ID: 430603
Sample Name: DOCUMENTOS CORREOS.exe
Cookbook: default.jbs
Time: 17:26:33
Date: 07/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report DOCUMENTOS CORREOS.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
DNS Queries 13
DNS Answers 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: DOCUMENTOS CORREOS.exe PID: 5320 Parent PID: 5508 13
General 13
File Activities 14
Analysis Process: DOCUMENTOS CORREOS.exe PID: 5392 Parent PID: 5320 14
General 14
File Activities 14
File Created 14

Disassembly 14
Code Analysis 14

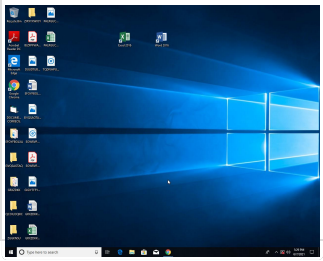
Analysis Report DOCUMENTOS CORREOS.exe

Overview

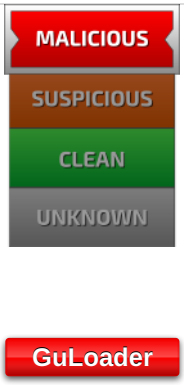
General Information

Sample Name:	DOCUMENTOS CORREOS.exe
Analysis ID:	430603
MD5:	c73ab52ccb3b77…
SHA1:	99e3f024e741388.
SHA256:	8fe1d7d80763561.
Infos:	

Most interesting Screenshot:



Detection



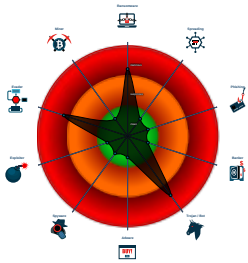
GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to hide a threa…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- DOCUMENTOS CORREOS.exe (PID: 5320 cmdline: 'C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe' MD5: C73AB52CCB3B77FFDA43AB3764FFF1AB)
  - DOCUMENTOS CORREOS.exe (PID: 5392 cmdline: 'C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe' MD5: C73AB52CCB3B77FFDA43AB3764FFF1AB)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://www.mediafire.com/file/md0mc3zocq6uh6b/gbam_encrypted_65A39A0.bin/file\u0000\u0000",
  "User Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.279722809.000000000062 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000004.00000000.278693331.000000000056 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000004.00000002.486013693.000000000056 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: DOCUMENTOS CORREOS.exe PID: 5392	JoeSecurity_VB6Downloaderic	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: DOCUMENTOS CORREOS.exe PID: 5392	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Anti Debugging:

Contains functionality to hide a thread from the debugger

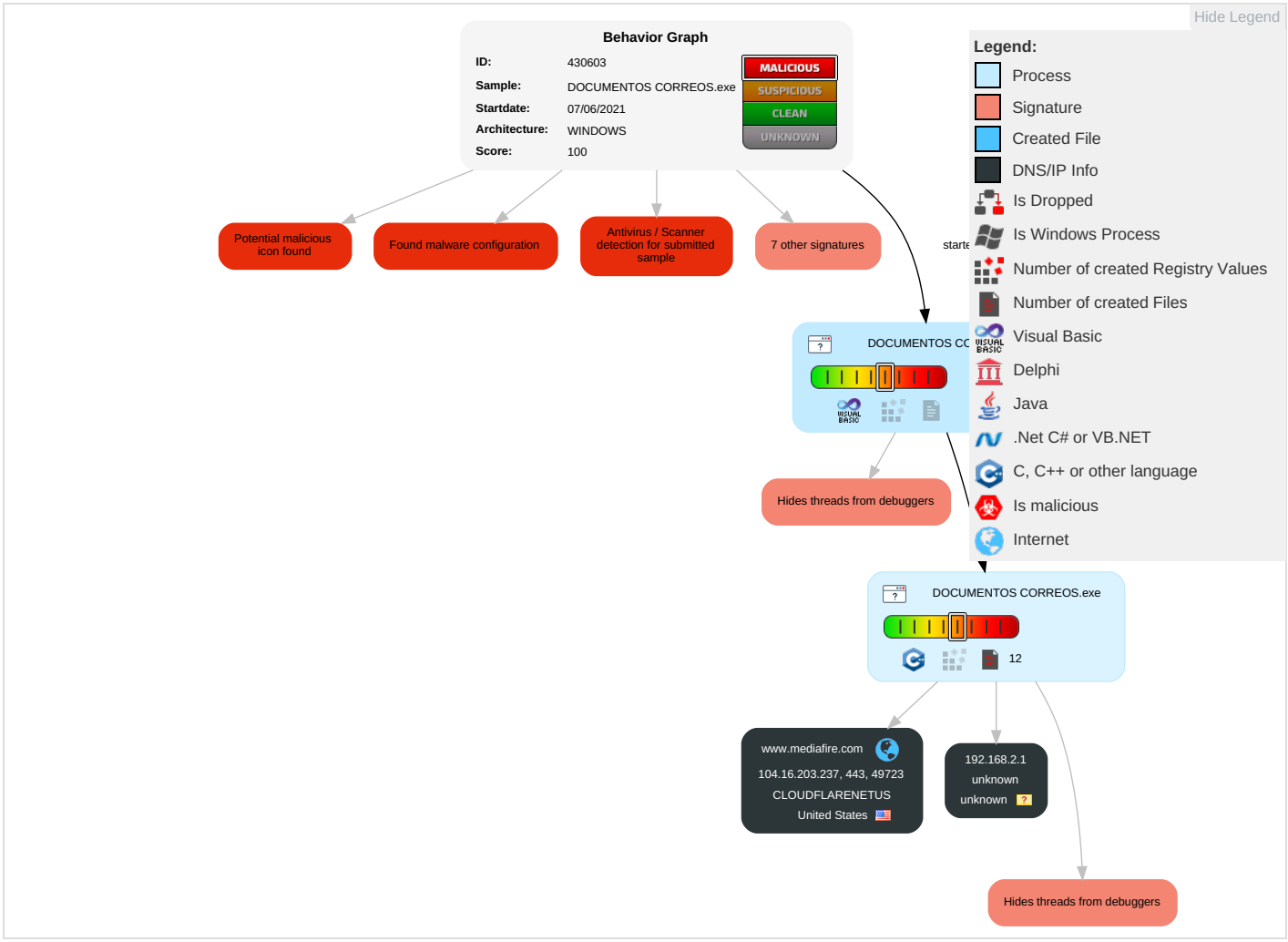
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

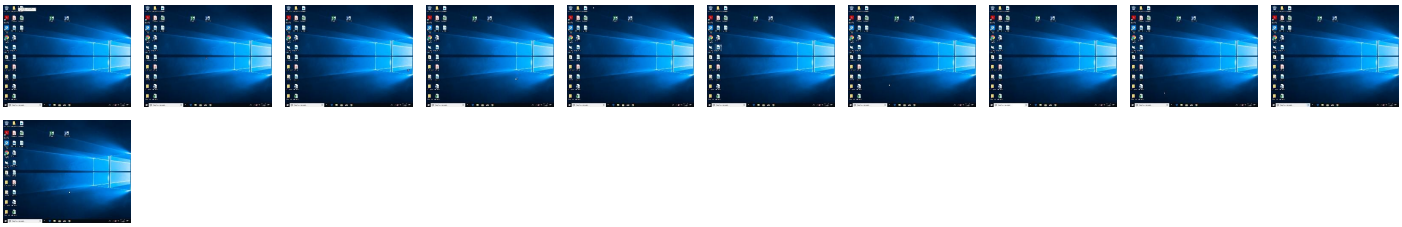
Behavior Graph



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
DOCUMENTOS CORREOS.exe	75%	Virustotal		Browse
DOCUMENTOS CORREOS.exe	86%	ReversingLabs	Win32.Trojan.Guloader	
DOCUMENTOS CORREOS.exe	100%	Avira	TR/AD.VBCryptor.vjznr	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.DOCUMENTOS CORREOS.exe.400000.0.unpack	100%	Avira	TR/AD.VBCryptor.vjznr		Download File
4.0.DOCUMENTOS CORREOS.exe.400000.0.unpack	100%	Avira	TR/AD.VBCryptor.vjznr		Download File
0.2.DOCUMENTOS CORREOS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1134906		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mediafire.com	104.16.203.237	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.mediafire.com/file/md0mc3zocq6uh6b/gbam_encrypted_65A39A0.bin/file	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.203.237	www.mediafire.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430603
Start date:	07.06.2021
Start time:	17:26:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOCUMENTOS CORREOS.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:	mal100.rans.troj.evad.winEXE@3/0@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.7% (good quality ratio 10.9%) • Quality average: 43.3% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 55% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:28:09	API Interceptor	107x Sleep call for process: DOCUMENTOS CORREOS.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.203.237	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• www.mediafire.com/images/icons/myfiles/default.png
	http://download2134.mediafire.com/6d7pu7669u7g/5vpr2kr4s29utk7/PAG004.tgz	Get hash	malicious	Browse	• www.mediafire.com/download_repair.php?flag=3&dkey=6d7pu7669u7&qkey=5vpr2kr4s29utk7&ip=84.17.52.40&ref=3
	http://www.mediafire.com/file/cnwik2kgdebsisy/PAG0002.tgz/file	Get hash	malicious	Browse	• www.mediafire.com/images/icons/myfiles/default.png
	http://www.mediafire.com/file/4xm9i7c25z2wtqj/Parsel+Detaylar%C4%B1.7z/file	Get hash	malicious	Browse	• www.mediafire.com/file/4xm9i7c25z2wtqj/Parsel+Detaylar%C4%B1.7z/file
	http://https://download1580.mediafire.com/4xprc4caulsg/qpuaxqx0pdqcik8/Solicitud+de+presupuesto.7z	Get hash	malicious	Browse	• www.mediafire.com/upgrade
	http://www.mediafire.com/file/f28ppsxzjuy1xsb/UPSRO+2809203321.7z/file	Get hash	malicious	Browse	• www.mediafire.com/file/f28ppsxzjuy1xsb/UPSRO+2809203321.7z/file
	http://www.mediafire.com/file/xn60pc8souxfqax/fac_01200.7z/file	Get hash	malicious	Browse	• www.mediafire.com/file/xn60pc8souxfqax/fac_01200.7z/file

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://www.mediafire.com/file/cmzz439j3nr3cp9/TNT1.7z/file	Get hash	malicious	Browse	• www.mediafire.com/file/cmzz439j3nr3cp9/TNT1.7z/file
	http://www.mediafire.com/file/59pevvifny3y35x/Comanda+de+achizitie.7z/file	Get hash	malicious	Browse	• www.mediafire.com/file/59pevvifny3y35x/Comanda+de+achizitie.7z/file
	http://https://download2272.mediafire.com/dee0x8gd9lhg/kfsfaocy6dzql61/Cheque+Copy.7z	Get hash	malicious	Browse	• www.mediafire.com/about/
	http://www.mediafire.com/file/449cj5l0pxynnlh/Endesa-Facturacion20201806.zip	Get hash	malicious	Browse	• www.mediafire.com/file/449cj5l0pxynnlh/Endesa-Facturacion20201806.zip
	http://cartadelcobro.com/pdf_carta_cobro-23-04-2020/	Get hash	malicious	Browse	• www.mediafire.com/file/ss26bj0bvghigyj/Cobro.zip/file

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.mediafire.com	DOCUMENTOS CORREOS.exe	Get hash	malicious	Browse	• 104.16.202.237
	BRnRfGXrIP.exe	Get hash	malicious	Browse	• 104.16.202.237
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.202.237
	Autuacao-2305148784007A.exe	Get hash	malicious	Browse	• 104.16.202.237
	http://download2134.mediafire.com/6d7pu7669u7g/5vpr2kr4s29utk7/PAG004.tgz	Get hash	malicious	Browse	• 104.16.203.237
	http://www.mediafire.com/file/cnwik2kgdebsisy/PAG0002.tgz/file	Get hash	malicious	Browse	• 104.16.203.237
	http://download1716.mediafire.com/4ovq1dagh3qg/llznllwcu118fj5/New+Order.tgz	Get hash	malicious	Browse	• 104.16.202.237
	http://www.mediafire.com/file/4xm9i7c25z2wtqj/Parsel+Detaylar%C4%B1.7z/file	Get hash	malicious	Browse	• 104.16.203.237
	http://www.mediafire.com/file/4xm9i7c25z2wtqj/Parsel+Detaylar%C4%B1.7z/file	Get hash	malicious	Browse	• 104.16.202.237
	http://https://download1580.mediafire.com/4xprc4caulsg/qpuaxqx0pdqcik8/Solicitud+de+presupuesto.7z	Get hash	malicious	Browse	• 104.16.203.237
	http://https://download1582.mediafire.com/ntorjrq3jvwg/xpqdxdvhyo668qg/Android+WhatsApp+to+iPhone+Transfer+-+DU+x32.zip	Get hash	malicious	Browse	• 104.16.202.237
	http://www.mediafire.com/file/f28ppsxzjuy1xsb/UPSRO+2809203321.7z/file	Get hash	malicious	Browse	• 104.16.203.237
	http://https://www.mediafire.com/file/que9zdctac0t9w8/Cerere_de_achizitie.7z/file	Get hash	malicious	Browse	• 104.16.203.237
	http://www.mediafire.com/file/69twv65ip7pnmit/Pago+de+septiembre.7z/file	Get hash	malicious	Browse	• 104.16.202.237
	http://www.mediafire.com/file/xn60pc8souxfqax/fac_01200.7z/file	Get hash	malicious	Browse	• 104.16.203.237
	http://www.mediafire.com/file/cmzz439j3nr3cp9/TNT1.7z/file	Get hash	malicious	Browse	• 104.16.203.237
	http://download1525.mediafire.com/a2niozn5iheg/ayhephnsi8hnlgv/test.exe	Get hash	malicious	Browse	• 104.16.202.237
	http://https://www.mediafire.com/file/q4ic4hzhjjsvrdr/Posta+Romana+12082033201829.7z/file	Get hash	malicious	Browse	• 104.16.202.237
	http://https://www.mediafire.com/file/q4ic4hzhjjsvrdr/Posta+Romana+12082033201829.7z/file	Get hash	malicious	Browse	• 104.16.203.237

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	DOCUMENTOS CORREOS.exe	Get hash	malicious	Browse	• 104.16.202.237
	DOCUMENTOS CORREOS.exe	Get hash	malicious	Browse	• 104.16.202.237
	BBS FX.xlsx	Get hash	malicious	Browse	• 104.26.0.222
	PAYMENT RECEIPT #FO1420111.exe	Get hash	malicious	Browse	• 104.21.19.200
	StubV4.exe	Get hash	malicious	Browse	• 172.67.188.154
	Order No. BCM #03122020.exe	Get hash	malicious	Browse	• 104.21.93.53
	Confirmation Transfer Note MT103 Ref#8892626882.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping documents & Proforma invoice.exe	Get hash	malicious	Browse	• 172.67.188.154
	TT500202106029589435472.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment Swift copy MT103.exe	Get hash	malicious	Browse	• 104.21.19.200
	plagin.exe	Get hash	malicious	Browse	• 104.25.233.53
	New Order.exe	Get hash	malicious	Browse	• 172.67.155.26
	rtgs_2021-06-07_02-01.exe	Get hash	malicious	Browse	• 104.21.93.70
	FORM C1.xlsx	Get hash	malicious	Browse	• 104.21.61.102
	rtgs_pdf.exe	Get hash	malicious	Browse	• 104.21.93.70
	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.227.38.74
	sample.EXE	Get hash	malicious	Browse	• 172.67.206.104
	CSTB FR ORDER 789.exe	Get hash	malicious	Browse	• 172.67.193.3
	SC-BANK TRANSFER TT-COPY-FRIDAY0621_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENT MT103 REMITTANCE SWIFT.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	OewA04QDBh.exe	Get hash	malicious	Browse	• 104.16.203.237
	plagin.exe	Get hash	malicious	Browse	• 104.16.203.237
	statistic-608048546.xls	Get hash	malicious	Browse	• 104.16.203.237
	Zd1j3hnY8u.exe	Get hash	malicious	Browse	• 104.16.203.237
	HNUQajtypz.exe	Get hash	malicious	Browse	• 104.16.203.237
	SOA_Outstanding_Balance.exe	Get hash	malicious	Browse	• 104.16.203.237
	85OpNw6eXm.exe	Get hash	malicious	Browse	• 104.16.203.237
	QUMuMnixcc.exe	Get hash	malicious	Browse	• 104.16.203.237
	riy66qgtIR.exe	Get hash	malicious	Browse	• 104.16.203.237
	R43YJpd6nj.exe	Get hash	malicious	Browse	• 104.16.203.237
	RFQ.exe	Get hash	malicious	Browse	• 104.16.203.237
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	• 104.16.203.237
	SecuriteInfo.com.Trojan.DownLoader39.38629.28832.exe	Get hash	malicious	Browse	• 104.16.203.237
	3vuLRePalU.exe	Get hash	malicious	Browse	• 104.16.203.237
	sZBBKNIKMX.exe	Get hash	malicious	Browse	• 104.16.203.237
	lnD4uofi2O.exe	Get hash	malicious	Browse	• 104.16.203.237
	KWLMpN39y2.exe	Get hash	malicious	Browse	• 104.16.203.237
	JJ1PbTh0SP.dll	Get hash	malicious	Browse	• 104.16.203.237
	Secured-Message_7634-7.html	Get hash	malicious	Browse	• 104.16.203.237
	treetop-payroll-075491-pdf.HtmL	Get hash	malicious	Browse	• 104.16.203.237

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):	4.338112761945723
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:	DOCUMENTOS CORREOS.exe
File size:	122880
MD5:	c73ab52ccb3b77ffda43ab3764fff1ab
SHA1:	99e3f024e741388c0a788df19fb87bf105ab84f4
SHA256:	8fe1d7d807635615314910e8145e2e050afd648a5eb7be8 5908563b30290e2fd
SHA512:	80a6e6794465186450b8e8776de0b0598459319b42494a 4937da373caa2dae63f12e197130c76edb76d3f5cba86c6 11f5eaa221eb62152089a682d0ff33decfe
SSDEEP:	1536:Qth8H3nVcq+YnRThE1K/ZZusX0b/g8uz:QU3n6p YFRu+08p
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L....e`K..... ....$.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401524
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:	0x4B6065C8 [Wed Jan 27 16:11:52 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:	f40fcd81751084aec6b61b1899b8625f

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1a978	0x1b000	False	0.30138708044	data	4.55242334496	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1c000	0xb4c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x934	0x1000	False	0.173828125	data	1.99326688739	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 7, 2021 17:28:08.968982935 CEST	192.168.2.3	8.8.8.8	0x39a7	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 7, 2021 17:28:09.019900084 CEST	8.8.8.8	192.168.2.3	0x39a7	No error (0)	www.mediafire.com		104.16.203.237	A (IP address)	IN (0x0001)
Jun 7, 2021 17:28:09.019900084 CEST	8.8.8.8	192.168.2.3	0x39a7	No error (0)	www.mediafire.com		104.16.202.237	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DOCUMENTOS CORREOS.exe PID: 5320 Parent PID: 5508

General

Start time:	17:27:29
Start date:	07/06/2021
Path:	C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	C73AB52CCB3B77FFDA43AB3764FFF1AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.279722809.0000000000620000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: DOCUMENTOS CORREOS.exe PID: 5392 Parent PID: 5320

General

Start time:	17:27:56
Start date:	07/06/2021
Path:	C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOCUMENTOS CORREOS.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	C73AB52CCB3B77FFDA43AB3764FFF1AB
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: 00000004.00000000.278693331.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000004.00000002.486013693.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis