



ID: 452531
Sample Name:
MWSW9nxmUK.exe
Cookbook: default.jbs
Time: 15:01:15
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report MWSW9nxmUK.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 3
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
Authenticode Signature 9
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 9
Imports 9
Version Infos 9
Possible Origin 9
Network Behavior 10
Code Manipulations 10
Statistics 10
System Behavior 10
Analysis Process: MWSW9nxmUK.exe PID: 1844 Parent PID: 5732 10
General 10
File Activities 10
Disassembly 10
Code Analysis 10

Copyright Joe Security LLC 2021

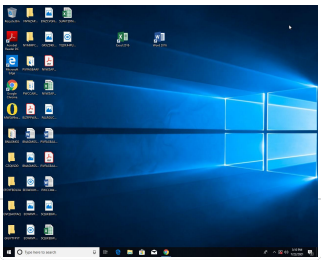
Windows Analysis Report MWSW9nxmUK.exe

Overview

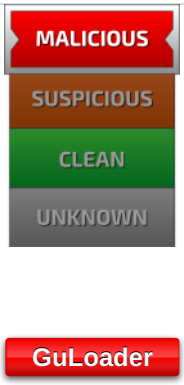
General Information

Sample Name:	MWSW9nxmUK.exe
Analysis ID:	452531
MD5:	c937fc9ed4325e6..
SHA1:	00439295920e78..
SHA256:	d54cafc1ca36d0d..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



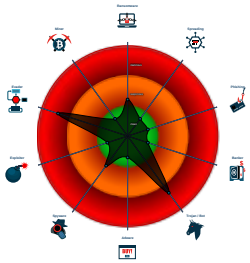
GuLoader

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**
- MWSW9nxmUK.exe (PID: 1844 cmdline: 'C:\Users\user\Desktop\MWSW9nxmUK.exe' MD5: C937FC9ED4325E6AB24D49A3175F3A5C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://kinmirai.org/wp-content/bin_inUIdCgQk163.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1292263867.0000000002F70000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

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:

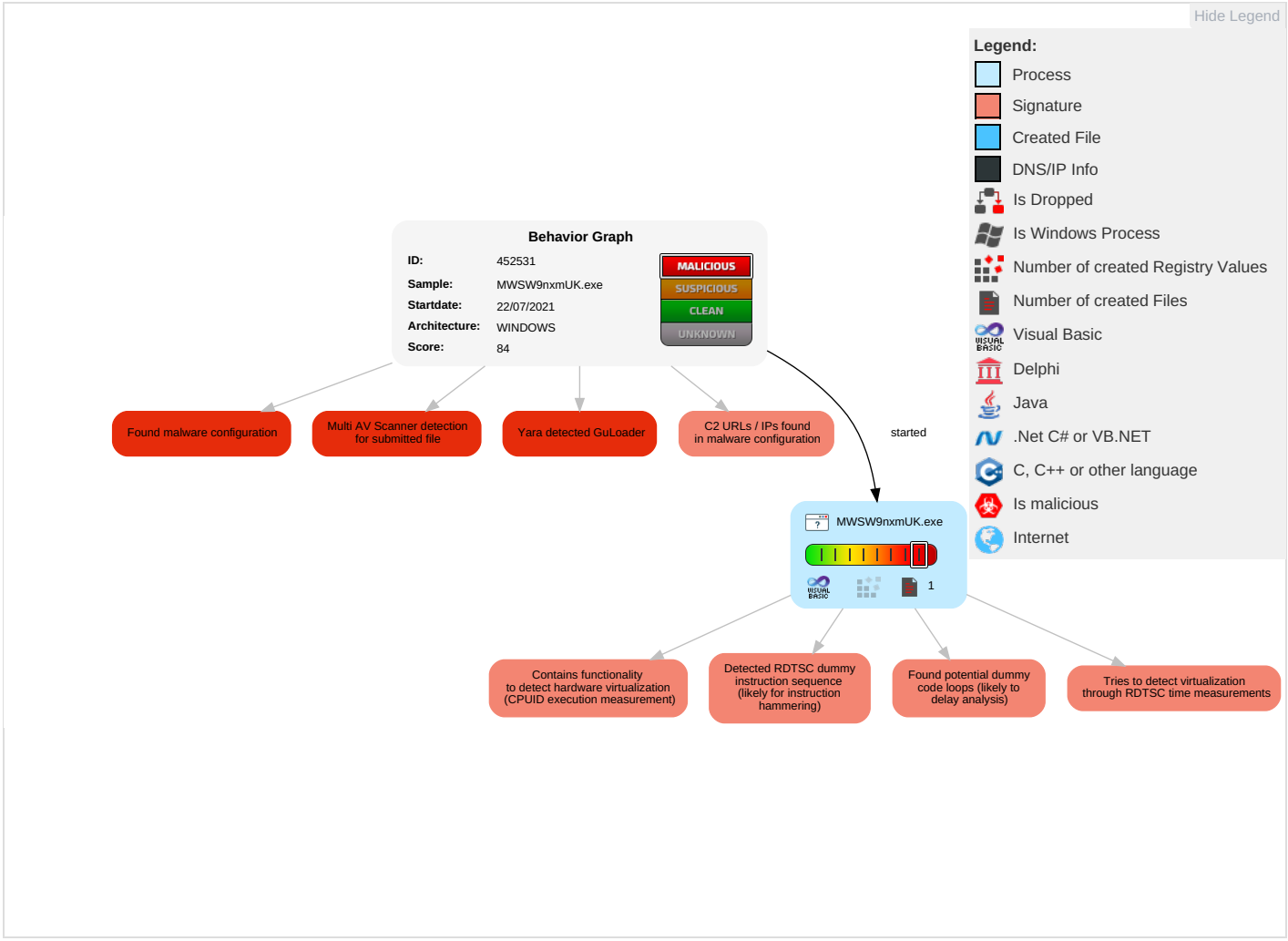


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
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 T W A
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 A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	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 C B
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	

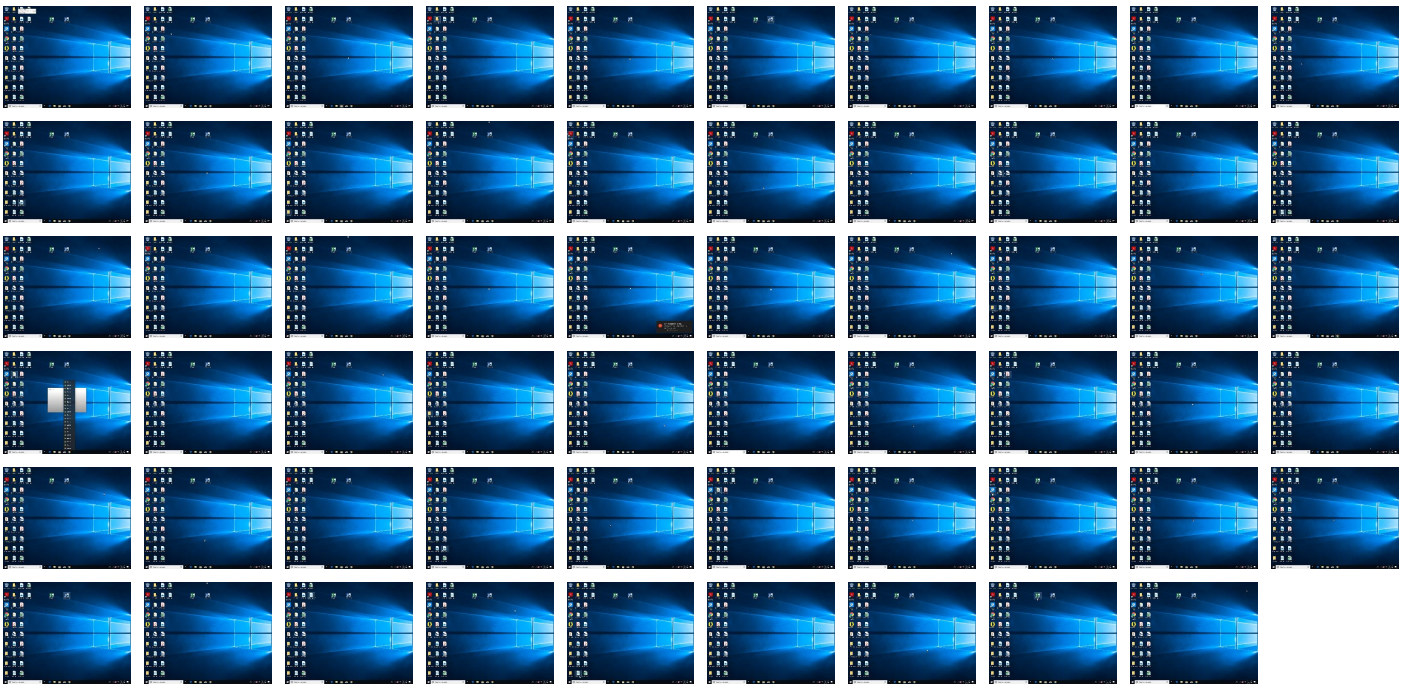
Behavior Graph



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
MWSW9nxmUK.exe	44%	Virustotal		Browse
MWSW9nxmUK.exe	43%	ReversingLabs	Win32.Trojan.Vebzenpak	

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_inUIdCgQk163.bin	0%	Virustotal		Browse
http://https://kinmirai.org/wp-content/bin_inUIdCgQk163.bin	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://kinmirai.org/wp-content/bin_inUIdCgQk163.bin	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452531
Start date:	22.07.2021
Start time:	15:01:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MWSW9nxmUK.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	41
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:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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):	4.648392883751036
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:	MWSW9nxmUK.exe
File size:	246888
MD5:	c937fc9ed4325e6ab24d49a3175f3a5c
SHA1:	00439295920e78ecac31d1dbf7eb67118d76299a
SHA256:	d54cafc1ca36d0ddd134f53d033ebbaaa490721d62d4168106a9b6c7cfa200ba
SHA512:	ff13a5d3bfd503e0f11c9d974a4ac88f965eec14cbf07723ac9ed425222aaa7c5871a6438cd7491fbd694424ebe4c8675dc076e81564204583336a2940e9a9d0
SSDEEP:	1536:HrnnnnnnnnnnnnnnrKDnnnnnnnnnnnnnnnCnnnnrnnnnnnnnnXnnnnnnnnnnnnE:H6LVbA8nT1vnv9dnj6czcW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L.....\S.....0...p.....0.....@....@.....

File Icon



Icon Hash:	e8ccce8e8ececce8

Static PE Info

General

Entrypoint:	0x401330
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:	0x535CB682 [Sun Apr 27 07:49:22 2014 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:	4e1e57f6de47f654992269152dd1e659

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Matri7@conn.Gru, CN=Characte2, OU=presolvep, O=Neapol8, L=styk, S=Laur, C=LC
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	• 7/21/2021 3:37:16 PM 7/21/2022 3:37:16 PM
Subject Chain	• E=Matri7@conn.Gru, CN=Characte2, OU=presolvep, O=Neapol8, L=styk, S=Laur, C=LC
Version:	3
Thumbprint MD5:	79CF1ECF512D0016E6565DBDBB4BA3BB
Thumbprint SHA-1:	E4666F2B8BC7DC083B23415376F21E8E4C2CEB0D
Thumbprint SHA-256:	89E6F5909EC358780F7165075AE7073138BA8B7BE49CFEB5B401AF72BDC5E42B
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x324c0	0x33000	False	0.249516505821	data	4.59513440104	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x34000	0xb90	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x54c4	0x6000	False	0.293294270833	data	4.11736046499	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

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: MWSW9nxmUK.exe PID: 1844 Parent PID: 5732

General

Start time:	15:02:04
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\MWSW9nxmUK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MWSW9nxmUK.exe'
Imagebase:	0x400000
File size:	246888 bytes
MD5 hash:	C937FC9ED4325E6AB24D49A3175F3A5C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1292263867.0000000002F70000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021