

JOeSandbox Cloud BASIC



**ID:** 451828

**Sample Name:**

SecuriteInfo.com.Variant.Graftor.981190.24096.12674

**Cookbook:** default.jbs

**Time:** 12:02:10

**Date:** 21/07/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Variant.Graftor.981190.24096.12674	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Initial Sample	3
Memory Dumps	3
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
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: SecuriteInfo.com.Variant.Graftor.981190.24096.exe PID: 5092 Parent PID: 5732	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report SecuriteInfo.com.Variant.Graf...

## Overview

### General Information

Sample Name:

SecuriteInfo.com.Variant.Grafter.981190.24096.12674 (renamed file extension from 12674 to exe)

Analysis ID:

451828

MD5:

19cac1ee3a6e5e...

SHA1:

5b7f16098760f88..

SHA256:


3709110cc04e0e..

Tags:

exe

Infos:

Most interesting Screenshot:



### Process Tree

### 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

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Contains functionality to detect hard...

Found potential dummy code loops (...)

Abnormal high CPU Usage

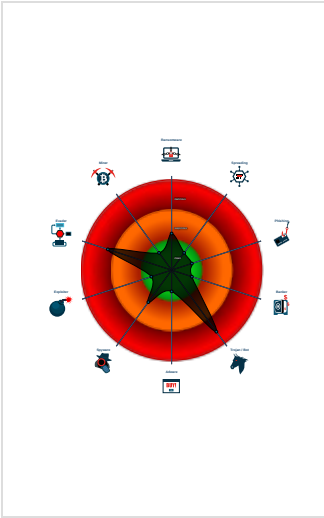
Contains functionality for execution ...

Contains functionality to call native f...

Contains functionality to query CPU ...

Contains functionality to read the PEB

### Classification



- System is w10x64
- SecuriteInfo.com.Variant.Grafter.981190.24096.exe (PID: 5092 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Grafter.981190.24096.exe' MD5: 19CAC1EE3A6E5E9F83054616F5D5CE6F)
- cleanup

## Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "https://kinmirai.org/wp-content/bin_l0ulvHP91.bip"  
}
```

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Variant.Grafter.981190.24096.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.325526342.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000002.00000002.850474872.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000002.00000002.852029233.0000000002A9 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.SecuriteInfo.com.Variant.Graftor.981190.24096.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
2.0.SecuriteInfo.com.Variant.Graftor.981190.24096.exe.400000.0.unpack	JoeSecurity_GuLoader_1	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

Yara detected GuLoader

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

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	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
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	Recovery
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





# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Graftor.981190.24096.exe	15%	Virustotal		<a href="#">Browse</a>
SecuriteInfo.com.Variant.Graftor.981190.24096.exe	20%	ReversingLabs	Win32.Trojan.Graftor	

## 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_I0ulvHP91.bip	0%	Virustotal		<a href="#">Browse</a>
http://https://kinmirai.org/wp-content/bin_I0ulvHP91.bip	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
<a href="http://https://kinmirai.org/wp-content/bin_IOulvHP91.bip">http://https://kinmirai.org/wp-content/bin_IOulvHP91.bip</a>	true	<ul style="list-style-type: none"><li>0%, Virustotal, <a href="#">Browse</a></li><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:	451828
Start date:	21.07.2021
Start time:	12:02:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Graftor.981190.24096.12674 (renamed file extension from 12674 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:	21
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:	Failed
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</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):	4.635501230509535
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:	SecuriteInfo.com.Variant.Graftor.981190.24096.exe
File size:	246888
MD5:	19cac1ee3a6e5e9f83054616f5d5ce6f
SHA1:	5b7f16098760f887b0bdc5fee9223d022e0597fb
SHA256:	3709110cc04e0eaffe10bec5e8a5c82b858bee4195975e7bcd30c50b246f56c3
SHA512:	75d7cc20b44224ab616b9d4e6edd2c527c4245f5752430a08ed7a68a3d1596bfe5f9a16a447a57e8cbb965b7377c6259f481c6a1ae8d262238ad25dce14a0ad
SSDEEP:	3072:MitU2Qf98DH332/jEvQuUZZNzPmhd3QPBP:KU2Qf9iXm/jduUNzPKNC
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......y..... .....Rich.....PE..L....QU.....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:	0x5551E11C [Tue May 12 11:16:44 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:	4e1e57f6de47f654992269152dd1e659

### Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Lertj1@impifo.Tw, CN=Konc, OU=HVEPSERED, O=Sulfur2, L=Delings, S=tyskla, C=IS
Signature Validation Error:	<b>A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider</b>
Error Number:	-2146762487
Not Before, Not After	<ul style="list-style-type: none"><li>7/20/2021 2:04:04 PM 7/20/2022 2:04:04 PM</li></ul>
Subject Chain	<ul style="list-style-type: none"><li>E=Lertj1@impifo.Tw, CN=Konc, OU=HVEPSERED, O=Sulfur2, L=Delings, S=tyskla, C=IS</li></ul>
Version:	3
Thumbprint MD5:	E001EFB7FC2CF4F9AF90A05F56C0FF24
Thumbprint SHA-1:	FCE4066FC44A76DB5BD40EDCD674457947994F61
Thumbprint SHA-256:	30E21C2F0117B69F54088BA86D9ACD07DCB63504497576DBD473335F67BB6F5D
Serial:	00

### Entrypoint Preview

### Data Directories

### Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x324a0	0x33000	False	0.249899471507	data	4.58227124451	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	0x54b4	0x6000	False	0.293172200521	data	4.10742387863	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: SecuriteInfo.com.Variant.Graftor.981190.24096.exe PID: 5092**

**Parent PID: 5732**

### General

Start time:	12:03:02
Start date:	21/07/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Graftor.981190.24096.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Graftor.981190.24096.exe'
Imagebase:	0x400000
File size:	246888 bytes
MD5 hash:	19CAC1EE3A6E5E9F83054616F5D5CE6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000002.00000000.325526342.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li> <li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000002.00000002.850474872.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li> <li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.852029233.0000000002A90000.00000040.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis

