

JOeSandbox Cloud BASIC



ID: 491364

Sample Name:

Payment_Advice.exe

Cookbook: default.jbs

Time: 14:15:52

Date: 27/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Payment_Advice.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	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
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	8
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Network Port Distribution	9
UDP Packets	9
Code Manipulations	9
Statistics	10
System Behavior	10
Analysis Process: Payment_Advice.exe PID: 4472 Parent PID: 6116	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report Payment_Advice.exe

Overview

General Information

Sample Name:

Payment_Advice.exe

Analysis ID:

491364

MD5:

3a27f66a430a3b5.

SHA1:

4af41cd66669d3c..

SHA256:

dd996392170826..

Tags:

exe

guloader

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

84

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected GuLoader

Initial sample is a PE file and has a ...

Tries to detect virtualization through...

Executable has a suspicious name (...)

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

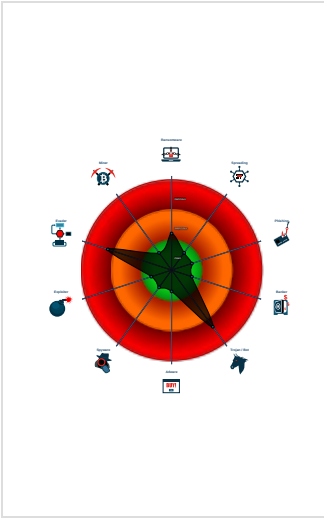
Uses 32bit PE files

Sample file is different than original ...

PE file contains strange resources

Contains functionality to read the PEB

Classification



Process Tree

System is w10x64

Payment_Advice.exe (PID: 4472 cmdline: 'C:\Users\user\Desktop\Payment_Advice.exe' MD5: 3A27F66A430A3B54D24FB8F75E837175)

cleanup

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.816420146.0000000000227 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Initial sample is a PE file and has a suspicious name

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

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

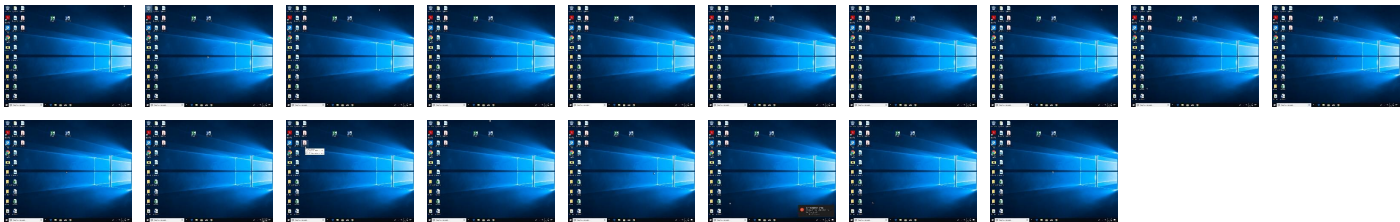
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Time Windows Communication
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	Recovery Time Windows Communication
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	Operational Data Collection
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery Time Windows 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
Payment_Advice.exe	11%	ReversingLabs	Win32.Trojan.Mucc	

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:	33.0.0 White Diamond
Analysis ID:	491364
Start date:	27.09.2021
Start time:	14:15:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_Advice.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:	<ul style="list-style-type: none">• 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:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 17.7% (good quality ratio 10.9%)• Quality average: 36.7%• Quality standard deviation: 33.6%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

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):	5.758289537816364
TrID:	<ul style="list-style-type: none">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:	Payment_Advice.exe
File size:	90112
MD5:	3a27f66a430a3b54d24fb8f75e837175
SHA1:	4af41cd66669d3c2307c1b5af5c198778d174826
SHA256:	dd996392170826c47b9ab378464423e470a1bdfdf7bcd183c61e3e7896d4326
SHA512:	2be02118a3affd640c2b1489816cd396ad3d1af6ab229a3a86bcc20f695445777c1146ffc7488b5bc664d16a6283a3bfa3256758804c2d0851a2bd261c1e1034
SSDEEP:	768:tCbCZDdDSaAhQ41sPuTPfBcrGemB0KxtNavGJluWmqzYlf5sh/YDtOika:twCDDt41hO9mBHp88CmQua
File Content Preview:	MZ.....@.....!.L.!Th is program cannot be run in DOS mode...\$......i.....*.....Rich.....PE..L..0..V..... 0... ..@...@.....

File Icon

	
Icon Hash:	821ca88c8e8c8c00

Static PE Info

General	
Entrypoint:	0x4012c8

General

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:	0x5692D030 [Sun Jan 10 21:42:08 2016 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:	e73b8c032c82c64991ebe487a7ffcd43

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1297c	0x13000	False	0.520379317434	data	6.25517473092	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0xcf4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x550	0x1000	False	0.131591796875	data	1.42355103484	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

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: Payment_Advice.exe PID: 4472 Parent PID: 6116

General

Start time:	14:16:47
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Payment_Advice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	3A27F66A430A3B54D24FB8F75E837175
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.816420146.0000000002270000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis