

JoeSandbox Cloud BASIC



ID: 546457

Sample Name: 2i85zGtHll.exe

Cookbook: default.jbs

Time: 06:07:12

Date: 30/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 2i85zGtHll.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: RedLine	3
Yara Overview	3
Initial Sample	3
PCAP (Network Traffic)	3
Memory Dumps	3
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
Malware Analysis System Evasion:	4
Stealing of Sensitive Information:	4
Remote Access Functionality:	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	7
URLs	7
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
Contacted IPs	7
Public	8
General Information	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	10
Sections	10
Resources	10
Imports	10
Version Infos	10
Network Behavior	10
Network Port Distribution	10
TCP Packets	11
Code Manipulations	11
Statistics	11
System Behavior	11
Analysis Process: 2i85zGtHll.exe PID: 4972 Parent PID: 5012	11
General	11
File Activities	11
File Created	11
File Written	11
File Read	11
Disassembly	11
Code Analysis	11

Windows Analysis Report 2i85zGtHll.exe

Overview

General Information

Sample Name:	2i85zGtHll.exe
Analysis ID:	546457
MD5:	5367ca900ff1988..
SHA1:	9b5ef337871490e.
SHA256:	07bb36227d8121..
Tags:	exe RedLineStealer
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

RedLine

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected RedLine Stealer

Found malware configuration

Multi AV Scanner detection for subm...

Queries sensitive video device inform...

Tries to steal Crypto Currency Wallets

Queries sensitive disk information (v...

Found many strings related to Crypt...

Tries to harvest and steal browser in...

Creates a DirectInput object (often fo...

Is looking for software installed on th...

Uses 32bit PE files

Found a high number of Window / Us...

Classification

Process Tree

- System is w10x64
- 2i85zGtHll.exe (PID: 4972 cmdline: "C:\Users\user\Desktop\2i85zGtHll.exe" MD5: 5367CA900FF1988CE2EE1C93B241C764)
- cleanup

Malware Configuration

Threatname: RedLine

```
{  "C2 url": [    "45.150.67.151:31440"  ],  "Bot Id": "svech2"}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
2i85zGtHll.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.327925997.00000000007A 2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000000.275405145.00000000007A 2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.329114422.00000000002B2 0000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: 2i85zGtHll.exe PID: 4972	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	


Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.2i85zGtHll.exe.7a0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.0.2i85zGtHll.exe.7a0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched


Jbx Signature Overview

 Click to jump to signature section

AV Detection: 


Found malware configuration

Multi AV Scanner detection for submitted file

Malware Analysis System Evasion: 

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Stealing of Sensitive Information: 

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

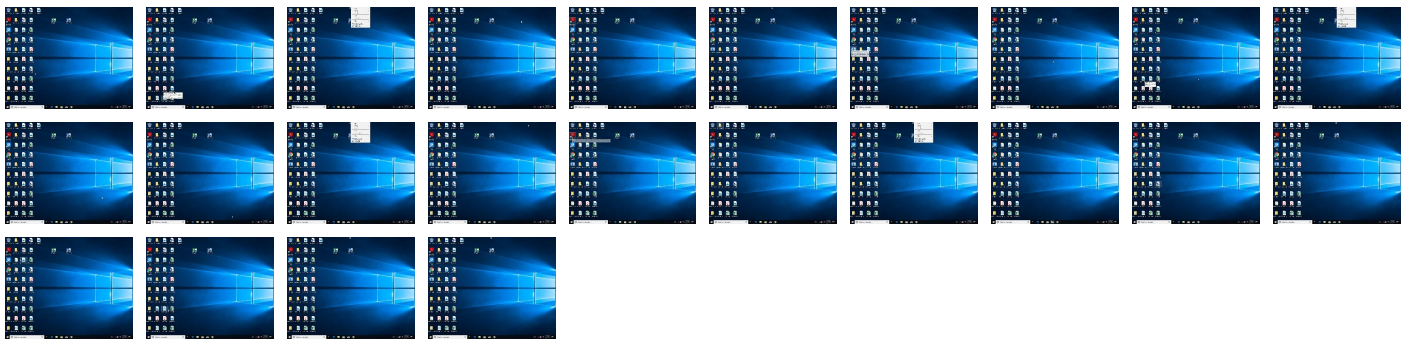
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality: 

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
----------------	-----------	-------------	----------------------	-----------------	-------------------	-----------	------------------	------------	--------------	---------------------	-----------------



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
2i85zGtHll.exe	44%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://ns.adobe.com/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14V	0%	Avira URL Cloud	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs


Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.150.67.151	unknown	Montenegro		61317	ASDETUKhttpwwwheficedcomGB	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546457
Start date:	30.12.2021
Start time:	06:07:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2i85zGtHll.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:	25
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:	mal92.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 0.1% (good quality ratio 0%)• Quality average: 24.2%• Quality standard deviation: 35.4%
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs


Time	Type	Description
06:08:23	API Interceptor	25x Sleep call for process: 2i85zGtHll.exe modified

Joe Sandbox View / Context

IPs

No context
Domains
No context
ASN
No context
JA3 Fingerprints
No context
Dropped Files
No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2i85zGtHll.exe.log		
Process:	C:\Users\user\Desktop\2i85zGtHll.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	2291	
Entropy (8bit):	5.3192079301865585	
Encrypted:	false	
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHlmHKoLHG1qHjHKdHAHDJn:vq5qXAqLdqUqzcGYqhQnoPtIxHbqoL1	
MD5:	B8B968C6C5994E11C0AEF299F6CC13DF	
SHA1:	60351148A0D29E39DF51AE7F8D6DA7653E31BCF9	
SHA-256:	DD53198266985E5C23239DCDDE91B25CF1FC1F4266B239533C11DDF0EF0F958D	
SHA-512:	CFBCFCB650EF8C84A4BA005404E90ECAC9E77BDB618F53CD5948C085E44D099183C97C1D818A905B16C5E495FF167BD47347B14670A6E68801B0C01BC264F16	
Malicious:	true	
Reputation:	moderate, very likely benign file	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.Ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\Nb219d4630d26b88041b59c21e8e2b95c\System.Xml.Ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=	


Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.772942751694307
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) Net Framework (10011505/4) 49.79%Win32 Executable (generic) a (10002005/4) 49.75%Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%Windows Screen Saver (13104/52) 0.07%Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	2i85zGtHll.exe
File size:	106496
MD5:	5367ca900f1988ce2ee1c93b241c764
SHA1:	9b5ef337871490ed36f31bb18b0b4d318039e23c
SHA256:	07bb36227d8121f29c43baae188b43f3d5c4885ef4b20410fca8985235168c68

General

SHA512:	5eea26bb98893617a4fbdaad8cba09d09985170936f340773fab38b656a0ac19ca296a3d6cce2114399affdbd7d1cd4f08a6bc4aedebe4d6c55a5ff4ce841a41
SSDEEP:	1536:uUVrk5Rh6BuHDZlzwuZsri/zs/2ZZ8ZZZqa5ZvLA bYpfVxeRKZ3vsS800x:uUVofrHDakuZv/+qU9LQYUIZP
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$.PE..L...{ K.....0.....@.. ..@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4191ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xA3CD4B7B [Wed Jan 31 04:20:11 2057 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x18d84	0x19000	False	0.4330859375	data	5.88115313974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x4cc	0x800	False	0.2822265625	data	2.97023887572	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1e000	0xc	0x400	False	0.025390625	data	0.0558553080537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: 2i85zGtHll.exe PID: 4972 Parent PID: 5012

General

Start time:	06:08:02
Start date:	30/12/2021
Path:	C:\Users\user\Desktop\2i85zGtHll.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2i85zGtHll.exe"
Imagebase:	0x7a0000
File size:	106496 bytes
MD5 hash:	5367CA900FF1988CE2EE1C93B241C764
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.327925997.00000000007A2000.00000002.00020000.sdmp, Author: Joe SecurityRule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000000.275405145.00000000007A2000.00000002.00020000.sdmp, Author: Joe SecurityRule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.329114422.0000000002B20000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis