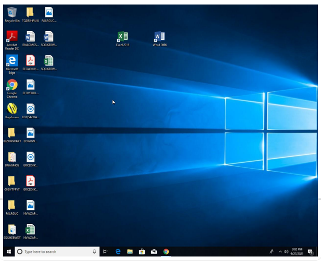
ID: 491405
Sample Name: Kapitu.exe
Cookbook: default.jbs
Time: 14:57:50
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report Kapitu.exe

Overview

General Information

Sample Name:	Kapitu.exe
Analysis ID:	491405
MD5:	149b6bd6b0d3dd..
SHA1:	33cdaa42e1a5c1..
SHA256:	b622dbe8021483..
Tags:	exe guloader
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

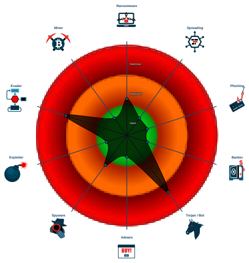
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- PE file contains strange resources
- Contains functionality to read the PEB
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- Kapitu.exe (PID: 6004 cmdline: 'C:\Users\user\Desktop\Kapitu.exe' MD5: 149B6BD6B0D3DD2B0FBB111632D59FCC)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.824313775.000000000215 0000.00000040.00000001.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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

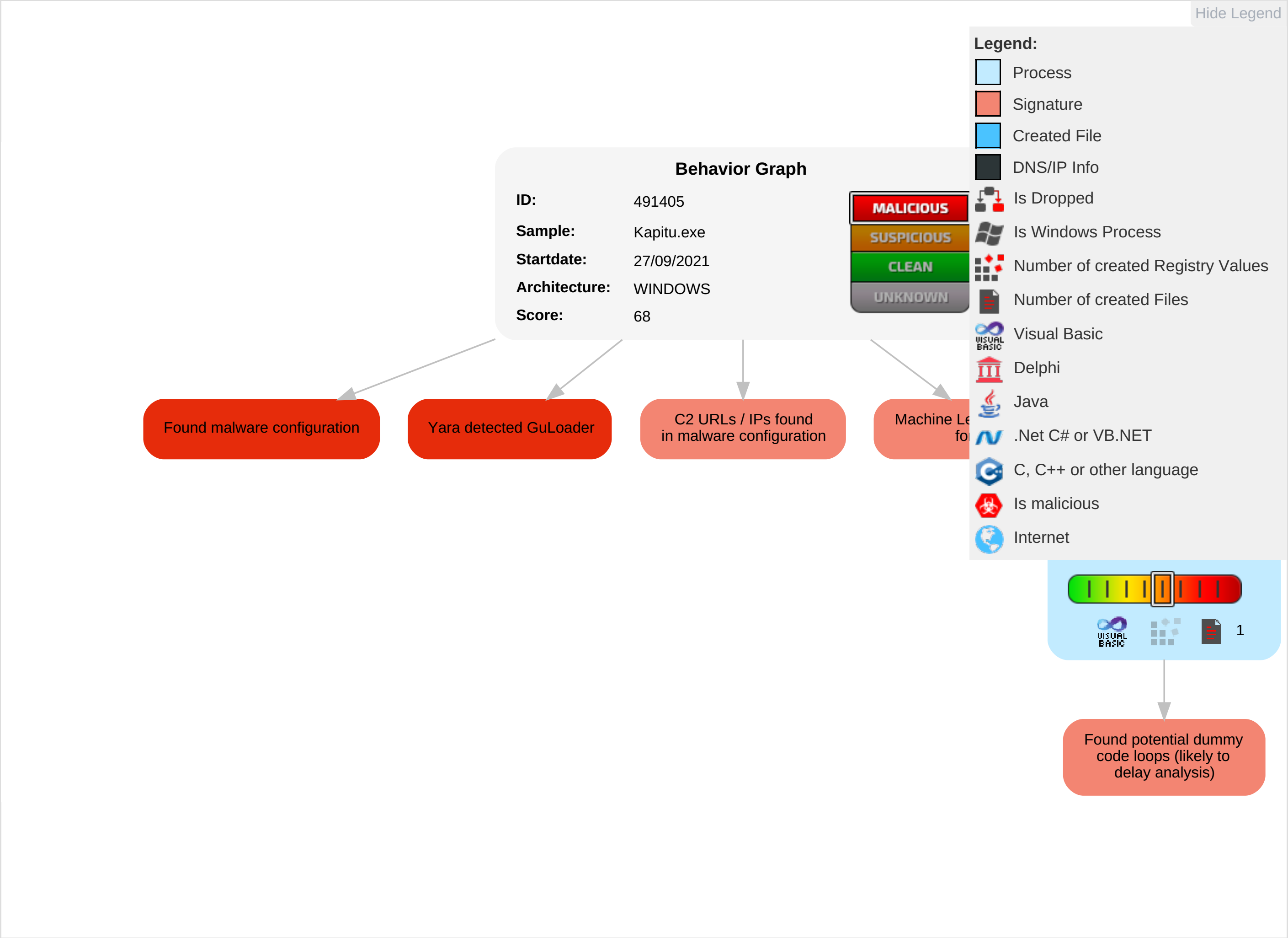
Anti Debugging:

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re 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	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re 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	Ol De Cl Ba
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	

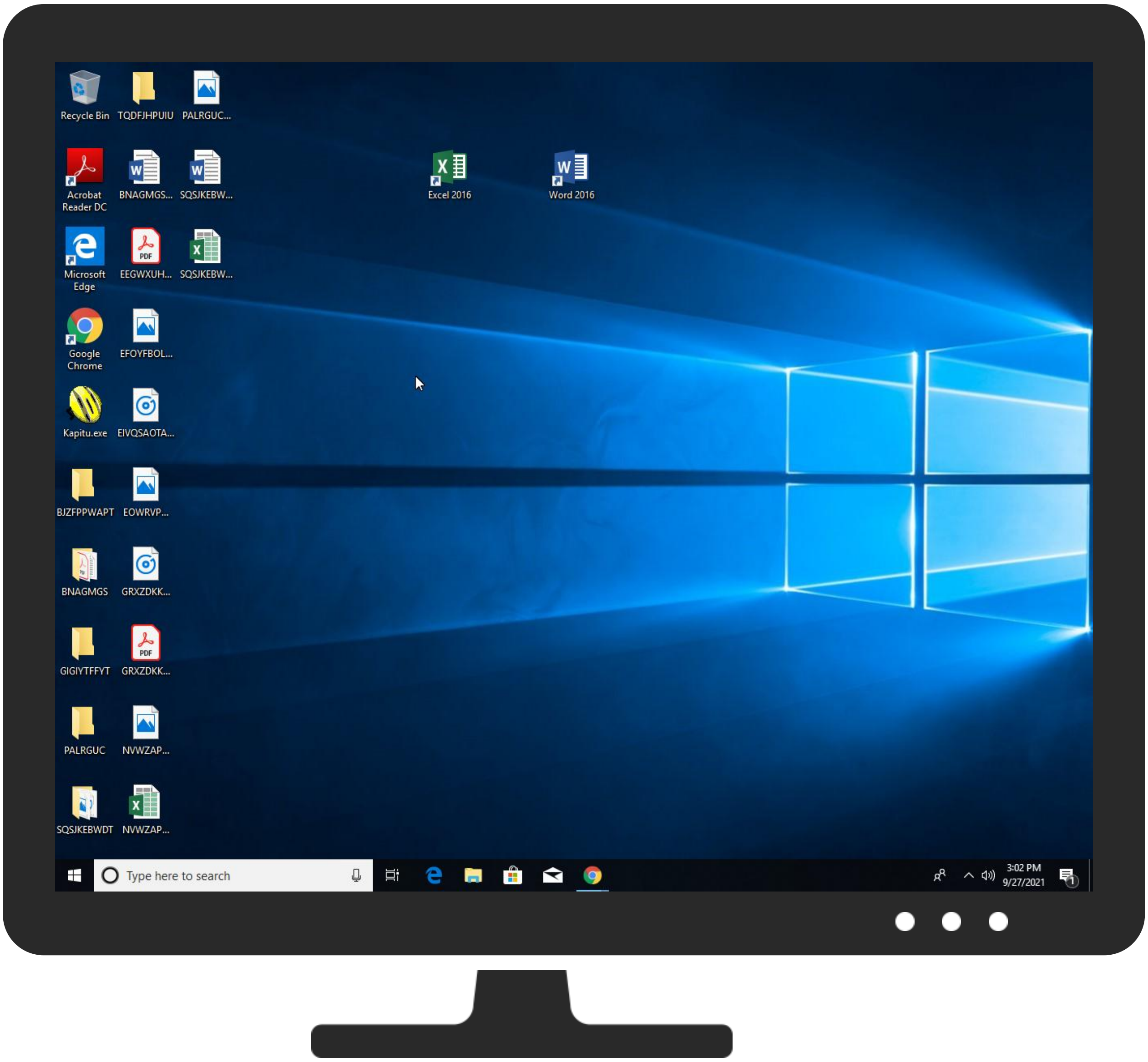
Behavior Graph



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
Kapitu.exe	9%	ReversingLabs	Win32.Trojan.Mucc	
Kapitu.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491405
Start date:	27.09.2021
Start time:	14:57:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Kapitu.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:	17
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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 21.4%) • Quality average: 36.6% • Quality standard deviation: 32%
HCA Information:	Failed
Cookbook Comments:	• 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

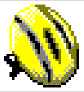
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.2510687218535645
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:	Kapitu.exe
File size:	102400
MD5:	149b6bd6b0d3dd2b0fbb111632d59fcc
SHA1:	33cdaa42e1a5c1fad1aa4f38dd9ad6ea75113aa7
SHA256:	b622dbe802148305104ef456835748d2fc0d8edeffa64787c43c78bcb1914b2f
SHA512:	d2783ef1112d892b9501cf0e8ce6e74277d0d55d0eb9cd3841802381682bc1e7631389c24a2f6f297a82f406fdb6c942ae7987df96f227d00e73ebbc6d01c51f
SSDEEP:	1536:RMigxMWRwt1aaGhFNEAAF9vq/eVlQ4F5kOrpdh/:aicCQhFWfFqWlQa19d1
File Content Preview:	MZ....................@..!..L.!This program cannot be run in DOS mode....$.......u...1...1...1.......0...~...0.......0...Rich1...........PE..L......G................P...0..............`....@................

File Icon



Icon Hash:	78f8d6d4ac88d0e2

Static PE Info

General

Entrypoint:	0x4012d4

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:	0x47939ED5 [Sun Jan 20 19:19:49 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:	1eb0aaa4f15bbd841e91215ce68e26d2

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14548	0x15000	False	0.564581008185	data	6.64813091297	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x9f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1cb8	0x2000	False	0.264526367188	data	3.48286092723	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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: Kapitu.exe PID: 6004 Parent PID: 5272

General

Start time:	14:58:52
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Kapitu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Kapitu.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	149B6BD6B0D3DD2B0FBB111632D59FCC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.824313775.0000000002150000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond