

JoeSandbox Cloud BASIC



ID: 435174

Sample Name: OFFER-
8768777765554-PDF.exe

Cookbook: default.jbs

Time: 05:32:24

Date: 16/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report OFFER-8768777765554-PDF.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
Initial Sample	3
Sigma Overview	3
Signature Overview	4
AV Detection:	4
Networking:	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 URLs	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	9
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	10
System Behavior	10
Analysis Process: OFFER-8768777765554-PDF.exe PID: 5804 Parent PID: 5696	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report OFFER-8768777765554-PDF.e...

Overview

General Information

Sample Name:

OFFER-8768777765554-PDF.exe

Analysis ID:

435174

MD5:

dd34ccb897fa3b8..

SHA1:

01f5eebafc304ec..

SHA256:

709cc1b84208f4d..

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

C2 URLs / IPs found in malware con...

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

Tries to detect virtualization through...

Abnormal high CPU Usage

Contains functionality for execution ...

Contains functionality to call native f...

Contains functionality to query CPU ...

Classification

Process Tree

- System is w10x64
- OFFER-8768777765554-PDF.exe (PID: 5804 cmdline: 'C:\Users\user\Desktop\OFFER-8768777765554-PDF.exe' MD5: DD34CCB897FA3B88AF6D3DA17B713B3A)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "https://onedrive.live.com/download?cid=51D628A65732BF05&resid=51D628A65732BF05%21161&authkey=ABg4zwojo0rC4rM, https://onedrive.live.com/download?cid=CC6C941704A208C4&resid=CC6C941704"}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
OFFER-8768777765554-PDF.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

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:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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	Input Capture 1	Security Software Discovery 4 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	Process Injection 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)	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	Other
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Other

Behavior Graph

Thumbnails



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OFFER-8768777765554-PDF.exe	13%	Virustotal		Browse

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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=51D628A65732BF05&resid=51D628A65732BF05%21161&authkey=ABg4zwujoOrC4rM, https://onedrive.live.com/download?cid=CC6C941704A208C4&resid=CC6C941704	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435174
Start date:	16.06.2021
Start time:	05:32:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OFFER-8768777765554-PDF.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:	36
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:	<ul style="list-style-type: none">• Successful, ratio: 100%
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 52.5% (good quality ratio 31.2%)• Quality average: 37.6%• Quality standard deviation: 35.6%
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):	5.8993604994375675
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:	OFFER-8768777765554-PDF.exe
File size:	94208
MD5:	dd34ccb897fa3b88af6d3da17b713b3a
SHA1:	01f5eebafc304ec00e25c2c52751cc24d05dd8c9
SHA256:	709cc1b84208f4dd7f541a50772c7888f704561866eccd4b1aee0e1ba6e3ac74
SHA512:	a27103e8c475bfe2edbbc1d6de7b9526fc2eca1b0ac2f029c784088fc635892d3fe5c402fe8c55971face6309bd17b8f326c1b384a940803fd4ea1eede4b9f29
SSDEEP:	1536:0VktxQ6lleR1nwjoWlc7hyCTyStNCEXHa3y2C/u5W3EUanOYA2nJ29GLwb7zN9gm:0OXQqIG1w0WqwCTySPNu5W3EUanOYA2a
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......c.S..... ...&.....\$......Rich.....PE.L.....:H..... ...@...0.....D.....P...@.....

File Icon

	
Icon Hash:	11c0c48486cc08c4

Static PE Info

General

Entrypoint:	0x401644
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:	0x48913AA8 [Thu Jul 31 04:08:08 2008 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:	d5d16d1b76210dd28c8586fe9bac3119

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x131c8	0x14000	False	0.495971679688	data	6.27184152045	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x1b84	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0xd86	0x1000	False	0.346435546875	data	3.582300179	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: OFFER-8768777765554-PDF.exe PID: 5804 Parent PID: 5696

General

Start time:	05:33:09
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\OFFER-8768777765554-PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OFFER-8768777765554-PDF.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	DD34CCB897FA3B88AF6D3DA17B713B3A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis