

JOeSandbox Cloud BASIC



ID: 430961

Sample Name: PC21-
270421.exe

Cookbook: default.jbs

Time: 09:38:59

Date: 08/06/2021

Version: 32.0.0 Black Diamond



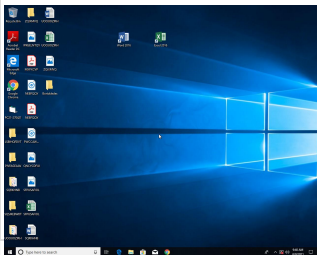
Table of Contents

Table of Contents	2
Analysis Report PC21-270421.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
Initial Sample	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	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 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	8
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	9
Statistics	9
System Behavior	10
Analysis Process: PC21-270421.exe PID: 6376 Parent PID: 5780	10
General	10
File Activities	10
File Created	10
Disassembly	10
Code Analysis	10

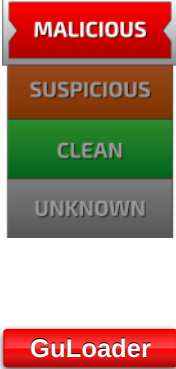
Analysis Report PC21-270421.exe

Overview

General Information

Sample Name:	PC21-270421.exe
Analysis ID:	430961
MD5:	140733109e3a3b..
SHA1:	5f8685572c91386.
SHA256:	4bb04df120eb27c.
Infos:	 
Most interesting Screenshot:	

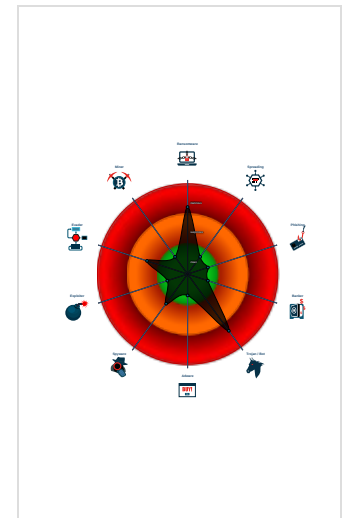
Detection

	
Score:	57
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains capabilities to detect virtua...
Detected potential crypto function
Found large amount of non-executed...
PE file contains strange resources
Program does not show much activi...
Queries the volume information (nam...
Sample file is different than original ...

Classification



Process Tree

- System is w10x64
-  PC21-270421.exe (PID: 6376 cmdline: 'C:\Users\user\Desktop\PC21-270421.exe' MD5: 140733109E3A3B3DE2AE1AAF164178DA)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1IyeIvFG2j6rM8MkH-0GyKJbMY3m1XbJ6"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
PC21-270421.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

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

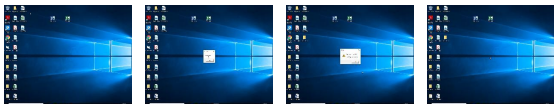
Mitre Att&ck Matrix

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	Path Interception	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 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	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	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	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

Behavior Graph



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
PC21-270421.exe	33%	Virustotal		Browse
PC21-270421.exe	17%	ReversingLabs	Win32.InfoStealer.VBodius	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430961
Start date:	08.06.2021
Start time:	09:38:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PC21-270421.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:	6
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:	mal57.rans.troj.winEXE@1/0@0/0
EGA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 2.9% (good quality ratio 0.6%)• Quality average: 12.4%• Quality standard deviation: 25%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Stop behavior analysis, all processes terminated
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):	4.5836210897416745
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:	PC21-270421.exe
File size:	147456
MD5:	140733109e3a3b3de2ae1aaf164178da
SHA1:	5f8685572c91386045a5f458b298ee8c6934277c
SHA256:	4bb04df120eb27c3f5b3a46a54891b927fe4232daf75b9ecaddc2f24d61533c
SHA512:	4877a2f6b11143837daa69527b42307c1381e0aec14ada161157937ad4bed29dbf9e5c27734d976c11bc37d3caf9c1066e84d4f0d041092c71dace2010d613c7
SSDEEP:	1536:ELaMxQEBAFJaW5RmJjug+YbhRjurq7NxYZMvkastkn23U:EGOlmpu5eRjurq7NuZM8ask
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...`..`.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x4014b8
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:	0x60BDF60 [Mon Jun 7 10:52:16 2021 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:	b1d5215cf0ff1abab4dacdc311d642d4

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x201ac	0x21000	False	0.324573863636	data	4.82414979296	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1234	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0xa04	0x1000	False	0.182373046875	data	2.19382824201	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
Sesotho (Sutu)	South Africa	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: PC21-270421.exe PID: 6376 Parent PID: 5780

General

Start time:	09:39:52
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\PC21-270421.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PC21-270421.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	140733109E3A3B3DE2AE1AAF164178DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis