

JOeSandbox Cloud BASIC



**ID:** 457852

**Sample Name:**

97bXaukEWI.exe

**Cookbook:** default.jbs

**Time:** 11:51:41

**Date:** 02/08/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report 97bXaukEWI.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: 97bXaukEWI.exe PID: 4908 Parent PID: 5516	10
General	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report 97bXaukEWl.exe

## Overview

### General Information

Sample Name:

97bXaukEWl.exe

Analysis ID:

457852

MD5:

9318cd06a9a0b7..

SHA1:

a296ea3e1cf6d41.

SHA256:




7ad18b09938d40..

Tags:

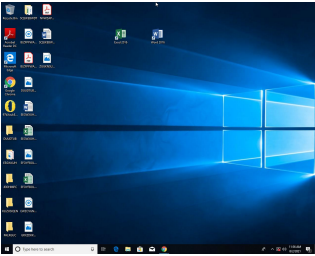
exe

GuLoader

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...

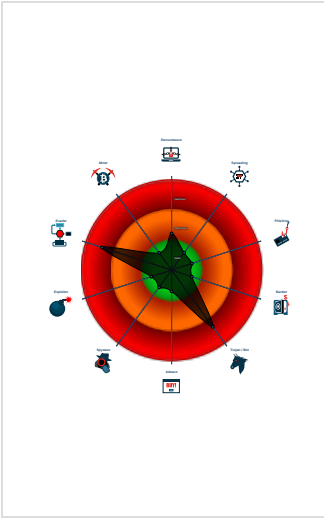
Abnormal high CPU Usage

Contains functionality for execution ...

Contains functionality to call native f...


Contains functionality to read the PEB

### Classification



## Process Tree

System is w10x64

 97bXaukEWl.exe (PID: 4908 cmdline: 'C:\Users\user\Desktop\97bXaukEWl.exe' MD5: 9318CD06A9A0B788DC043A63C97D4FCE)

cleanup

## Malware Configuration

Threatname: GuLoader

{

"Payload URL": "https://kinmirai.org/wp-content/bin\_NIapfDNXM183.bin"

}

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.747139743.00000000020A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

## 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:

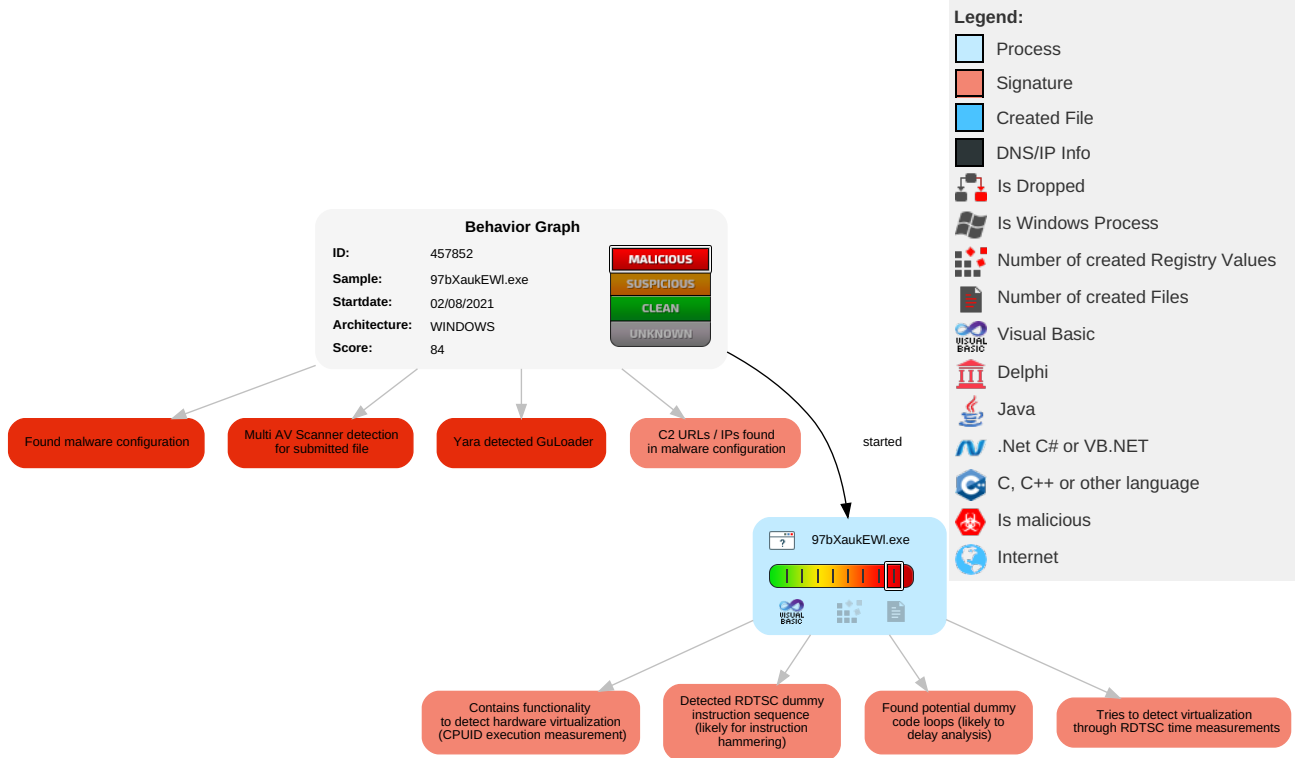


Found potential dummy code loops (likely to delay analysis)

## 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	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	Recovery Time Windows Analysis
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	Recovery Time Windows Analysis
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 Data Collection
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	

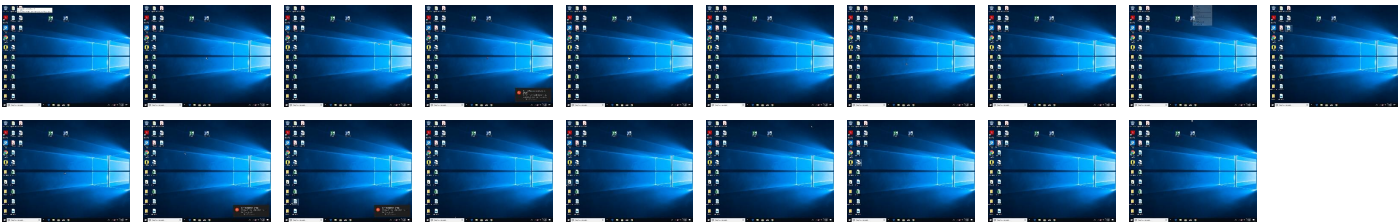
## Behavior Graph



## 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
97bXaukEWI.exe	24%	Virustotal		<a href="#">Browse</a>
97bXaukEWI.exe	17%	ReversingLabs	Win32.InfoStealer.Generic	

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://https://kinmirai.org/wp-content/bin_NlapfDNXM183.bin">http://https://kinmirai.org/wp-content/bin_NlapfDNXM183.bin</a>	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_NlapfDNXM183.bin	true	<ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul>	unknown

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457852
Start date:	02.08.2021
Start time:	11:51:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	97bXaukEWI.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:	39
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"><li>HCA enabled</li><li>EGA enabled</li><li>HDC enabled</li><li>AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 0.4% (good quality ratio 0.4%)</li><li>Quality average: 55.3%</li><li>Quality standard deviation: 9.3%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</li><li>Found application associated with file extension: .exe</li><li>Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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):	4.6012516392465255
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	97bXaukEWI.exe
File size:	259192
MD5:	9318cd06a9a0b788dc043a63c97d4fce
SHA1:	a296ea3e1cf6d41f9d059d7d6e5058882b03161a
SHA256:	7ad18b09938d40e8ec342ee6bee6b190a986ffedce7567a638b8d25b4098cb69
SHA512:	da057bf10d5a7ae8863dd0310b3d4116af6535aacc68074c9c301e79f580860c2cecba991628d274d62e029ee210f92705c12125dc390072556ca031a16cd4b3
SSDEEP:	1536:2blgLWMXncWYqmOeDA6W6h8eaBWTvYeigJ2cI6wt:NLWMXntzVAA6W6GwZJgt
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......y..... .....Rich.....PE..L.....zY.....@.... .....P...@.....

File Icon





Icon Hash:	e8cccece8eccc68
------------	-----------------

## Static PE Info

### General

Entrypoint:	0x401388
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:	0x597AB081 [Fri Jul 28 03:33:21 2017 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:	c75b2cceb55bee276cddf57134b154d2

### Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Andreyg5@anaerobi.Pr, CN=ANSTNDI, OU=COLOROTO, O=krem, L=Token, S=Skuffels5, C=PG
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	<ul style="list-style-type: none"><li>8/1/2021 1:24:20 PM 8/1/2022 1:24:20 PM</li></ul>
Subject Chain	<ul style="list-style-type: none"><li>E=Andreyg5@anaerobi.Pr, CN=ANSTNDI, OU=COLOROTO, O=krem, L=Token, S=Skuffels5, C=PG</li></ul>
Version:	3
Thumbprint MD5:	5F240938C81B57F5F43DD818766923DB
Thumbprint SHA-1:	D39BA4A993AF1C3AF864520F7A5E572CFBAF3C4A
Thumbprint SHA-256:	98F39CD1A5C825C14DA71726F851E1712E5FD89B52C590FC4D1763D249A25976
Serial:	00

### Entrypoint Preview

### Data Directories

### Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x33a64	0x34000	False	0.258328951322	data	4.55415043374	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x35000	0xb94	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x36000	0x70f2	0x8000	False	0.2998046875	data	4.01130957517	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: 97bXaukEWI.exe PID: 4908 Parent PID: 5516

### General

Start time:	11:52:38
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\97bXaukEWI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\97bXaukEWI.exe'
Imagebase:	0x400000
File size:	259192 bytes
MD5 hash:	9318CD06A9A0B788DC043A63C97D4FCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.747139743.00000000020A0000.00000040.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	low

## Disassembly

### Code Analysis