\Temp\FJERKRFARMENES.ini 8
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll 9
Static File Info 9
General 9
File Icon 9
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 10
Rich Headers 11
Data Directories 11
Sections 11
Resources 12
Imports 12
Version Infos 13
Possible Origin 13
Network Behavior 13
Statistics 13
System Behavior 13
Analysis Process: Transferencia.exePID: 4736, Parent PID: 2376 13
General 13
File Activities 13
File Created 13
File Deleted 15
File Written 15
File Read 15
Disassembly 16

Copyright Joe Security LLC 2022

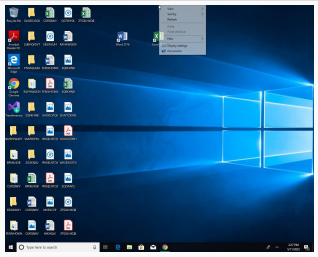
Windows Analysis Report

Transferencia.exe

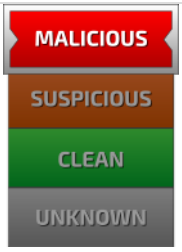
Overview

General Information

Sample Name:	Transferencia.exe
Analysis ID:	624276
MD5:	fb1d131568bdd2..
SHA1:	ff02df2cb07c221...
SHA256:	42625067621ac2..
Tags:	exe
Infos:	



Detection



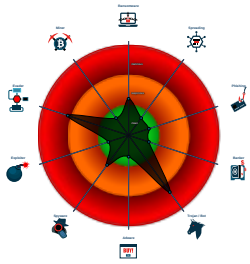
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Tries to detect virtualization through...
- C2 URLs / IPs found in malware con...
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /...
- Uses code obfuscation techniques (...
- Detected potential crypto function
- PE / OLE file has an invalid certifica...

Classification



Process Tree

- **System is w10x64**
- Transferencia.exe (PID: 4736 cmdline: "C:\Users\user\Desktop\Transferencia.exe" MD5: FB1D131568BDD2FA951608534F83A75C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1hB?$1A"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.756250628.0000000002D50000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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

Malware Analysis System Evasion

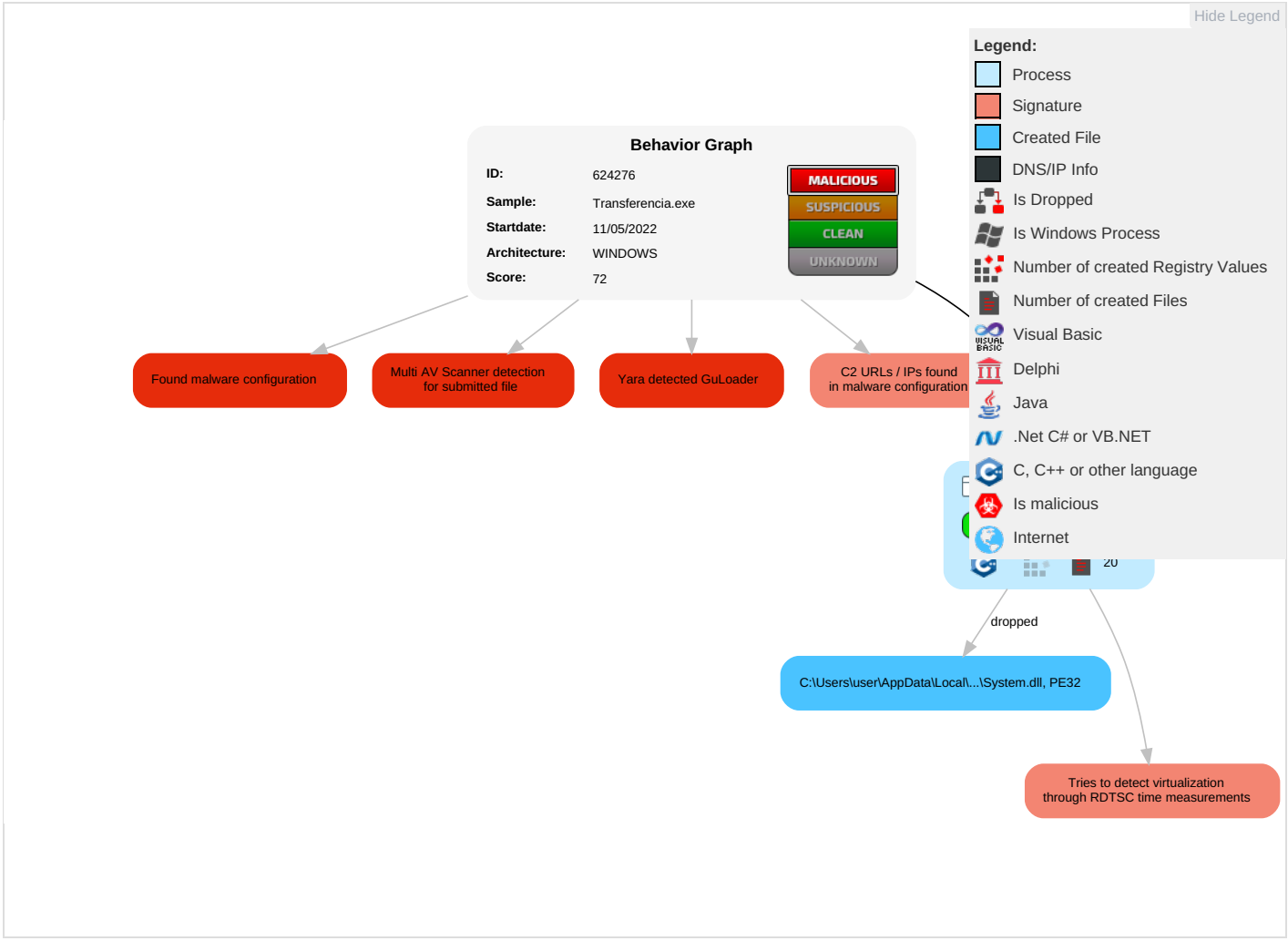


Tries to detect virtualization through RDTSC time measurements

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 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

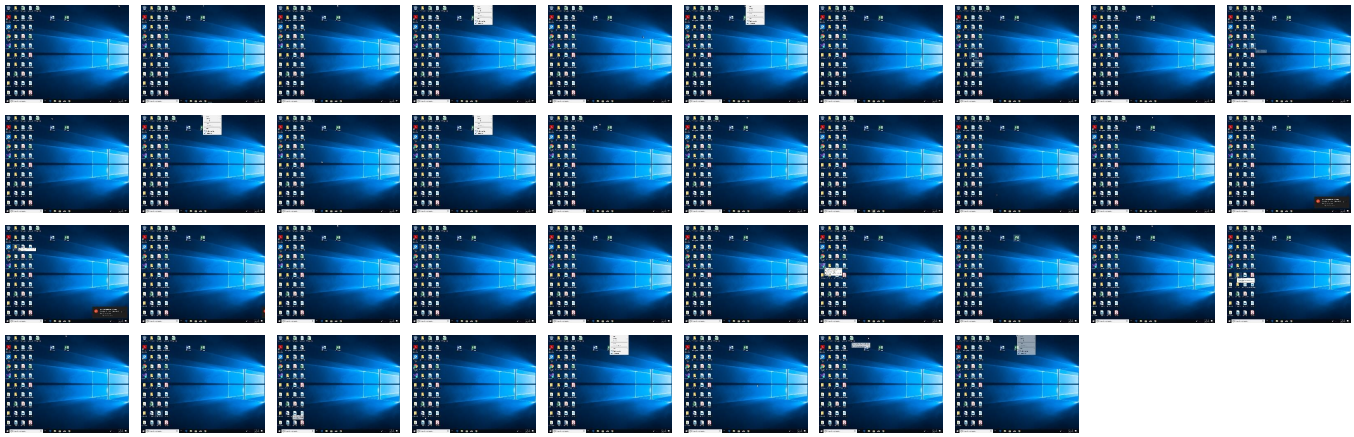
Behavior Graph



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	27%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	Transferencia.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624276
Start date and time: 11/05/202213:17:05	2022-05-11 13:17:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Transferencia.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:	29
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:	mal72.troj.evad.winEXE@1/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 62%) • Quality average: 88.3% • Quality standard deviation: 21.7%
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 • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, time.windows.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Copyright Joe Security LLC 2022

Simulations

Behavior and APIs

No simulations

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\Local\Temp\Dadoes.thi

Process:	C:\Users\user\Desktop\Transferencia.exe
File Type:	data
Category:	dropped
Size (bytes):	163440
Entropy (8bit):	7.327257313432124
Encrypted:	false
SSDEEP:	3072:TAJ8oRPFQ7IfdpA9PCAHmkvLI75I504TTRajaO7HlnKEmou:Mmcd2nGkvLI504TTIb7Fbmou
MD5:	12189C0F205D353F5492E0231A237B97
SHA1:	0ADAC1C37C0B1D812B77FA9466E501B068802061
SHA-256:	4C5C37CDD6B432A2E245CB3E4D5E31919BBA8A9A7246769A40E781EA4A407D71
SHA-512:	B67C7470BB1D1898A6233DF1D61034A76BC9A862A97C885CE9312A1FF318D0D1C7BBF228FB8E0846D3BAA5AC14751F562943356305569C9DF88F8449B70D7DC
Malicious:	false
Reputation:	low
Preview:	.E.S..$.....B...^... ..u.H...&..t.....14.x].....}N..+.G.....Tp.$..{S...`).....b..Av.....X..n....^.IO`lw.(.....G..).=.<.B...8.t.&.iy.../R8...W..Ji.....cF...(.E..{c.....B*>y..6.....1f.r./.....\.@. .2J...w.....0.8..D.;.<de..p.G.i....'...*.&.B..W<..I2.....!..w&.=I.P..x..e.kH.....K.....[*..9..3....(...,..T.i.JP.W.%w.w=..r.w7X... 6.....Z...Q..bN..H..<..d..Q7...w..?.. Q.....Y[g._.... e...%m+6k.h.oT.\..aF.(..%....k..*L.....O.....B..... .....B..9."....w. ..s..a....U@....N..{}.}D....8 ..k..Rp..\.1..).4.]{..9..&.X._...t}...v.1...p%Ts.B-'... `_>.....0.<1..Cqd....l'.....c.}8XB.. 8...,.m6Zm.v..X+..wG.pq...MY`.g....hX.....2..%.G.O....h....I...G....c.....J_.pF|;f.v.....X.i.....b....7d.%...24..s..h.....v`...M7....o.`....&..,.E.0:.u...F....q.;..n..,..s.-.r*.....S.m...5 .+.U.....~.h7.Z..sX..>"...zU.g1<.hA...../%.....N.G.n?..FJ.v.....k...$.X.LCN..T.^O..)..=.l..e,.P.*+xuF...Q.D..qC6...jr..I..7...Et...VV ..d1...2_W..Y&.;.

C:\Users\user\AppData\Local\Temp\FJERKRFARMENES.ini

Process:	C:\Users\user\Desktop\Transferencia.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	35
Entropy (8bit):	4.193429088311724
Encrypted:	false
SSDEEP:	3:Nn4y2XEIlz4Acv:t12ez4Acv
MD5:	459F02DD36C8D63BCDF3A4078AEBD592
SHA1:	C61BA4265FB1C24ED73775149BB1F9A62B688CC9
SHA-256:	428CF1D18B7B06811B313C57DF8D240EB44350F63336BD2822B3477525C8BC1A
SHA-512:	A90C2BF7B01C34C5E6E16BA0391258942EDE941424BEF83398F5FE6F8936D75AD68148787F51AE80E03F565D6533811726D8C958888DE02738F514383AA7F7F6
Malicious:	false
Reputation:	low
Preview:	[surucucu]..Lockram2=strandlberen..

C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll

Process:	C:\Users\user\Desktop\Transferencia.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.5547497516761295
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:	Transferencia.exe
File size:	254208
MD5:	fb1d131568bdd2fa951608534f83a75c
SHA1:	ff02df2cb07c221b8ed3583c6dafb8c0e35684f8
SHA256:	42625067621ac2dba6b95e565a48454637f46185356034da214a00a3d453c971
SHA512:	ef46d1fc90b046234a2939d1cbbadeb99cca056bfba74b3b1480af1a1171698a436cc23a809c8f0ec9f2ce5ca45d91db31151311415ed38a137070924476dc10
SSDEEP:	6144:s3yztNlmkDzzo+3sYIEJwqq1XPo6BktVrQGs20z:s3+FvzxsPXj1/o6Aiz
TLSH:	2344D01E3225C4E6F88883765F3A9B0B198FAC03219105177772BBB99B39383C95F5D5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L...h.Oa.....h....:....

File Icon



Icon Hash:	8803969c49c2c3c0

Static PE Info

General

Entrypoint:	0x40350a
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9A68 [Sat Sep 25 21:53:44 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Talonen Pral NONPERFECTIBILITY Unmigrant6 ", O=ORDLYDEN, L=Bourg-Saint-Maurice, S=Auvergne-RhÃ´ne-Alpes, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/10/2022 12:58:17 PM 5/10/2023 12:58:17 PM
Subject Chain	• CN="Talonen Pral NONPERFECTIBILITY Unmigrant6 ", O=ORDLYDEN, L=Bourg-Saint-Maurice, S=Auvergne-RhÃ´ne-Alpes, C=FR
Version:	3
Thumbprint MD5:	C01462F3E1A1421FC7156C98C104EC74
Thumbprint SHA-1:	92A7393883A3AF47A744D137119C6E6BAEA9BC27
Thumbprint SHA-256:	41ACF6A35BC3571C0748976A332965863E86A47C8FBBED9FE240EE0D66E8DEA9
Serial:	F7E6FA3055C43850

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch

Copyright Joe Security LLC 2022

Instruction
call esi
test eax, eax
jne 00007F0474C9CC0Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F0474C9CBDAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B18h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3da000	0x139f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3da38	0x6c8	.data
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6670	0x6800	False	0.667931189904	data	6.43600264122	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb78	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x31000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3da000	0x139f0	0x13a00	False	0.570872312898	data	6.54983643379	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3da358	0x8592	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x3e28f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 1056964863	English	United States
RT_ICON	0x3e6b18	0x25a8	data	English	United States
RT_ICON	0x3e90c0	0x1a68	data	English	United States
RT_ICON	0x3eab28	0x10a8	data	English	United States
RT_ICON	0x3ebbd0	0x988	data	English	United States
RT_ICON	0x3ec558	0x6b8	data	English	United States
RT_ICON	0x3ecc10	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x3ed078	0x100	data	English	United States
RT_DIALOG	0x3ed178	0x11c	data	English	United States
RT_DIALOG	0x3ed298	0xc4	data	English	United States
RT_DIALOG	0x3ed360	0x60	data	English	United States
RT_GROUP_ICON	0x3ed3c0	0x76	data	English	United States
RT_VERSION	0x3ed438	0x274	data	English	United States
RT_MANIFEST	0x3ed6b0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos	
Description	**Data**
LegalCopyright	Markedsana
FileVersion	24.8.29
CompanyName	vugvalidatin
LegalTrademarks	METACINNAB
Comments	Spiroloculin113
ProductName	Leuk
FileDescription	Janfridelefrek82
Translation	0x0409 0x04b0

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: Transferencia.exe PID: **4736**, Parent PID: **2376**

General	
Target ID:	0
Start time:	13:18:06
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\Transferencia.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Transferencia.exe"
Imagebase:	0x400000
File size:	254208 bytes
MD5 hash:	FB1D131568BDD2FA951608534F83A75C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.756250628.0000000002D50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsnC5D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nstC730.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
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	405AD4	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
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	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nstC730.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A94	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	7	406036	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
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	405AD4	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
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	405AD4	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Dadoes.thi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	6	406036	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsnC5D7.tmp	success or wait	1	403852	DeleteFileW
C:\Users\user\AppData\Local\Temp\nstC730.tmp	success or wait	1	405C55	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstC730.tmp\System.dll	0	12288	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Transferencia.exe	unknown	512	success or wait	231	4060A7	ReadFile
C:\Users\user\Desktop\Transferencia.exe	unknown	4	success or wait	2	4060A7	ReadFile
C:\Users\user\Desktop\Transferencia.exe	unknown	4	success or wait	11	4060A7	ReadFile
C:\Users\user\AppData\Local\Temp\Dadoes.thi	unknown	1048576	success or wait	1	732A2C59	ReadFile

Disassembly

No disassembly

Copyright Joe Security LLC 2022