

JOeSandbox Cloud BASIC



ID: 482656

Sample Name: usd15.030

payment copy & signed invoice

SEPTEMBER 2021

shipment.exe

Cookbook: default.jbs

Time: 00:53:03

Date: 14/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.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	4
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	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
URLs from Memory and Binaries	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
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	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe PID: 4488 Parent PID: 5160	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report usd15.030 payment copy & si...

Overview

General Information

Sample Name:

usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe

Analysis ID:

482656

MD5:

257e1f881863b02.

SHA1:

9cff8e3a2a2cb5a..

SHA256:



856d455d07bff40..

Tags:

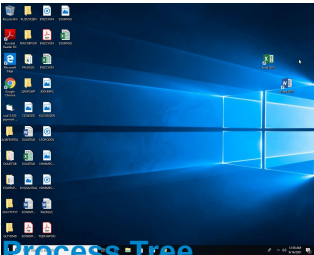
exe

guloader

Infos:

Most interesting Screenshot:



Process Tree

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

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

Signatures

Found malware configuration

Potential malicious icon found

Yara detected GuLoader

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

Executable has a suspicious name (...)

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Machine Learning detection for samp...

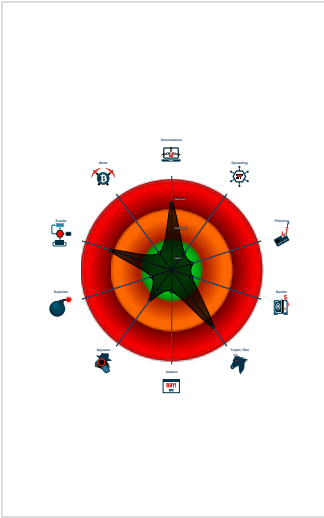
Creates a DirectInput object (often fo...


Uses 32bit PE files

Sample file is different than original ...

PE file contains strange resources

Classification



- System is w10x64
-  usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe (PID: 4488 cmdline: 'C:\Users\user\Desktop\usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe' MD5: 257E1F881863B023FCDDAEDB2AC22E68)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "https://drive.google.com/uc?export=download&id=10snU8Pga"  
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.777526639.000000000221 0000.00000040.00000001.sdump	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

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

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

Anti Debugging:

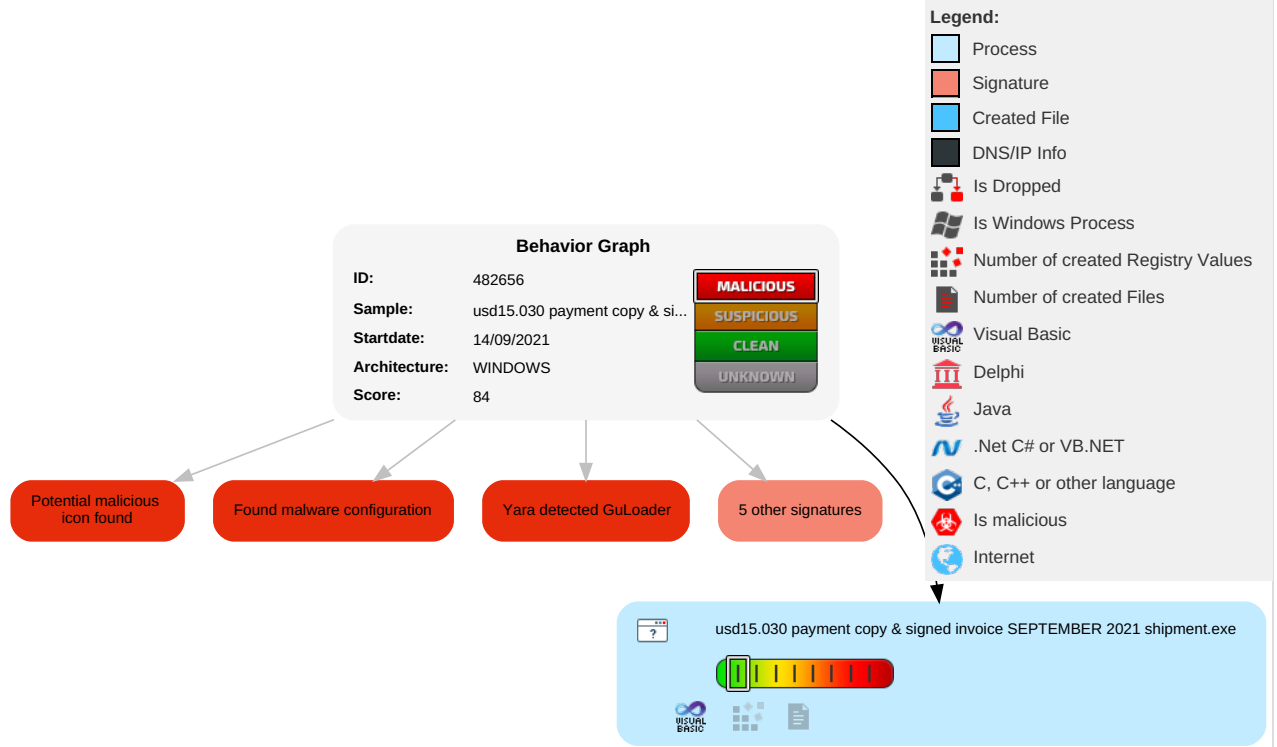


Found potential dummy code loops (likely to delay analysis)

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	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 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	Other
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Backup

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
usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe	10%	ReversingLabs		
usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe	100%	Joe Sandbox ML		

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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482656
Start date:	14.09.2021
Start time:	00:53:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.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:	31
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.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 28.7% (good quality ratio 11.4%)• Quality average: 21.1%• Quality standard deviation: 29.4%
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):	6.872419363708927
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:	usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe
File size:	131072
MD5:	257e1f881863b023fcddaedb2ac22e68
SHA1:	9cff8e3a2a2cb5ad3acba8d4260b2581e0098ac9
SHA256:	856d455d07bff404e39b422f1ad0bbff9397707c86670dbc1134729b44a8c868
SHA512:	a3bdd1a69f697a1fe2f806f2e4cdb821bbbb837fe251151473c2af56b3785ecd4ad0902f099d83063da3f122fdd25cf781299e96c9ea035b6c90e72695166dda
SSDEEP:	3072:qywIsPNymxmFhABX/QzheEmIFVw7qdlmz:qwsY4MABX/QHmEw8Im
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......O.....D.....=.....Rich.....PE..L.....BW..... .P.....t.....@.....

File Icon



Icon Hash: 20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x401574
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:	0x5742A6F8 [Mon May 23 06:45:12 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:	44cde914d1969d7de2a52adae7c22460

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ad84	0x1b000	False	0.591182002315	data	7.12774451895	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1c000	0x1910	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1e000	0x297b	0x3000	False	0.703776041667	data	6.62716963651	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

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: usd15.030 payment copy & signed invoice SEPTEMBER 2021
shipment.exe PID: 4488 Parent PID: 5160

General

Start time:	00:54:04
Start date:	14/09/2021
Path:	C:\Users\user\Desktop\usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\usd15.030 payment copy & signed invoice SEPTEMBER 2021 shipment.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	257E1F881863B023FCDDAEDB2AC22E68
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: 00000001.00000002.777526639.0000000002210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis