ID: 532897
Sample Name: 20211129.exe
Cookbook: default.jbs
Time: 19:45:00
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 20211129.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 4
System Summary: 4
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 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
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 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Authenticode Signature 11
Entrypoint Preview 11
Data Directories 11
Sections 11
Resources 11
Imports 11
Version Infos 11
Possible Origin 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
DNS Queries 11
DNS Answers 11
Code Manipulations 12
Statistics 12
Behavior 12
System Behavior 12
Analysis Process: 20211129.exe PID: 8840 Parent PID: 7092 12
General 12
File Activities 12
File Created 12

Registry Activities 12
Key Created 12
Key Value Created 12
Analysis Process: CasPol.exe PID: 3264 Parent PID: 8840 12
General 12
Analysis Process: CasPol.exe PID: 3248 Parent PID: 8840 13
General 13
File Activities 13
File Created 13
Analysis Process: conhost.exe PID: 3200 Parent PID: 3248 13
General 13
File Activities 13
Analysis Process: svchost.exe PID: 3264 Parent PID: 956 13
General 13
File Activities 14
Registry Activities 14
Disassembly 14
Code Analysis 14

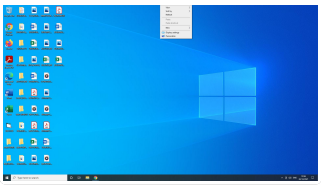
Windows Analysis Report 20211129.exe

Overview

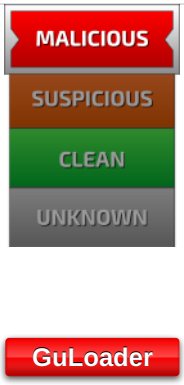
General Information

Sample Name:	20211129.exe
Analysis ID:	532897
MD5:	672587fb175264e.
SHA1:	ab7c2f5edf572d5..
SHA256:	c00b66ef61df201..
Infos:	

Most interesting Screenshot:



Detection



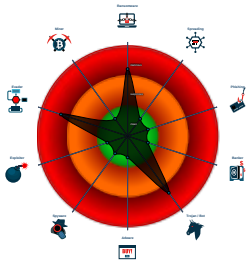
GuLoader

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Sigma detected: Suspicious Svchos…
- 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…

Classification



Process Tree

- **System is w10x64native**
- 20211129.exe (PID: 8840 cmdline: "C:\Users\user\Desktop\20211129.exe" MD5: 672587FB175264EF8B45A2B0857F273F)
  - CasPol.exe (PID: 3264 cmdline: "C:\Users\user\Desktop\20211129.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 3248 cmdline: "C:\Users\user\Desktop\20211129.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - svchost.exe (PID: 3264 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: F586835082F632DC8D9404D83BC16316)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=down"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.785162355.0000000000E10000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

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

System Summary:

Potential malicious icon found

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:

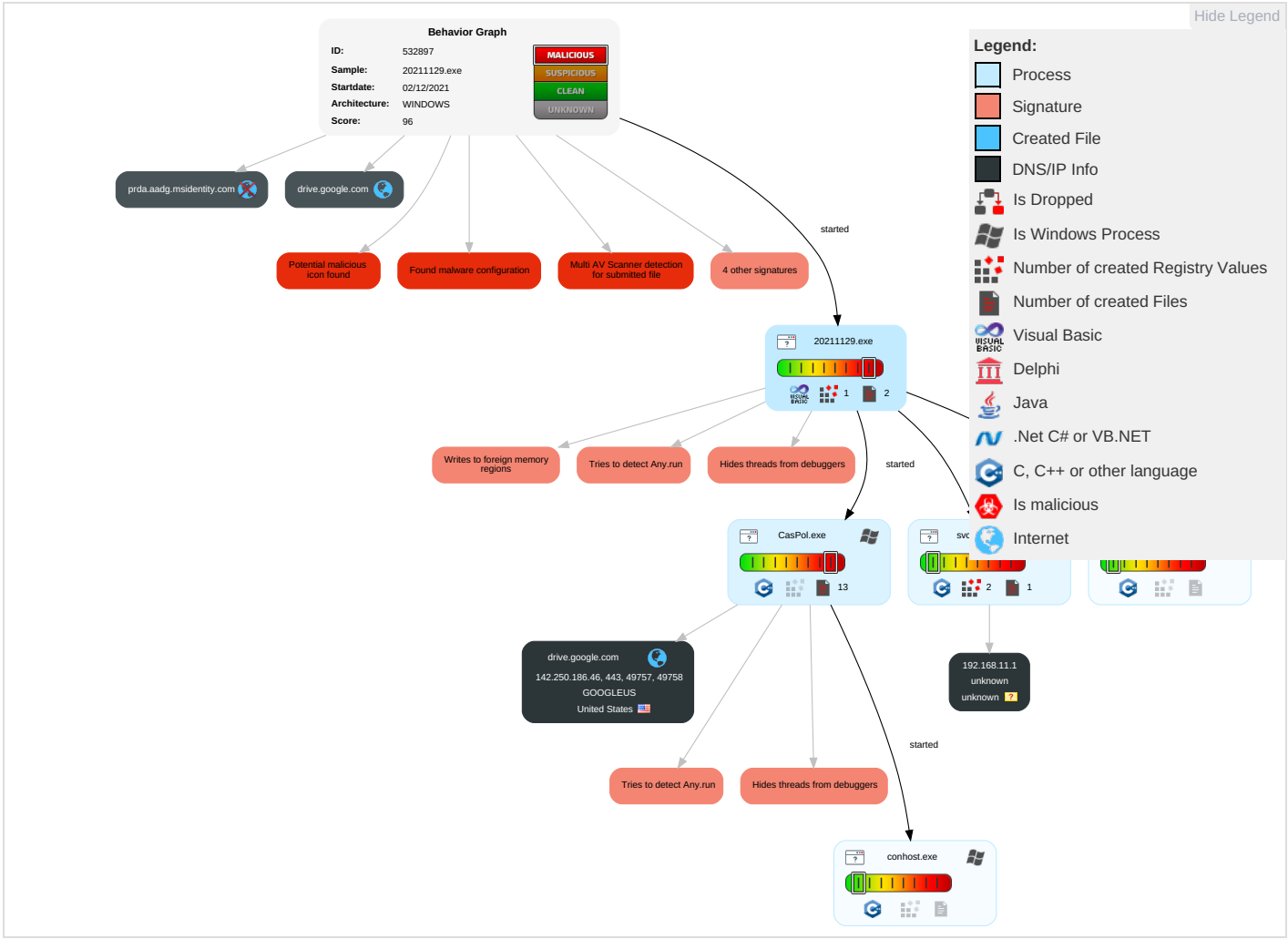
Writes to foreign memory regions

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 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 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)	Process Injection 1 1 1	Security Account Manager	Application Window 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)	DLL Side-Loading 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	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	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

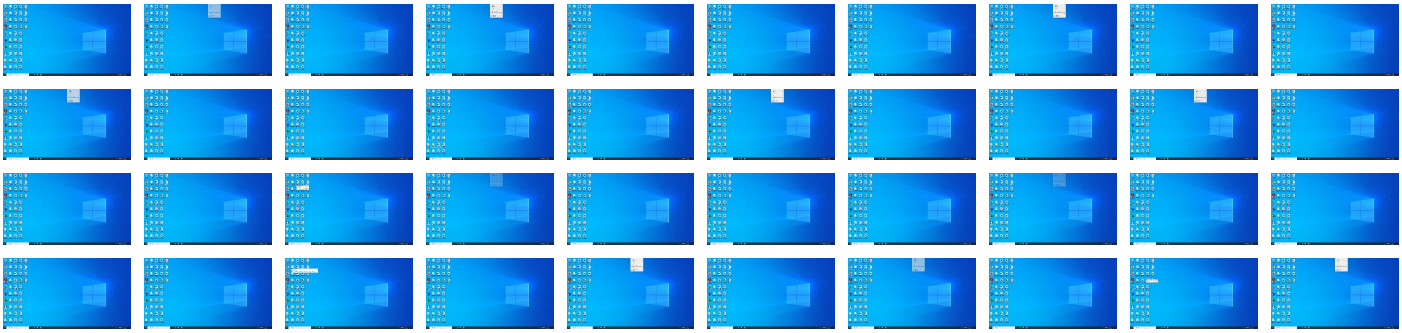
Behavior Graph

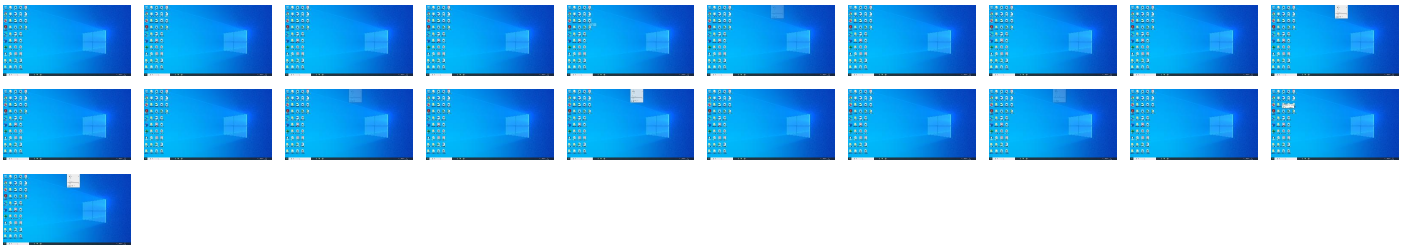


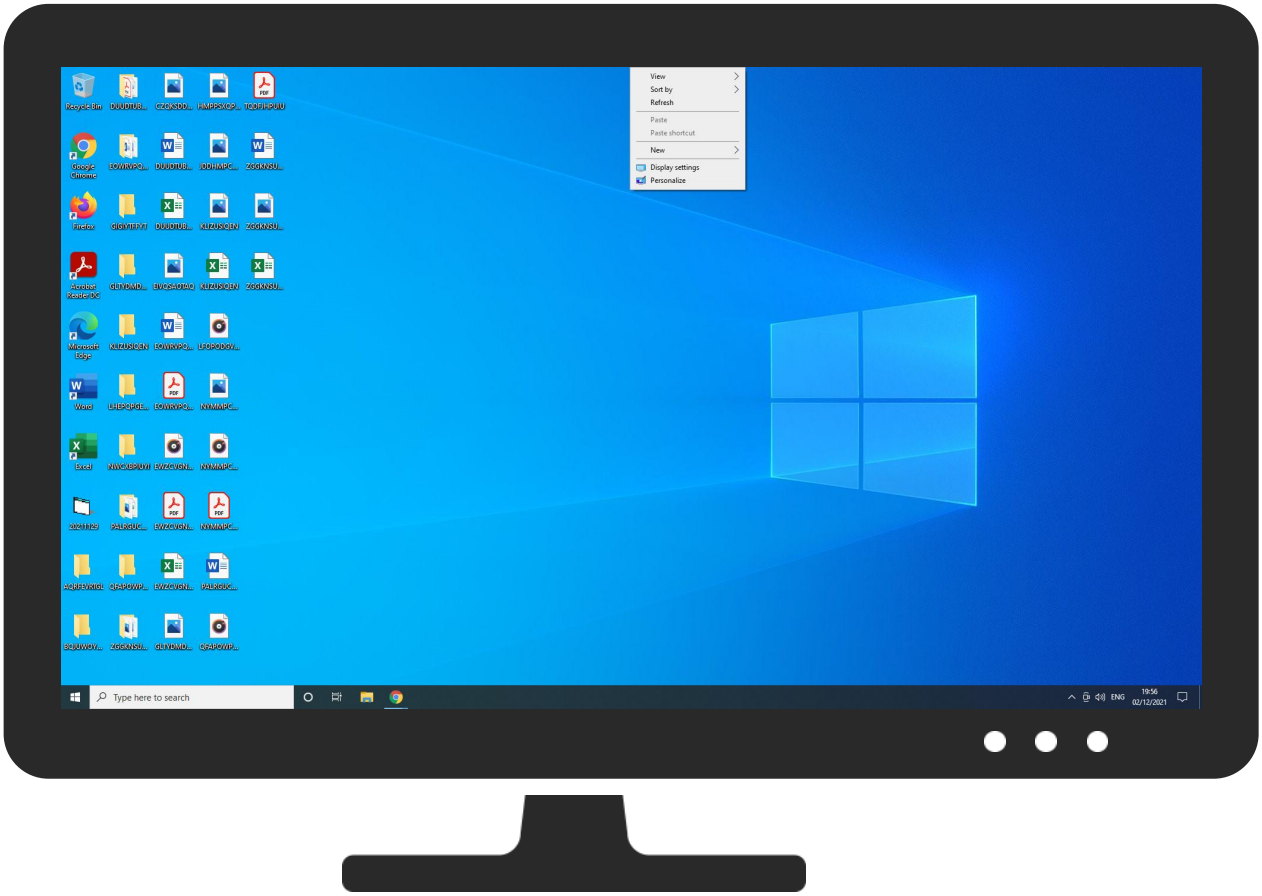
Screenshots

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
20211129.exe	37%	Virustotal		Browse
20211129.exe	22%	Metadefender		Browse
20211129.exe	51%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.20211129.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
3.2.20211129.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/drive-	0%	Avira URL Cloud	safe	
http://schemas.xmlsoap.o	0%	Virustotal		Browse
http://schemas.xmlsoap.o	0%	Avira URL Cloud	safe	
http://https://login.liUTF-16p	0%	Avira URL Cloud	safe	
http://https://csp.witW	0%	Avira URL Cloud	safe	
http://https://login.liUTF-8p	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	
http://passport.net/tb	0%	Avira URL Cloud	safe	
http://go.microsoft.c	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.186.46	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

Private

IP
192.168.11.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532897
Start date:	02.12.2021
Start time:	19:45:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20211129.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:	42
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.rans.troj.evad.winEXE@7/0@1/2
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
19:47:47	Task Scheduler	Run new task: Intel PTT EK Recertification path: "C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_75ffca5eec865b4b\lib\IntelPTTEKRecertification.exe"
19:48:23	API Interceptor	1429x 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	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 142.250.186.46
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 142.250.186.46
	FT A75619637369.vbs	Get hash	malicious	Browse	• 142.250.186.46
	OSJlMxel05.exe	Get hash	malicious	Browse	• 142.250.186.46
	fel.com.html	Get hash	malicious	Browse	• 142.250.186.46
	S6RqSs1LsE.exe	Get hash	malicious	Browse	• 142.250.186.46
	4RXRHeZIG8.exe	Get hash	malicious	Browse	• 142.250.186.46
	kEwILWnlG5.exe	Get hash	malicious	Browse	• 142.250.186.46
	kEwILWnlG5.exe	Get hash	malicious	Browse	• 142.250.186.46
	SecuriteInfo.com.W32.AIDetect.malware2.32340.exe	Get hash	malicious	Browse	• 142.250.186.46
	mUYEdn5OC0.exe	Get hash	malicious	Browse	• 142.250.186.46
	new offers885111832.docx	Get hash	malicious	Browse	• 142.250.186.46
	_0.html	Get hash	malicious	Browse	• 142.250.186.46
	lifehacks_6582318243.docx	Get hash	malicious	Browse	• 142.250.186.46
	counter-1248368226.xls	Get hash	malicious	Browse	• 142.250.186.46
	counter-1248368226.xls	Get hash	malicious	Browse	• 142.250.186.46
	ukmxWblFcs.exe	Get hash	malicious	Browse	• 142.250.186.46
	Narudzba.0953635637.PDF.exe	Get hash	malicious	Browse	• 142.250.186.46
	Orden de compra.exe	Get hash	malicious	Browse	• 142.250.186.46
	EmployeeAssessment.html	Get hash	malicious	Browse	• 142.250.186.46

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):	5.14253569878617
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:	20211129.exe
File size:	156816
MD5:	672587fb175264ef8b45a2b0857f273f
SHA1:	ab7c2f5edf572d5b28d7da50f548d73d49f92b71
SHA256:	c00b66ef61df2012b269bca3e60b301478641292948f1cac579096603ad67f98
SHA512:	67d7444cb44d8b9be7ed2301e64a2368ac21f370b98cbdcdcff895ad35d66e097372c3b50eb5906ef8acc942316a6fe117522988e433660989abaa9caed9076f
SSDEEP:	1536:BUHEm7YNXO6rJiEqawzLDnzf4YIOBFKrf2m6+TFy2rsm1uQBH:BgEm7c+wk7rLDBKH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...*D.X..... .. .0.....0....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401888
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:	
Time Stamp:	0x58F4442A [Mon Apr 17 04:27:22 2017 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:	b209c8634733456633136bfedc71877a

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=affaldsproblemernes@Sisi.tr, CN=Topmargenernes6, OU=Discoplacenta4, O=Pearlings4, L=Tryptone, S=Hydrencephalus4, C=CC
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	• 01/12/2021 11:02:36 01/12/2022 11:02:36
Subject Chain	• E=affaldsproblemernes@Sisi.tr, CN=Topmargenernes6, OU=Discoplacenta4, O=Pearlings4, L=Tryptone, S=Hydrencephalus4, C=CC
Version:	3
Thumbprint MD5:	A09281A46CB4122164B30FB05611CD3F
Thumbprint SHA-1:	75FB258FE049C5BD134BB76066831E5C0A29A387
Thumbprint SHA-256:	8502EA39172E6385A457D26EB0847AE9378028A76658050B270AB02D86DCDB01
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x210b4	0x22000	False	0.360753676471	data	5.21959711886	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x23000	0x122c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x970	0x1000	False	0.174072265625	data	2.04745900646	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
Chinese	Taiwan	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:48:24.089648008 CET	192.168.11.20	1.1.1.1	0xb7e4	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
Dec 2, 2021 19:48:24.099092007 CET	1.1.1.1	192.168.11.20	0xb7e4	No error (0)	drive.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Dec 2, 2021 19:54:03.931977034 CET	1.1.1.1	192.168.11.20	0x5aee	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 20211129.exe PID: 8840 Parent PID: 7092

General

Start time:	19:47:46
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\20211129.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\20211129.exe"
Imagebase:	0x400000
File size:	156816 bytes
MD5 hash:	672587FB175264EF8B45A2B0857F273F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: CasPol.exe PID: 3264 Parent PID: 8840

General

Start time:	19:48:04
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\20211129.exe"
Imagebase:	0x4c0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 3248 Parent PID: 8840

General

Start time:	19:48:05
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\20211129.exe"
Imagebase:	0xa30000
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: 0000000A.00000000.785162355.0000000000E10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 3200 Parent PID: 3248

General

Start time:	19:48:05
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff65f6a0000
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: svchost.exe PID: 3264 Parent PID: 956

General

Start time:	19:54:02

Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
Imagebase:	0x7ff78c080000
File size:	57360 bytes
MD5 hash:	F586835082F632DC8D9404D83BC16316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis

