ID: 450884
Sample Name: F63V4i8eZU
Cookbook: default.jbs
Time: 20:11:12
Date: 19/07/2021
Version: 33.0.0 White Diamond

Table of Contents

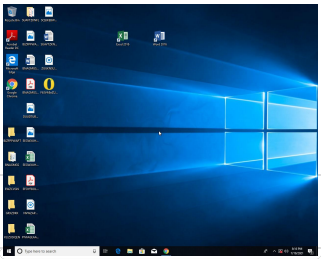
Windows Analysis Report F63V4i8eZU

Overview

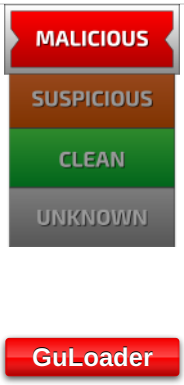
General Information

Sample Name:	F63V4i8eZU (renamed file extension from none to exe)
Analysis ID:	450884
MD5:	08730cdd286a4c..
SHA1:	001bb7b5b8d63e..
SHA256:	cb2a2537987e45..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection

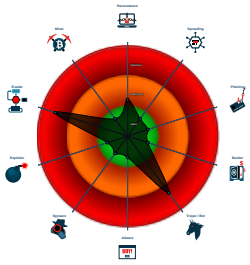


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 (…
- Potentially malicious time measurem…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…

Classification



Process Tree

- **System is w10x64**
- F63V4i8eZU.exe (PID: 3528 cmdline: 'C:\Users\user\Desktop\F63V4i8eZU.exe' MD5: 08730CDD286A4C9D46B38BB6545AC311)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://kinmirai.org/wp-content/bin_QVwo"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.737783934.00000000021D0000.00000040.00000001.sdmp	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

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:

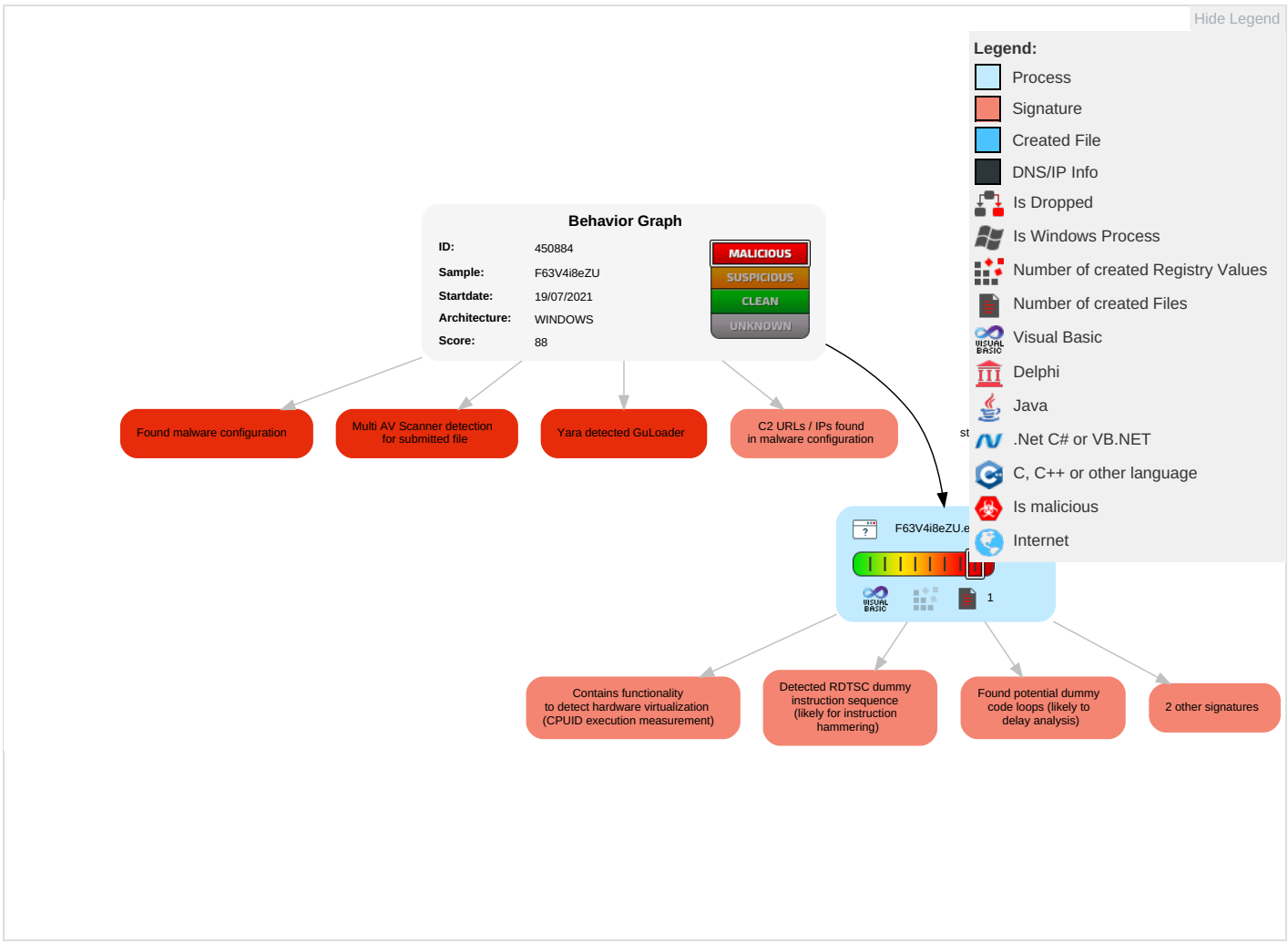
Found potential dummy code loops (likely to delay analysis)

Potentially malicious time measurement code found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R Se El
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R Tr W Au
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	R W W Au
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	O D Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

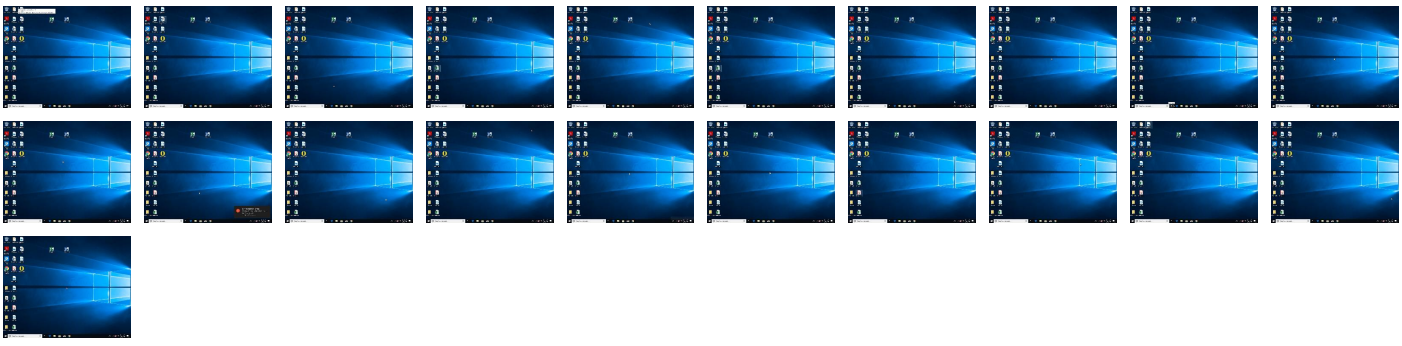
Behavior Graph



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
F63V4i8eZU.exe	10%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://kinmirai.org/wp-content/bin_QVwo	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://kinmirai.org/wp-content/bin_QVwo	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450884
Start date:	19.07.2021
Start time:	20:11:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	F63V4i8eZU (renamed file extension from none to 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:	34
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:	mal88.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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):	4.804431914533398
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:	F63V4i8eZU.exe
File size:	271464
MD5:	08730cdd286a4c9d46b38bb6545ac311
SHA1:	001bb7b5b8d63e505661d7e4a178d08abe6bbad7
SHA256:	cb2a2537987e45c8461d40a0ec6c24215920519257134db91dd1369ff5abf342
SHA512:	a6531eb4709af3e1270f1c4434d9abc87097e9f8d38c4ba5dc0ed61d7f469552de7259f638728fe71297d3748823064f75728e71df3531657a5aeb1952f412d8
SSDEEP:	1536:d/k1xdvMuWnLtmBcSa9O/C0UzIY+SpAkaYQryC7AfT/k1xD:5ktvMu8GcSaw/RQ80fDkz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L....fl.....`.....<.....p....@.....

File Icon

Icon Hash:	e8ccce8e8ececce8

Static PE Info

General

Entrypoint:	0x40133c
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:	0x49669CB5 [Fri Jan 9 00:39:17 2009 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:	ce5c4ac311690d884b7f964e897cf716

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=MIDLE@perkysex.Sta, CN=Tykho, OU=LRDAGSD, O=Oedogo, L=gener, S=Succuss7, C=FO
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	• 7/19/2021 1:52:32 AM 7/19/2022 1:52:32 AM
Subject Chain	• E=MIDLE@perkysex.Sta, CN=Tykho, OU=LRDAGSD, O=Oedogo, L=gener, S=Succuss7, C=FO
Version:	3
Thumbprint MD5:	6B2F2AEC1CD19ADB58F69D332AA6EB10
Thumbprint SHA-1:	A168A0624017FAD1687EFD7218165EAAD0667521
Thumbprint SHA-256:	7B29D7974E330B45B5772C1F20898DB73558EAF4668727D08A94229F6C2C5A9A
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x35908	0x36000	False	0.261126482928	data	4.74357269576	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x37000	0xb90	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x80e2	0x9000	False	0.31982421875	data	4.39996163411	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: F63V4i8eZU.exe PID: 3528 Parent PID: 5628

General

Start time:	20:12:04
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\F63V4i8eZU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\F63V4i8eZU.exe'
Imagebase:	0x400000
File size:	271464 bytes
MD5 hash:	08730CDD286A4C9D46B38BB6545AC311
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.737783934.00000000021D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis