ID: 528679
Sample Name: BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
Cookbook: default.jbs
Time: 16:46:22
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

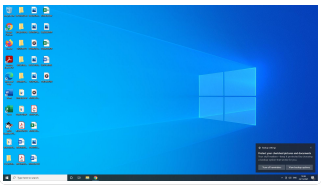
Windows Analysis Report BBVA Liquidaci#U00f3n por F…

Overview

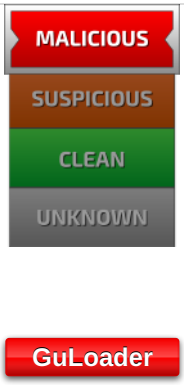
General Information

Sample Name:	BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
Analysis ID:	528679
MD5:	d879bb7572225e..
SHA1:	c34286e6e9d150..
SHA256:	b29f69052169c50.
Infos:	

Most interesting Screenshot:



Detection



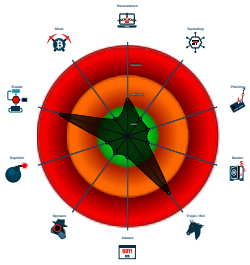
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Found a high number of Window / Us…
- Sample file is different than original …
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64native**
- BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe (PID: 2056 cmdline: "C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe" MD5: D879BB7572225EBF68F74406710F6EA0)
  - CasPol.exe (PID: 7084 cmdline: "C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 7096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- UserOOBEBroker.exe (PID: 7188 cmdline: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000000.1479594231.00000000011 60000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

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

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

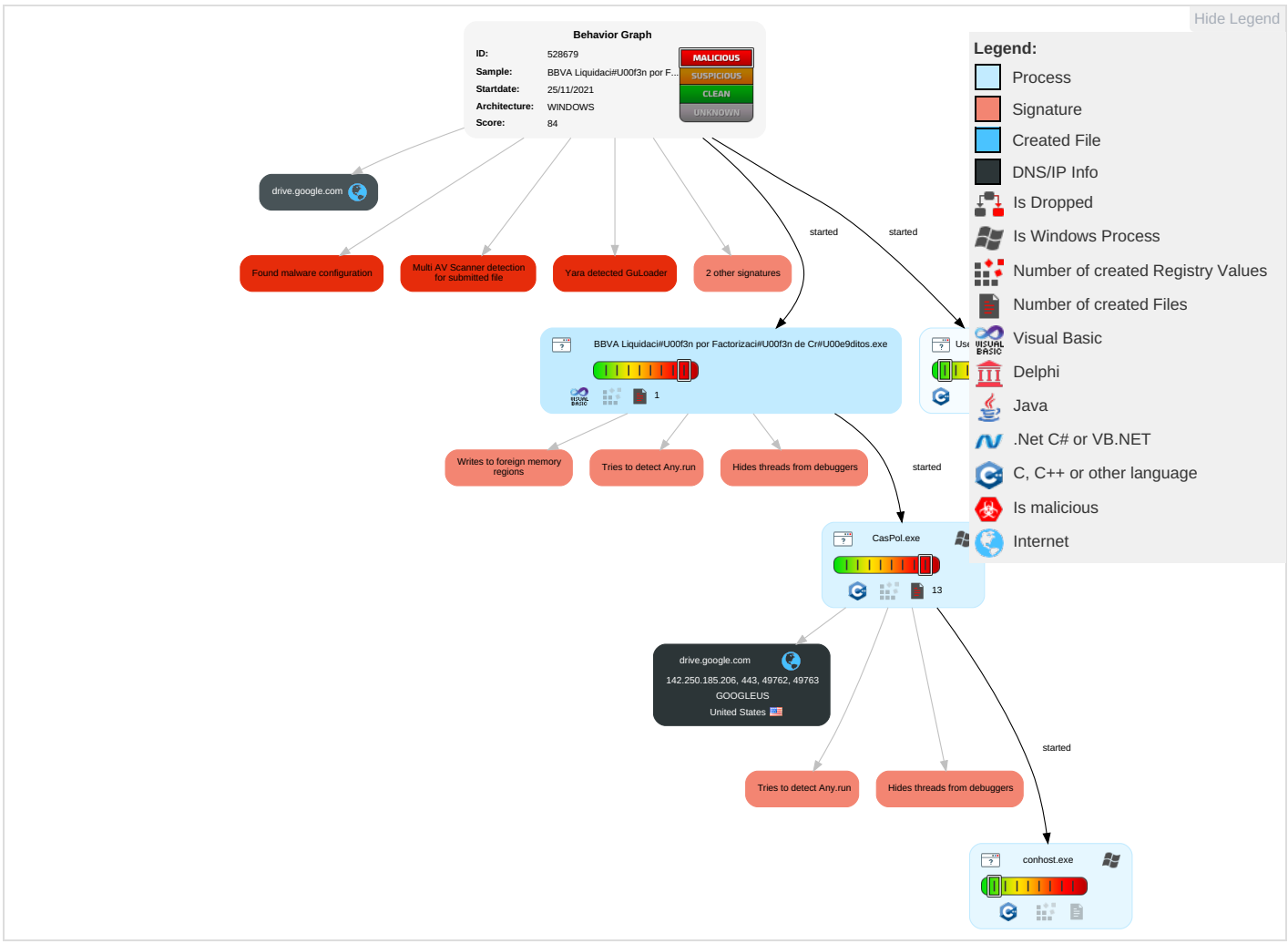
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

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	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phor Calls/SMS
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	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 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	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

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
BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe	54%	Virustotal		Browse
BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe	49%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.206	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528679
Start date:	25.11.2021
Start time:	16:46:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	34
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@5/1@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:48:55	API Interceptor	1307x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Statement.html	Get hash	malicious	Browse	• 142.250.185.206
	Michal November 23, 2021.html	Get hash	malicious	Browse	• 142.250.185.206
	survey-1384723731.xls	Get hash	malicious	Browse	• 142.250.185.206
	Wfedtqxbgeorkwcgiehsnsjbdjghrpjtlr.exe	Get hash	malicious	Browse	• 142.250.185.206
	survey-1378794827.xls	Get hash	malicious	Browse	• 142.250.185.206
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 142.250.185.206
	mN2NobuuDv.exe	Get hash	malicious	Browse	• 142.250.185.206
	cs.exe	Get hash	malicious	Browse	• 142.250.185.206
	ORDINE + DDT A.M.F SpA.exe	Get hash	malicious	Browse	• 142.250.185.206
	mal1.html	Get hash	malicious	Browse	• 142.250.185.206
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 142.250.185.206
	DOC5629.htm	Get hash	malicious	Browse	• 142.250.185.206
	Racun je u prilogu.exe	Get hash	malicious	Browse	• 142.250.185.206
	exe.exe	Get hash	malicious	Browse	• 142.250.185.206
	INF-BRdocsx.NDVDELDKRS.msi	Get hash	malicious	Browse	• 142.250.185.206
	2GEg45PlG9.exe	Get hash	malicious	Browse	• 142.250.185.206
	cJ2wN3RKmh.exe	Get hash	malicious	Browse	• 142.250.185.206
	J73PTzDghy.exe	Get hash	malicious	Browse	• 142.250.185.206
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 142.250.185.206
	xzmHphquAP.exe	Get hash	malicious	Browse	• 142.250.185.206

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DFDCBA8CD39083ECED.TMP	
Process:	C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DFDCBA8CD39083ECED.TMP	
Size (bytes):	16384
Entropy (8bit):	0.9277305547216628
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vncU7pCr8P:VSKUpACLFcUVCrG
MD5:	19809EDD1FF00A1D7C105BC58A97CD02
SHA1:	26FB6D339CF2A7474DE6F785166163FA9B2ADBB1
SHA-256:	4745D04A4BB99D70866D722394D9E71F3FAE597AA84E229A1E3B40F31521594C
SHA-512:	434722936006B56B042FB5C72CAB98D8B7615A5A0E48EE6746DD6839BE029029E3BCECF7EFA49DDC8A9DB016FA472FB9EE1CE75126C13E06D66EAA12166A387
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.77275893064669
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:	BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
File size:	131072
MD5:	d879bb7572225ebf68f74406710f6ea0
SHA1:	c34286e6e9d1502a8e3aff050c35781aee371bbc
SHA256:	b29f69052169c50b19f3f6cc8d724a228a7b378bb8e0a23c6f5b25d01c5b4e3c
SHA512:	1e53afe90647afdb80f3524965cdb3ae58938af6af3d58c642dc3dc30d47a4fb903e0fc71bee32e354c1f0843fd65bcba74cb64aef6b08ff5929943a77685992
SSDEEP:	1536:ttfDCDIBpvzJAmFeyzDoyJ/NaSubkMnYdUXXgSlTtD:tVOIB1t7lyJl16fYdUASlt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....$N.....0.....@.....

File Icon

Icon Hash:	981dca909cee36b0

Static PE Info

General

Entrypoint:	0x4013b4
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:	0x4E24F810 [Tue Jul 19 03:20:48 2011 UTC]
TLS Callbacks:	

General

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:	d77040f4614bccfda7b8aa2e04863738

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ccec	0x1d000	False	0.347235317888	data	4.95688708171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1e000	0x141c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0xf58	0x1000	False	0.337890625	data	3.25376572831	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	
Turkmen	Turkmenistan	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 16:48:54.707391024 CET	192.168.11.20	1.1.1.1	0x4bc	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)

DNS Answers

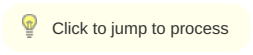
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 16:48:54.717353106 CET	1.1.1.1	192.168.11.20	0x4bc	No error (0)	drive.google.com		142.250.185.206	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe PID: 2056 Parent PID: 6784

General

Start time:	16:48:17
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe"
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	D879BB7572225EBF68F74406710F6EA0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 7084 Parent PID: 2056

General

Start time:	16:48:35
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BBVA Liquidaci#U00f3n por Factorizaci#U00f3n de Cr#U00e9ditos.exe"
Imagebase:	0xd80000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 0000000E.00000000.1479594231.0000000001160000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 7096 Parent PID: 7084

General

Start time:	16:48:36
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cf5d0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: UserOOBEBroker.exe PID: 7188 Parent PID: 1044

General

Start time:	16:56:20
Start date:	25/11/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff7126f0000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis