ID: 449805
Sample Name:
sVNHE4jjOw.exe
Cookbook: default.jbs
Time: 11:48:41
Date: 16/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report sVNHE4jjOw.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: sVNHE4jjOw.exe PID: 2412 Parent PID: 5704 10
General 10
File Activities 10
Disassembly 10
Code Analysis 10

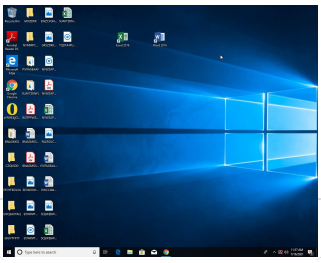
Windows Analysis Report sVNHE4jjOw.exe

Overview

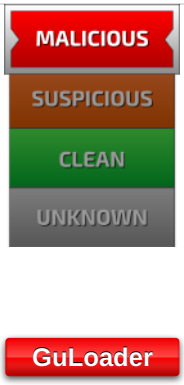
General Information

Sample Name:	sVNHE4jjOw.exe
Analysis ID:	449805
MD5:	72fe87cb4fd41cf…
SHA1:	2c8c745378f4a80..
SHA256:	6d26df7a7163053.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

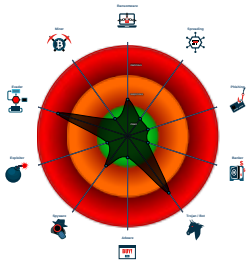


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- sVNHE4jjOw.exe (PID: 2412 cmdline: 'C:\Users\user\Desktop\sVNHE4jjOw.exe' MD5: 72FE87CB4FD41CF172A9CAECBDC6887F)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://ceattire.com/bin_BDePikHU25.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1293352201.00000000240 90000.00000040.00000001.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

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

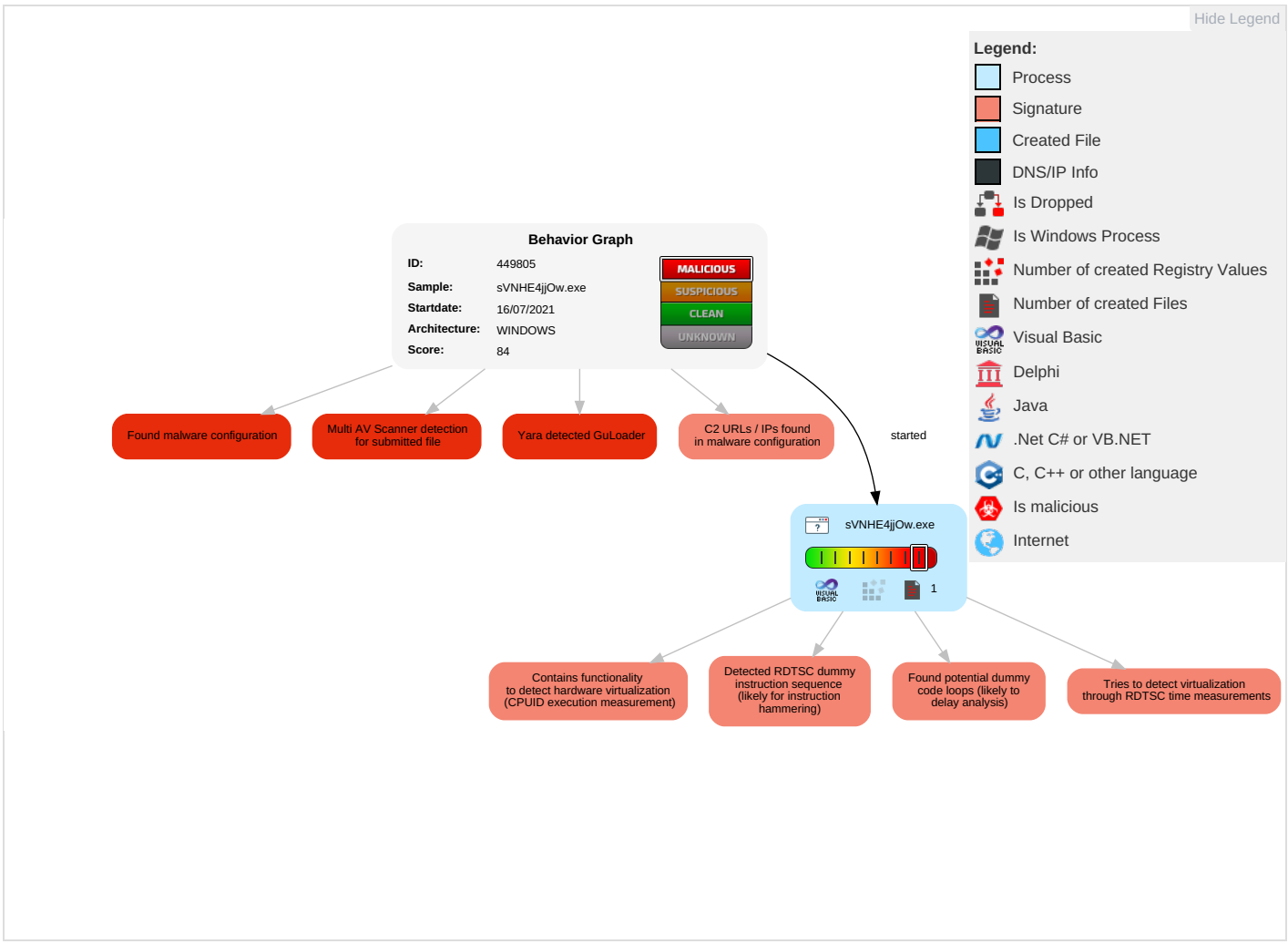
Anti Debugging:

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 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	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	

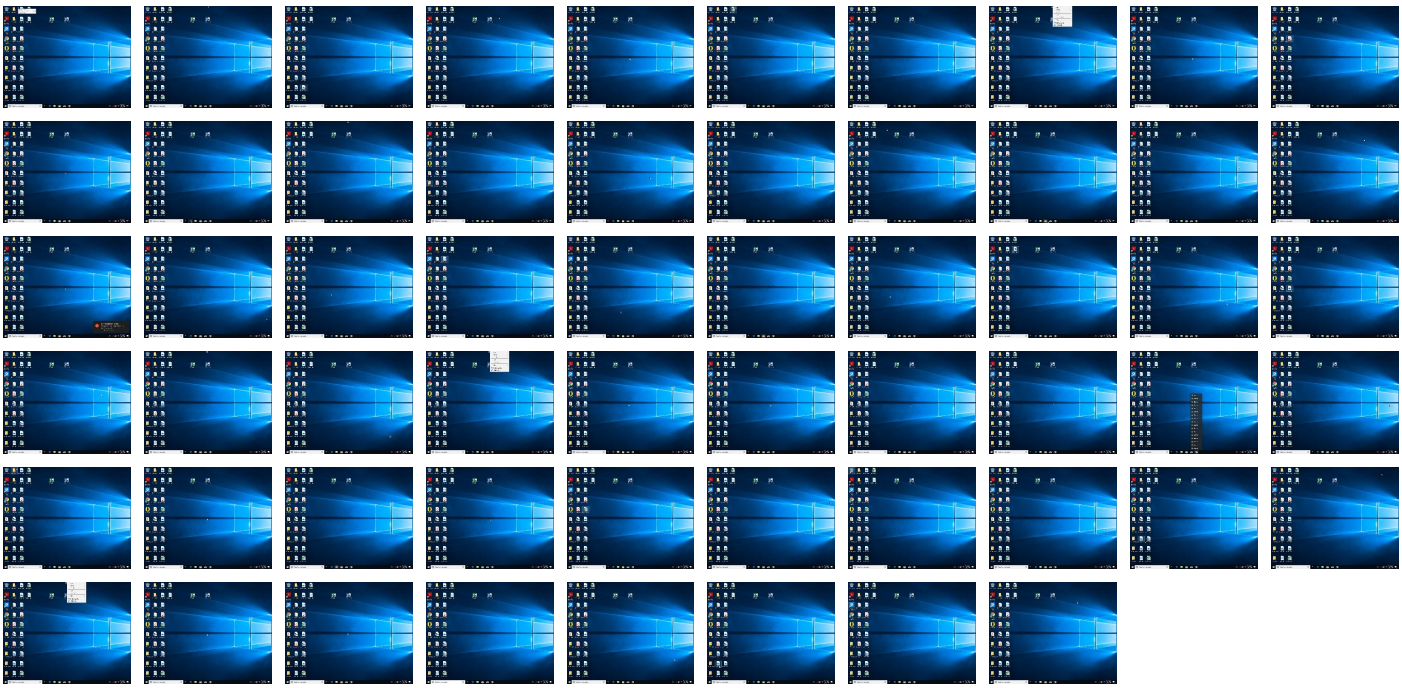
Behavior Graph



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
sVNHE4jjOw.exe	35%	Virustotal		Browse
sVNHE4jjOw.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ceattire.com/bin_BDePikHU25.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ceattire.com/bin_BDePikHU25.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	449805
Start date:	16.07.2021
Start time:	11:48:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sVNHE4jjOw.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:	40
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:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
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:	
Entropy (8bit):	4.800085383449222
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:	sVNHE4jjOw.exe
File size:	267408
MD5:	72fe87cb4fd41cf172a9caecbdc6887f
SHA1:	2c8c745378f4a80e96dbabf574d1ac2d6408df69
SHA256:	6d26df7a7163053aa756f62ee4504af93020696cee98a1fc891c600ac76acc1c
SHA512:	6fa975b8ba69692b6eb278f4145d13fea8d3c64c33d7f9267172f1718f4a4a1f0852cc65f4b16691d152afe9035f038c4c203deecf85e56ecf451448f8a6f60a
SSDEEP:	1536:35/ikBkzm219ZmFtg5sfrWrNjosvNmmCUibm84t3TxY/n:35/pkdPAw0iNVvNnbVZxY/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L..... L.....`.....p.....p....@.....

File Icon

Icon Hash:	e8ccce8e8ececce8

Static PE Info

General

Entrypoint:	0x401470
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:	0x4C20BCC1 [Tue Jun 22 13:38:09 2010 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:	a6a8fddf213e725d12277ffa52409c50

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Unstaunch1@Strygeork.GUN, CN=ryper, OU=Nonpropa4, O=Twisti8, L=Efterspil4, S=FORDUMM, C=AD
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	• 7/15/2021 2:48:16 PM 7/15/2022 2:48:16 PM
Subject Chain	• E=Unstaunch1@Strygeork.GUN, CN=ryper, OU=Nonpropa4, O=Twisti8, L=Efterspil4, S=FORDUMM, C=AD
Version:	3
Thumbprint MD5:	74A7224C73056759B33CA9EB4F1649A0
Thumbprint SHA-1:	C9DACC639E15797636E4B8185A4E5522E877B0B9
Thumbprint SHA-256:	CEEC9E9D00E6C96EE6ECF708C8F2812C2BC31DADAF84E625E66CEA556F34ABA7
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x35bb0	0x36000	False	0.257260923032	data	4.74248188384	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x37000	0xbd4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x7a8a	0x8000	False	0.294769287109	data	4.40772584771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

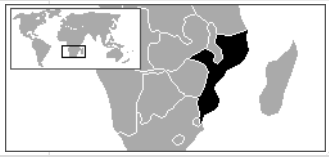
Resources

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
Swahili	Kenya	
Swahili	Mozambiq	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: sVNHE4jjOw.exe PID: 2412 Parent PID: 5704

General

Start time:	11:49:31
Start date:	16/07/2021
Path:	C:\Users\user\Desktop\sVNHE4jjOw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\sVNHE4jjOw.exe'
Imagebase:	0x400000
File size:	267408 bytes
MD5 hash:	72FE87CB4FD41CF172A9CAECBDC6887F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1293352201.0000000002490000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis