

JoeSandbox Cloud BASIC



ID: 448876

Sample Name: ZGNX11JMSc

Cookbook: default.jbs

Time: 19:51:35

Date: 14/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report ZGNX11JMSc	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	3
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: ZGNX11JMSc.exe PID: 5764 Parent PID: 5588	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report ZGNX11JMSc

Overview

General Information

Sample Name:	ZGNX11JMSc (renamed file extension from none to exe)
Analysis ID:	448876
MD5:	fcfb0ec70f1419e...
SHA1:	d3b529d77f1de00.
SHA256:	ff1b034c7060724..
Tags:	32 exe GuLoader trojan
Infos:	
Most interesting Screenshot:	

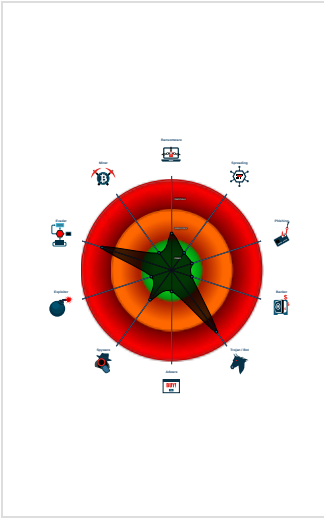
Detection

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

Signatures

Found malware configuration
Yara detected GuLoader
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
- ZGNX11JMSc.exe (PID: 5764 cmdline: 'C:\Users\user\Desktop\ZGNX11JMSc.exe' MD5: FCFB0EC70F1419EDE8A534CC95CB61E9)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://ceattire.com/bin_UYDMbHwI28.bin"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ZGNX11JMSc.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.741035420.000000000231 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000000.216935680.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.739221783.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	


Unpacked PE

Source	Rule	Description	Author	Strings
0.2.ZGNX11JMS.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.0.ZGNX11JMS.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

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)

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	Risk Score
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	Risk Score
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	Risk Score
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	Risk Score



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ZGNX11JMS.exe	7%	ReversingLabs	Win32.Trojan.Vebzenpak	

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_UYDMbHwI28.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_UYDMbHwI28.bin	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	448876
Start date:	14.07.2021
Start time:	19:51:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZGNX11JMSc (renamed file extension from none 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:	33
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 enabledEGA enabledHDC enabledAMSI 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:	Failed
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIOverride 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):	4.7769054763067915
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:	ZGNX11.JMSc.exe
File size:	267376
MD5:	fcfb0ec70f1419ede8a534cc95cb61e9
SHA1:	d3b529d77f1de00d63a75b3956d4bcf6bbce30ca
SHA256:	ff1b034c7060724133c6df0aa8cf5411ec0e6775d3aca83a127617340a8c588a
SHA512:	ffec36b157f889a2bd351b9d8423b247138a5fd2e57de83bb1253336518431136a265d244b653af470a8d04e2674c4cadf467c065a7fc38f10effedd705ab248
SSDEEP:	1536:x2M5j2eBXFScbssSe/W+dMa27qQ0Z9Dfs4lwNAVgilOm72tNHLg/8A:T5FXrbVTeE2uQU7s49AMUrg/8A
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......y.....Rich.....PE..L....FR.....`.....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:	0x5246CAE2 [Sat Sep 28 12:26:10 2013 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:	a6a8fddf213e725d1227ffa52409c50

Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Overbee@NONASSUM.DRA, CN=skrdd, OU=UNDE, O=prototypi, L=Nyordn5, S=sobs, C=MG
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">7/13/2021 10:05:37 AM 7/13/2022 10:05:37 AM
Subject Chain	<ul style="list-style-type: none">E=Overbee@NONASSUM.DRA, CN=skrdd, OU=UNDE, O=prototypi, L=Nyordn5, S=sobs, C=MG
Version:	3
Thumbprint MD5:	9036914828CBB0BD5603E92A0629EBCE
Thumbprint SHA-1:	502D44A3683EF19D6EE93B5A0BA39CEF214FA587
Thumbprint SHA-256:	D8DC1D893CD8ACCF7B4CB8910AC7F2C4539AB530AD74E93F825CCDA9E5C58408
Serial:	00

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x35930	0x36000	False	0.255479600694	data	4.71656794382	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	0x7a92	0x8000	False	0.294891357422	data	4.41054714474	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
Swahili	Kenya	

Language of compilation system	Country where language is spoken	Map
Swahili	Mozambiq	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: ZGNX11JMS.exe PID: 5764 Parent PID: 5588

General

Start time:	19:52:30
Start date:	14/07/2021
Path:	C:\Users\user\Desktop\ZGNX11JMS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ZGNX11JMS.exe'
Imagebase:	0x400000
File size:	267376 bytes
MD5 hash:	FCFB0EC70F1419EDE8A534CC95CB61E9
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: 00000000.00000002.741035420.0000000002310000.00000040.00000001.sdmp, Author: Joe Security Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.216935680.000000000401000.00000020.00020000.sdmp, Author: Joe Security Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.739221783.000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

