

JOeSandbox Cloud BASIC



ID: 431830

Sample Name:

SecuriteInfo.com.Variant.Jaik.46242.3594.22390

Cookbook: default.jbs

Time: 11:46:16

Date: 09/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report SecuriteInfo.com.Variant.Jaik.46242.3594.22390	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
Signature Overview	4
AV Detection:	4
Networking:	4
System Summary:	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	8
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	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: SecuriteInfo.com.Variant.Jaik.46242.3594.exe PID: 3920 Parent PID: 5824	10
General	10
Disassembly	10
Code Analysis	10

Analysis Report SecuriteInfo.com.Variant.Jaik.46242.35...

Overview

General Information

Sample Name:

SecuriteInfo.com.Variant.Jaik.46242.3594.22390 (renamed file extension from 22390 to exe)

Analysis ID:

431830

MD5:

99bbf83abe9d6e4.

SHA1:

b0bd6ba2dc10eb..

SHA256:




2b2a00650dc91d..

Tags:

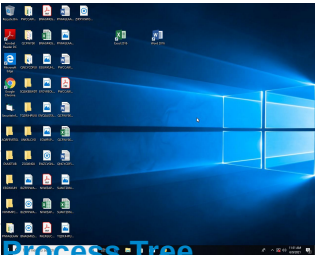
exe

GuLoader

Infos:



Most interesting Screenshot:



Process Tree

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

96

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Potential malicious icon found

Yara detected GuLoader

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

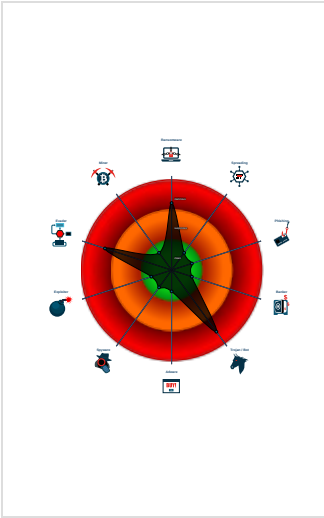
Tries to detect virtualization through...


Abnormal high CPU Usage

Contains functionality for execution ...

Contains functionality to call native f...

Classification



- System is w10x64
-  SecuriteInfo.com.Variant.Jaik.46242.3594.exe (PID: 3920 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.46242.3594.exe' MD5: 99BBF83ABE9D6E4ECC91493E32230833)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "https://www.pos.nblwarehouse.my.id/bin_GgrWeMMq137.bin, http://benvenuti.rs/wp-co"}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Variant.Jaik.46242.3594.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.722670441.0000000000228 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000000.197018556.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.721540373.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	


Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Variant.Jaik.46242.3594.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.0.SecuriteInfo.com.Variant.Jaik.46242.3594.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

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

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Yara detected GuLoader

Malware Analysis System Evasion:



Detected RDTS dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTS 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 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Techniques



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Jaik.46242.3594.exe	26%	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://www.pos.nblwarehouse.my.id/bin_GgrWeMMq137.bin, benvenuti.rs/wp-co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.pos.nblwarehouse.my.id/bin_GgrWeMMq137.bin, benvenuti.rs/wp-co	true	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431830
Start date:	09.06.2021
Start time:	11:46:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Jaik.46242.3594.22390 (renamed file extension from 22390 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:	28
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"> HCA enabled EGA enabled HDC enabled AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"> 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):	5.607689655560483
TrID:	<ul style="list-style-type: none">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:	SecuriteInfo.com.Variant.Jaik.46242.3594.exe
File size:	147456
MD5:	99bbf83abe9d6e4ecc91493e32230833
SHA1:	b0bd6ba2dc10eb5552edc7a3460c80ee0eb1b11e
SHA256:	2b2a00650dc91d1a7ccfa4a62e3462762c62d8a092bddb75943f87074f1d56a5
SHA512:	0f6b9f9a843f491b925aab0af5d4f08024a2d430c41022c23afb46ce3abdf7881e8d87ac6d93f5adfc2f11aee0f0bb0ac28fa2500ec118bc1ed496281d3afec6
SSDEEP:	1536:Fttu3FssKUmr9DJ1FJS1bQNZ6bp/+Dtr5m3XSt4IYS0eXJWUTFboob:ztu3alxx3fSQmbs55r4l6eXJWUB0ob
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....G.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401c10
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:	0x47BBB203 [Wed Feb 20 04:52:19 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:	9b8686288ab82fdbf8ede30bc55c83b7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x205e8	0x21000	False	0.356082800663	data	5.85827510304	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x950	0x1000	False	0.171875	data	2.03163651737	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: SecuriteInfo.com.Variant.Jaik.46242.3594.exe PID: 3920 Parent PID: 5824

General

Start time:	11:47:01
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.46242.3594.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.46242.3594.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	99BBF83ABE9D6E4ECC91493E32230833
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.722670441.0000000002280000.00000040.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.197018556.0000000000401000.00000020.00020000.sdmp, Author: Joe Security• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.721540373.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis