

JoeSandbox Cloud BASIC



ID: 483639

Sample Name: Halkbank02.exe

Cookbook: default.jbs

Time: 10:37:01

Date: 15/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Halkbank02.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
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
Code Manipulations	9
Statistics	10
System Behavior	10
Analysis Process: Halkbank02.exe PID: 6396 Parent PID: 3232	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report Halkbank02.exe

Overview

General Information

Sample Name:

Halkbank02.exe

Analysis ID:

483639

MD5:

a4cb6740c9195c...

SHA1:

54abe0f828d828d.

SHA256:

f1b1abf0182c865..

Tags:

exe



geo

GuLoader

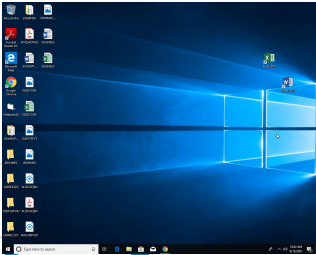
Halkbank

TUR


Infos:



Most interesting Screenshot:



Process Tree

- System is w10x64
-  [Halkbank02.exe](#) (PID: 6396 cmdline: 'C:\Users\user\Desktop\Halkbank02.exe' MD5: A4CB6740C9195C5579ACEF4F7C8E40C7)
- cleanup

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

88

Range:

0 - 100

Whitelisted:

false

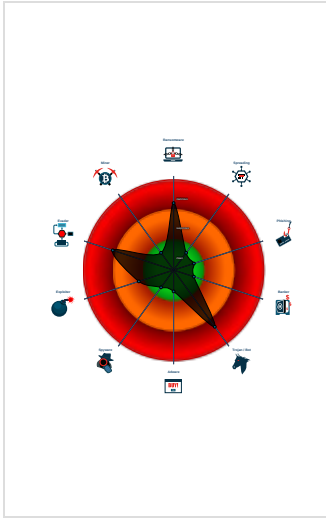
Confidence:

100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Yara detected GuLoader
- C2 URLs / IPs found in malware con...
- Found potential dummy code loops (...)
- Uses 32bit PE files
- Found inlined nop instructions (likely...
- Yara signature match
- Sample file is different than original ...
- PE file contains strange resources

Classification



Malware Configuration

Threatname: GuLoader

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

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.775767651.0000000002BD0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.772950247.0000000000410000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	<ul style="list-style-type: none">0x450:\$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000001.00000000.247791172.0000000000410000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	<ul style="list-style-type: none">0x450:\$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

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

System Summary:



Potential malicious icon found

Malicious sample detected (through community Yara rule)

Data Obfuscation:



Yara detected GuLoader

Anti Debugging:

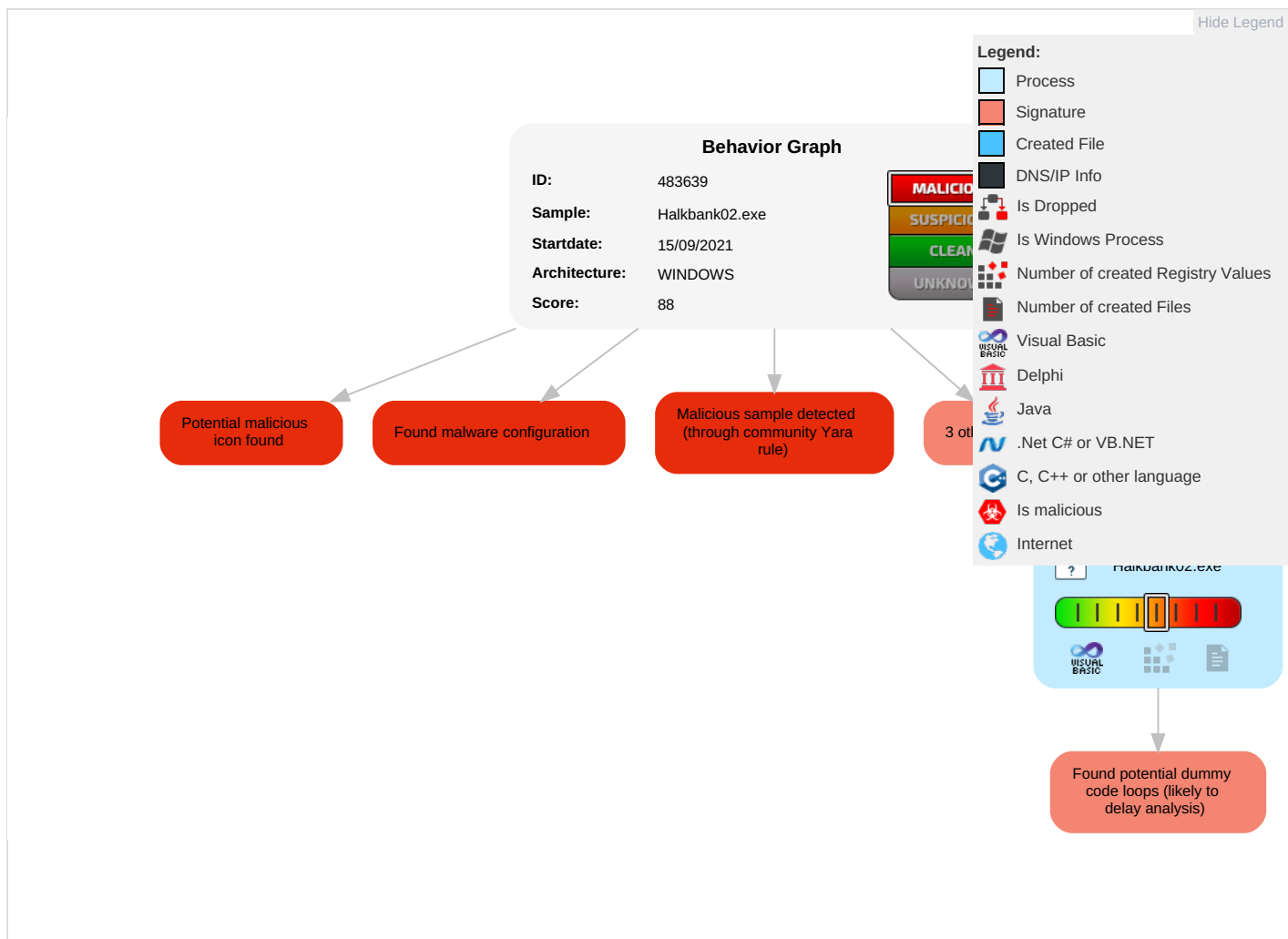


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Reputation
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	Reputation
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Reputation
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Reputation

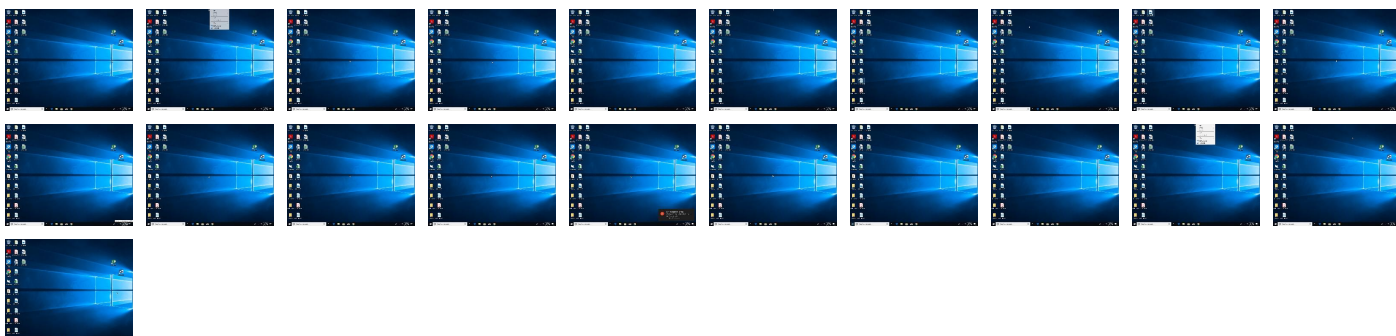
Behavior Graph



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
Halkbank02.exe	16%	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:	483639
Start date:	15.09.2021
Start time:	10:37:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Halkbank02.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:	30
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:	mal88.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 5.7% (good quality ratio 3%)• Quality average: 27.7%• Quality standard deviation: 26.8%
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):	5.903422169790693
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:	Halkbank02.exe
File size:	114688
MD5:	a4cb6740c9195c5579acef4f7c8e40c7
SHA1:	54abe0f828d828d5ff840b989fb5f010395961f6
SHA256:	f1b1abf0182c865a3521d659cbc4bd86a4b00b0e4be95468a1d3b5ff46a3efc8
SHA512:	454837e72cab7fb74b1997a9cb65f00f4f61f2c20df207af2bc68bb14b64b05bc335b7a5ee453872f39b0e4d2608d1c430355411784e810c631c2a48913e3de8
SSDEEP:	1536:eCTH2yl2XReXuS7oM7AS9GvCxrJodHrRdgGpVBPy6mgjd+:e62dAwSsO9GvCxrJ6HbrVBPY6jU
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......u...1..1. ..1.....0...~...0.....0..Rich1.....PE..L...{ewV..... ...`...P.....p....@.....B..

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401500
-------------	----------

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:	0x5677657B [Mon Dec 21 02:35:39 2015 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:	4907098a5ecd4cf1549046838d3d7c44

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x15dc4	0x16000	False	0.537486683239	data	6.51159061582	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0xa34	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x31be	0x4000	False	0.143920898438	data	2.81606437364	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	
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Halkbank02.exe PID: 6396 Parent PID: 3232

General

Start time:	10:38:01
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Halkbank02.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Halkbank02.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	A4CB6740C9195C5579ACEF4F7C8E40C7
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: 00000001.00000002.775767651.0000000002BD0000.00000040.00000001.sdmp, Author: Joe Security• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000001.00000002.772950247.0000000000410000.00000020.00020000.sdmp, Author: Florian Roth• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000001.00000000.247791172.0000000000410000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis