

JoeSandbox Cloud BASIC



**ID:** 434685

**Sample Name:** lpSbvoEkD6.exe

**Cookbook:** default.jbs

**Time:** 11:55:24

**Date:** 15/06/2021

**Version:** 32.0.0 Black Diamond




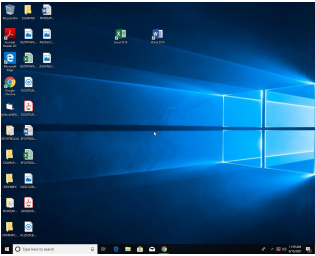
## Table of Contents

Table of Contents	2
Windows Analysis Report IpSbvoEkD6.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
Memory Dumps	3
Unpacked PEs	3
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 IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
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	8
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: IpSbvoEkD6.exe PID: 6092 Parent PID: 5672	10
General	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report IpSbvoEkD6.exe

## Overview

### General Information

Sample Name:	IpSbvoEkD6.exe
Analysis ID:	434685
MD5:	ab19307ba34923..
SHA1:	451cb1fc62f9fcd...
SHA256:	5445447afbc7e74.
Tags:	<div>exe</div> <div>GuLoader</div>
Infos:	  
Most interesting Screenshot:	

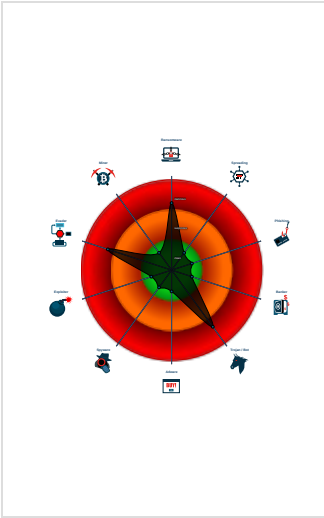
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
Score:	84
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...
Found potential dummy code loops (...)
Tries to detect virtualization through...
Abnormal high CPU Usage
Detected potential crypto function
PE file contains strange resources
Program does not show much activi...
Sample file is different than original ...

### Classification



## Process Tree

System is w10x64
 IpSbvoEkD6.exe (PID: 6092 cmdline: 'C:\Users\user\Desktop\IpSbvoEkD6.exe' MD5: AB19307BA349239ED32F7EC471C882E6)
cleanup

## Malware Configuration

### Threatname: GuLoader

<pre>{   "Payload URL": "http://theater.expodium.net/wp-content/plugins/m/Host_AvQmpG228.bin, https://meatflesh.com/b/Host_AvQmpG228.bin" }</pre>
---

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
IpSbvoEkD6.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.216224466.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.576531591.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	


### Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.IpSbvoEkD6.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.0.IpSbvoEkD6.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

### Malware Analysis System Evasion:



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	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Techniques Windows Anti-Malware
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	Recovery Techniques Windows Anti-Malware





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
IpSbvoEkD6.exe	29%	Virustotal		<a href="#">Browse</a>

### 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:	434685
Start date:	15.06.2021
Start time:	11:55:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lpSbvoEkD6.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:	24
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"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 34% (good quality ratio 8.5%)</li><li>• Quality average: 14.6%</li><li>• Quality standard deviation: 26%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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):	5.743654430674186
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	lpSbvoEkD6.exe
File size:	147456
MD5:	ab19307ba349239ed32f7ec471c882e6
SHA1:	451cb1fc62f9fcd4d6f5e8b187404d278f21c65e
SHA256:	5445447afbc7e74f9a827b122e1b38c4cb9715ec3dfc5bbfbf4805759bfc6eac
SHA512:	a18c355e4516741dc02f8bf1572b852db6a7d217b42da3fe1b8b4f35e1225e404858e3abf199b97024a2c7e412f6391a35edfc0e9a2397f4bf24334d4072764c
SSDEEP:	1536:z9g1+OOZDPJGMpTzmqEDAoZH0J4oJCEw3dceV1h7nSH2:AOOZrJGM5q1DAoZi4oY3dccY2
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....!..W.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x4018a4

<b>General</b>	
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:	0x57CF2100 [Tue Sep 6 20:03:12 2016 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:	2c08d8f9644132654eb702b279083d5c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2085c	0x21000	False	0.378432765152	data	5.99976435722	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1278	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x930	0x1000	False	0.170166015625	data	1.97470101836	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: IpSbvoEkD6.exe PID: 6092 Parent PID: 5672

General

Start time:	11:56:18
Start date:	15/06/2021
Path:	C:\Users\user\Desktop\IpSbvoEkD6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IpSbvoEkD6.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	AB19307BA349239ED32F7EC471C882E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.216224466.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li><li>• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.576531591.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li></ul>
Reputation:	low

Disassembly

Code Analysis