ID: 247696
Sample Name:
zeusaes_2.7.6.6.vir
Cookbook: default.jbs
Time: 13:09:34
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

Analysis Report zeusaes_2.7.6.6.vir

Overview

General Information

Sample Name:	zeusaes_2.7.6.6.vir (renamed file extension from vir to exe)
Analysis ID:	247696
MD5:	0e963c9b828204..
SHA1:	19017d8a1a7c6d..
SHA256:	1294e6cce42852..

Most interesting Screenshot:

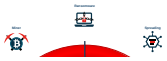
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Binary contains a suspicious time st…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to launch a pr…

Classification



Startup

- **System is w10x64**
- zeusaes_2.7.6.6.exe (PID: 4532 cmdline: 'C:\Users\user\Desktop\zeusaes_2.7.6.6.exe' MD5: 0E963C9B8282042690437D69A8AD7395)
  - zeusaes_2.7.6.6.exe (PID: 4504 cmdline: c:\users\user\desktop\zeusaes_2.7.6.6.exe MD5: 0E963C9B8282042690437D69A8AD7395)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

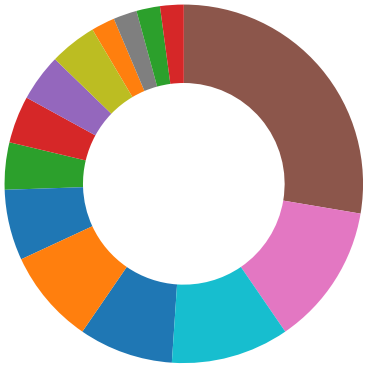
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Binary contains a suspicious time stamp

HIPS / PFW / Operating System Protection Evasion:

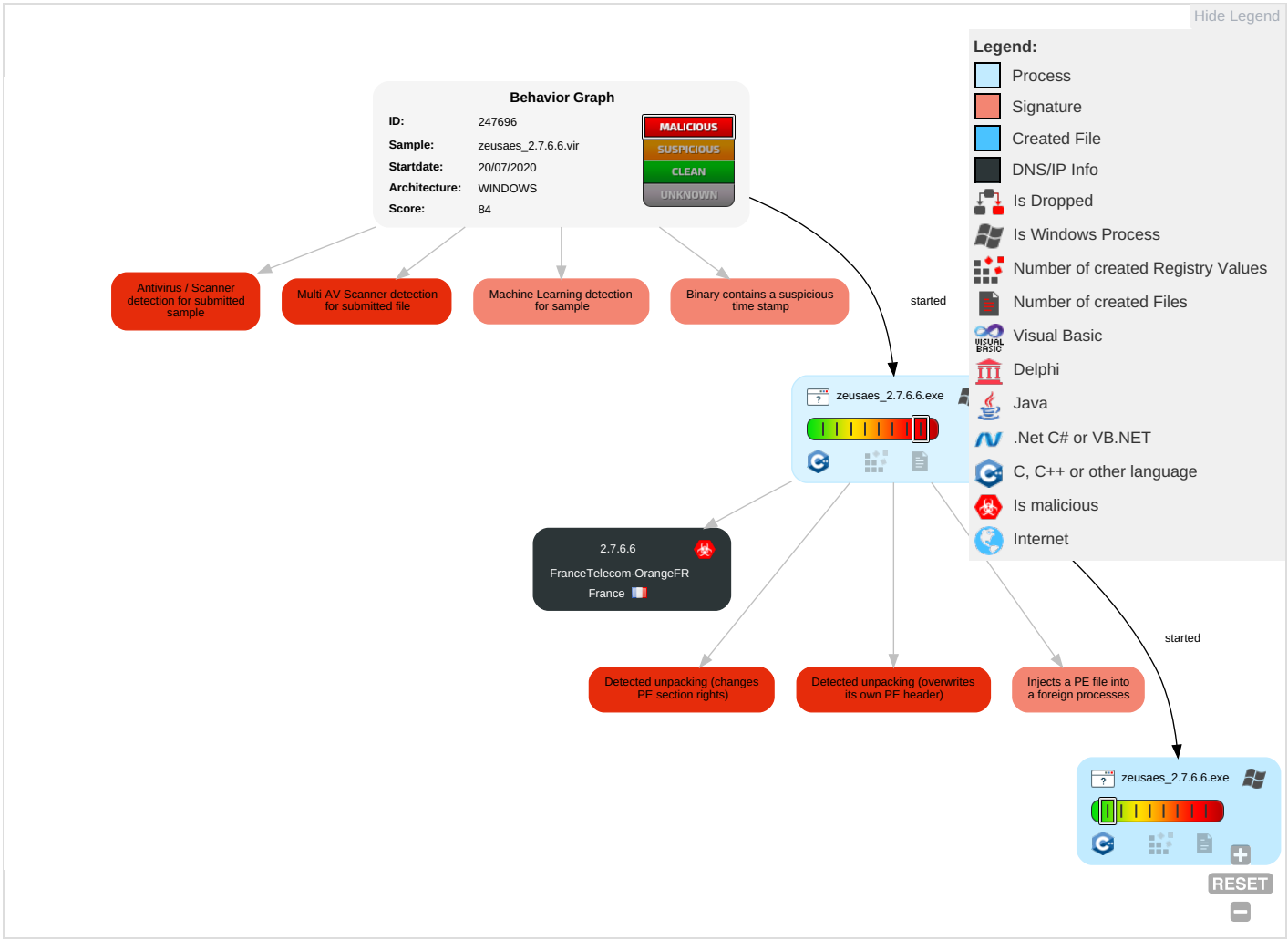
Injects a PE file into a foreign processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Execution through API 1	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	Input Capture 1 1	Network Share Discovery 1	Remote File Copy 1	Input Capture 1 1	Data Encrypted 1	Standard Cryptographic Protocol 2	Eavesdrop c Insecure Network Communica
Replication Through Removable Media	Service Execution	Application Shimming 1	Access Token Manipulation 1 1	Software Packing 2 1	Network Sniffing	System Time Discovery 2	Remote Services	Clipboard Data 1	Exfiltration Over Other Network Medium	Commonly Used Port 1	Exploit SS7 Redirect Ph Calls/SMS
External Remote Services	Windows Management Instrumentation	Accessibility Features	Process Injection 1 1 1	Access Token Manipulation 1 1	Input Capture	Process Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Remote File Copy 1	Exploit SS7 Track Devic Location
Drive-by Compromise	Scheduled Task	System Firmware	Application Shimming 1	Timestomp 1	Credentials in Files	Account Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Process Injection 1 1 1	Account Manipulation	System Owner/User Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communica
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Install Root Certificate 1	Brute Force	Security Software Discovery 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jamming or Denial of Service
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Obfuscated Files or Information 1	Two-Factor Authentication Interception	File and Directory Discovery 1	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Rogue Wi-F Access Poir

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Indicator Blocking	Bash History	System Information Discovery 4	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	Downgrade Insecure Protocols

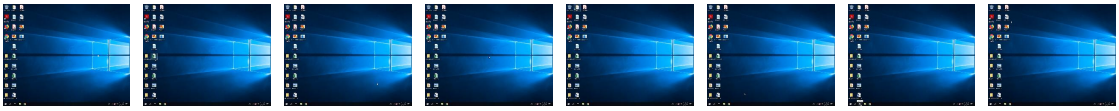
Behavior Graph



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
zeusaes_2.7.6.6.exe	82%	Virustotal		Browse
zeusaes_2.7.6.6.exe	67%	Metadefender		Browse
zeusaes_2.7.6.6.exe	97%	ReversingLabs	Win32.Trojan.Zbot	
zeusaes_2.7.6.6.exe	100%	Avira	TR/Spy.Zbot.ajoumea	
zeusaes_2.7.6.6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.zeusaes_2.7.6.6.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.ajoumea		Download File
1.2.zeusaes_2.7.6.6.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File
1.0.zeusaes_2.7.6.6.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.ajoumea		Download File
0.1.zeusaes_2.7.6.6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.zeusaes_2.7.6.6.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.ajoumea		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://smusicsoft.com/stat/stat.php?id=1	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://smusicsoft.com/stat/stat.php?id=1h	zeusaes_2.7.6.6.exe, 00000001.00000002.457622544.00000000040000.00000040.00000001.sdmp	false		unknown
http://smusicsoft.com/stat/stat.php?id=1	zeusaes_2.7.6.6.exe	false	• 1%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Country	Flag	ASN	ASN Name	Malicious
2.7.6.6	France		3215	FranceTelecom-OrangeFR	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper

Analysis ID:	247696
Start date:	20.07.2020
Start time:	13:09:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeusaes_2.7.6.6.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	7
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.evad.winEXE@3/0@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.8% (good quality ratio 91.5%) • Quality average: 81.9% • Quality standard deviation: 29.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FranceTelecom-OrangeFR	newdat.ps1	Get hash	malicious	Browse	• 90.121.249.114
	FederalAgency.x86	Get hash	malicious	Browse	• 145.242.17.155
	http://https://download.wbxhub.com:443/cgi/adk/chrdl.cgi?wb_id=35781x-0F&iid=Webexplorer	Get hash	malicious	Browse	• 2.1.0.5

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):	7.707763364756743
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	zeusaes_2.7.6.6.exe
File size:	183933
MD5:	0e963c9b8282042690437d69a8ad7395
SHA1:	19017d8a1a7c6ded1ca488d31aee23ce58e71ce8
SHA256:	1294e6cce4285225612898a4fbc75a640e69dc0f246af698e2c91d48ad2d61b8
SHA512:	d7216f5c12f1402fdb841a849d29c5fc8de3f1e31c58adadef84d4dcf7250247231b3355b949e0a27ab186ab0d405f1567c906dae62452d6e038abeac1520d19
SSDEEP:	3072:FSm3CTNRk5qJzdqmXnnx0FpDNu8inMpEYfAoo23ISQqTRJJ0ub2q5ti:FSmgk5qJD3nxc9iMXAo1IPqTRj0Ka
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...x.wnn.....d..."....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.code
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:	0x6E770278 [Sat Sep 23 03:39:36 2028 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	aeceeef30d07eabae260080b82b05c48

Entrypoint Preview

Instruction
push 00000880h
push 00000000h
push 0040B500h
call 00007FA9F06D9301h
add esp, 0Ch
push es
push es
add byte ptr [eax], al
add al, ch
cmc
das
add byte ptr [eax], al
mov dword ptr [0040B504h], eax
push 00000000h
push 00001000h
push 00000000h
call 00007FA9F06D92E7h
mov dword ptr [0040B500h], eax
call 00007FA9F06DC981h
call 00007FA9F06DC829h
call 00007FA9F06D98C7h
call 00007FA9F06D969Fh
mov dword ptr [0040B50Ch], 00000000h
push 000008AEh
push 49807920h
add eax, dword ptr [ebx]
add byte ptr [eax], al
fstp st(0)
push 0040BD60h
push 00000000h
push 0000000Ah
push 0001011Ah
push 000000FFh
call 00007FA9F06DC6E7h
push 0040BD68h
push 00000000h
push 00000005h
push 0000000Ah
push 00000004h
call 00007FA9F06DC6C9h
push 0040BD70h
push 00000000h
push 00000005h
push 0000001Ah
push 00000004h
call 00007FA9F06DC6ABh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2e4	0x101	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x1e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb38c	0x58	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x215a	0x2200	False	0.439108455882	data	5.64554736574	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text	0x4000	0x40d3	0x4200	False	0.555989583333	data	6.68525027588	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x42	0x200	False	0.09765625	data	0.792181153458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1dd0	0x1600	False	0.431107954545	data	3.89614250878	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x1e4	0x200	False	0.35546875	data	2.47977308096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc0a0	0x130	data	English	United States
None	0xc1d0	0x14	data	English	United States

Imports

DLL	Import
MSVCRT.dll	memset, floor, ceil, _CIlog, memcpy, strlen
KERNEL32.dll	GetModuleHandleA, HeapCreate, LoadLibraryA, GetProcAddress, HeapDestroy, ExitProcess, CloseHandle, HeapReAlloc, HeapAlloc, HeapFree, CreateFileA, ReadFile
USER32.DLL	MessageBoxA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

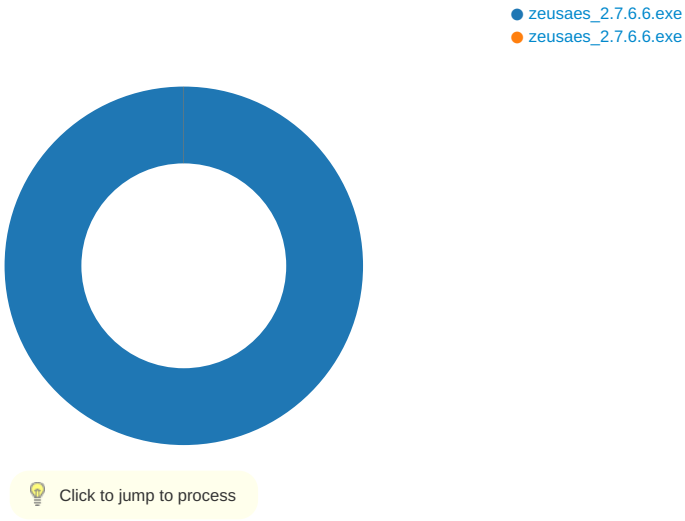
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: zeusaes_2.7.6.6.exe PID: 4532 Parent PID: 4612

General

Start time:	13:10:04
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeusaes_2.7.6.6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeusaes_2.7.6.6.exe'
Imagebase:	0x400000
File size:	183933 bytes
MD5 hash:	0E963C9B8282042690437D69A8AD7395
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\zeusaes_2.7.6.6.exe	unknown	183933	success or wait	1	2110084	ReadFile

Analysis Process: zeusaes_2.7.6.6.exe PID: 4504 Parent PID: 4532

General

Start time:	13:10:06
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeusaes_2.7.6.6.exe
Wow64 process (32bit):	true
Commandline:	c:\users\user\desktop\zeusaes_2.7.6.6.exe
Imagebase:	0x400000
File size:	183933 bytes
MD5 hash:	0E963C9B8282042690437D69A8AD7395
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis