

JoeSandbox Cloud BASIC



ID: 430813

Sample Name: vbc.exe.vir

Cookbook: default.jbs

Time: 02:40:39

Date: 08/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report vbc.exe.vir	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	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
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	9
Static PE Info	9
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	10
Statistics	10
System Behavior	10
Analysis Process: vbc.exe.exe PID: 3564 Parent PID: 5576	10
General	10
Disassembly	10
Code Analysis	10

Analysis Report vbc.exe.vir

Overview

General Information

Sample Name:

vbc.exe.vir (renamed file extension from vir to exe)

Analysis ID:

430813

MD5:

788016c9072423..


SHA1:

040f85b4ef512bb..

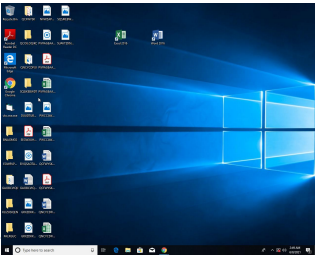
SHA256:

df34f3d4030a5ea..

Infos:



Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

88

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 functionality to detect hard...

Found potential dummy code loops (...)

Tries to detect virtualization through...

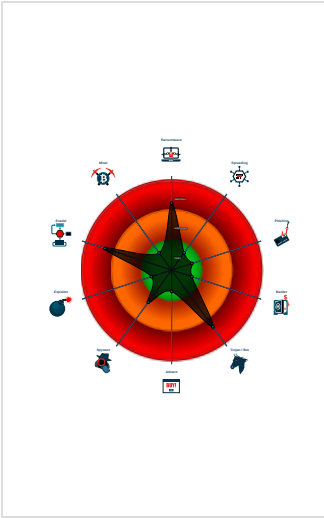
Abnormal high CPU Usage

Contains functionality for execution ...


Contains functionality to call native f...

Contains functionality to query CPU ...

Classification



Process Tree

- System is w10x64
-  vbc.exe.exe (PID: 3564 cmdline: 'C:\Users\user\Desktop\vbc.exe.exe' MD5: 788016C9072423914B96F0D15A61812D)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "https://bara-seck.com/bin_YIuwAXdc211.bin, https://wizumiya.co.jp/html/user_data/"}
```

Yara Overview

Initial Sample

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1277517703.000000000004	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
01000.00000020.00020000.sdmp				
00000000.00000000.194728526.0000000000040	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
1000.00000020.00020000.sdmp				

Unpacked PEs

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



Contains functionality to detect hardware virtualization (CPUID execution measurement)

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	Input Capture 1	Security Software Discovery 3 1	Remote Services	Input Capture 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	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Recovery



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vbc.exe.exe	13%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bara-seck.com/bin_YluwAXdc211.bin, https://wizumiya.co.jp/html/user_data/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bara-seck.com/bin_YluwAXdc211.bin, https://wizumiya.co.jp/html/user_data/	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430813
Start date:	08.06.2021
Start time:	02:40:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vbc.exe.vir (renamed file extension from vir 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:	35
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:	mal88.rans.troj.evad.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: 16.1% (good quality ratio 5.2%)Quality average: 17.8%Quality standard deviation: 27.1%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSI
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):	5.60090149728624
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:	vbc.exe.exe
File size:	147456
MD5:	788016c9072423914b96f0d15a61812d
SHA1:	040f85b4ef512bb74990becfa1a5029f92eb65c7
SHA256:	df34f3d4030a5ea484108271f749ca5fbc3af0f415051e98b342a505c88971e4
SHA512:	c9a75e6b54113d3d02c32d314ff76cc82b9bd4b88d07fec6b7636417e49184ebb691ecf63db3aac8dd4a96e49392959638c70ab20412f1c4454ac7963266c2c4
SSDEEP:	3072:JX84PzFh5UOkyp2te2+4IM20JMN0z3wnz:xxFjpYF+4IM20JMN0z3A

General

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...x..Q.....0..... ..@.....
-----------------------	---

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x401c10
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:	0x51CF9578 [Sun Jun 30 02:18:32 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:	9b8686288ab82fdbf8ede30bc55c83b7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20608	0x21000	False	0.357185132576	data	5.84922850488	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x970	0x1000	False	0.1728515625	data	2.05495100774	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: vbc.exe.exe PID: 3564 Parent PID: 5576

General

Start time:	02:41:23
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\vbc.exe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vbc.exe.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	788016C9072423914B96F0D15A61812D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.1277517703.0000000000401000.00000020.00020000.sdmp, Author: Joe SecurityRule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.194728526.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis