ID: 534009
Sample Name:
27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe
Cookbook: default.jbs
Time: 00:07:31
Date: 05/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

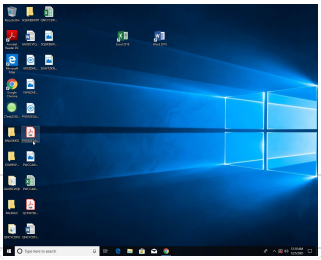
Windows Analysis Report 27eeb225876a7859c31bc8b1e…

Overview

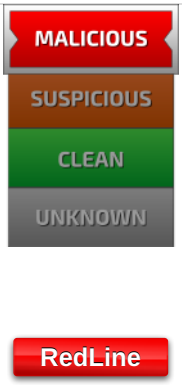
General Information

Sample Name:	27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe
Analysis ID:	534009
MD5:	49ecf401f61b285..
SHA1:	ab62be12fe61804.
SHA256:	27eeb225876a78..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

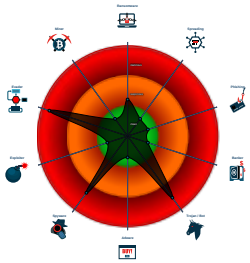


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- 27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe (PID: 3892 cmdline: "C:\Users\user\Desktop\27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe" MD5: 49ECF401F61B2856944B0603C2B56D3B)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "qucaiaregi.xyz:80"
  ],
  "Bot Id": "phoenix888"
}
```


Yara Overview

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
00000000.00000002.335006784.00000000022A0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.335058089.00000000022F5000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.278919255.000000000070D000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.335358845.00000000025B0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe PID: 3892	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.22a0000.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.25b0000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.2336246.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.233535e.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.2336246.5.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Performs DNS queries to domains with low reputation

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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)

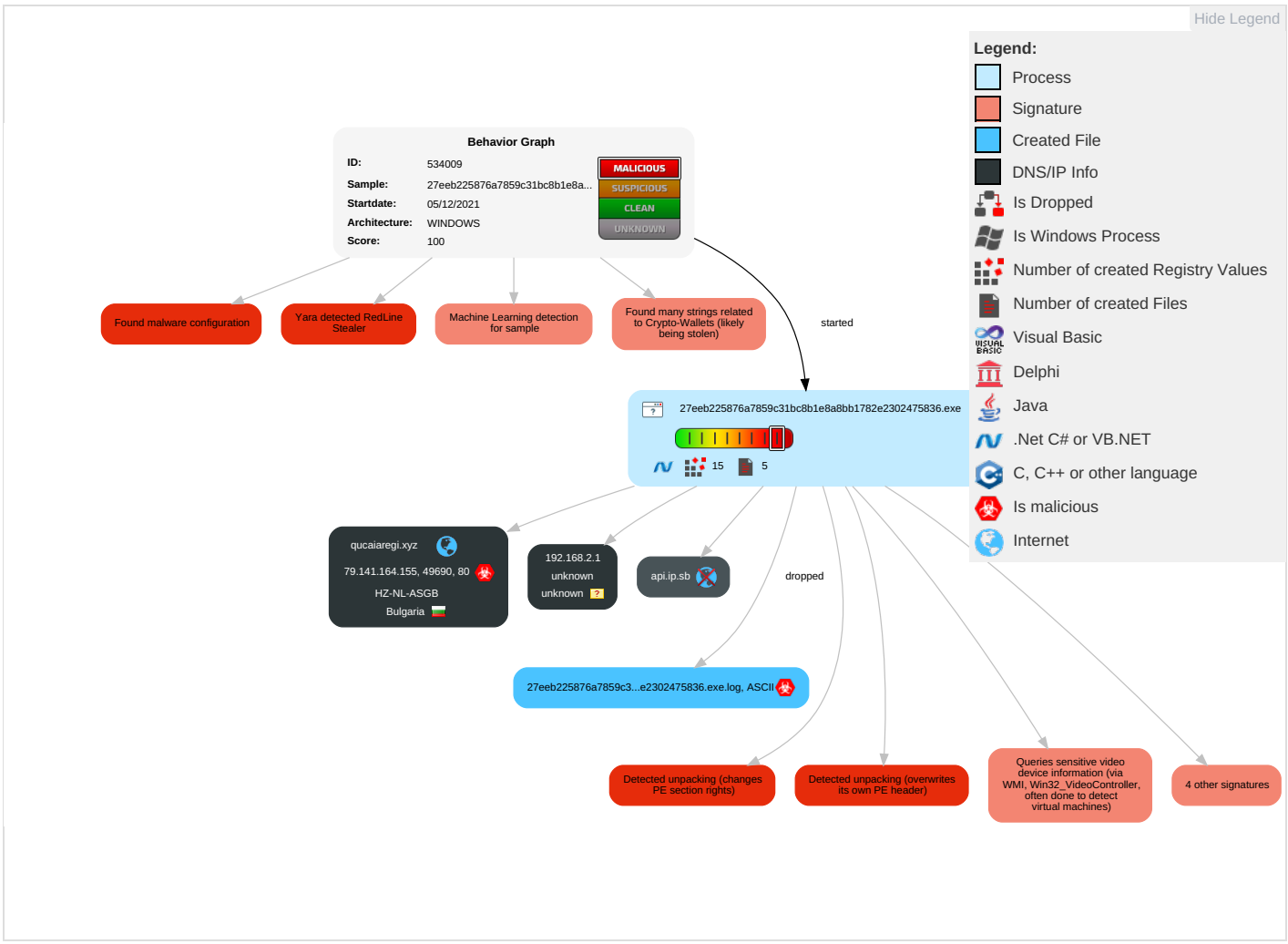
Remote Access Functionality:

- 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	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 6 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Explo Redire Calls/
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

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
27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api.ip.sb	4%	Virustotal		Browse

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	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	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/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://tempuri.org/Entity/Id15Response	0%	URL Reputation	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	
http://tempuri.org/Entity/Id4$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
qucaiaregi.xyz	79.141.164.155	true	true		unknown
api.ip.sb	unknown	unknown	false	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.141.164.155	qucaiaregi.xyz	Bulgaria		59711	HZ-NL-ASGB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	534009
Start date:	05.12.2021
Start time:	00:07:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.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:	11
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:	mal100.troj.spyw.evad.winEXE@1/1@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.9% (good quality ratio 4.8%) • Quality average: 84.3% • Quality standard deviation: 22.5%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:08:46	API Interceptor	24x Sleep call for process: 27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.141.164.155	780426DE24AE46F300FDAF9CBF597C8F2164F7B6C525C.exe	Get hash	malicious	Browse	
	C7304FF0966068D305DA031F9DA60C5B0EBE32AC43533.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HZ-NL-ASGB	780426DE24AE46F300FDAF9CBF597C8F2164F7B6C525C.exe	Get hash	malicious	Browse	• 79.141.164.155
	C7304FF0966068D305DA031F9DA60C5B0EBE32AC43533.exe	Get hash	malicious	Browse	• 79.141.164.155
	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	• 185.81.114.236
	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	• 185.81.114.236
	oX9UlQRaDf.dll	Get hash	malicious	Browse	• 185.117.90.36
	cc.dll	Get hash	malicious	Browse	• 185.117.90.36
	K5x2LIknQD.exe	Get hash	malicious	Browse	• 185.117.91.185
	hRZL5MN3p8.exe	Get hash	malicious	Browse	• 185.117.90.160
	4xH55rOtY7.exe	Get hash	malicious	Browse	• 185.117.91.185
	FWZr1TTo1W.dll	Get hash	malicious	Browse	• 185.117.90.36
	nrtZJ3frAY.dll	Get hash	malicious	Browse	• 185.117.90.36
	8zXDoUWw7l.dll	Get hash	malicious	Browse	• 185.117.90.36
	CheatValorant2.2.exe	Get hash	malicious	Browse	• 185.117.90.160
	fw7PVFc7bj.exe	Get hash	malicious	Browse	• 185.117.90.160
	SK9Nbi13Pv.exe	Get hash	malicious	Browse	• 185.117.90.160
	cFWMsY5Bz4.exe	Get hash	malicious	Browse	• 185.117.90.160
	BPzwq281b0.dll	Get hash	malicious	Browse	• 185.117.90.36
	TwmqQopC6l.dll	Get hash	malicious	Browse	• 185.117.90.36
	u2uI3z69bi.dll	Get hash	malicious	Browse	• 185.117.90.36
	HQoFEwbdKc.exe	Get hash	malicious	Browse	• 185.117.90.160

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe.log	
Process:	C:\Users\user\Desktop\27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHqHAHDJn:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbq8
MD5:	E7F4D63BCB0E635AA90D08AD1691969B
SHA1:	C7FECA489FACAE8FDBDCEC321B875DB94B01B69D
SHA-256:	AADCCE26CE71D0A90BD3824C4F5AB49EF0CF27BF02FC6BEE46BAC821EF409A50
SHA-512:	86DF01EB5E04A01414B984FB17EE418C1FB9283096555763BAE29BEEAE8946A27BB0AF585B2B29092249EA200CD9B9C4E8AB2EDA118D9CAD21CE514DB6FEA752
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.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\b219d4630d26b88041b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.1005523243193895
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe
File size:	421888
MD5:	49ecf401f61b2856944b0603c2b56d3b
SHA1:	ab62be12fe61804f272d13bc9e3336daa23b06dd
SHA256:	27eeb225876a7859c31bc8b1e8a8bb1782e2302475836b4a4ba127983a7a2b91
SHA512:	4ab28c6baf25403625194cd6cf5c352a4c3f9aed0c96787ef60d3f878be14b7f9c92c67d697216f76708839be8978424daed943d03ddd5cc3b09bb03a2ea4d68
SSDEEP:	6144:zVz3LKY3CcsOj7eX9AKIaaN3Q+ovCFv8XK5Nn3H/2xrVP9:zVDm3SeX9Rlj4CygH/2xp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.kD!...!.....?...;...?.....?.....n~.&...!.....?... ...?... ...?... ...Rich!.....PE..L...1..._.....b.

File Icon

Icon Hash:	dab1e4c4e4b9c7b8

Static PE Info

General

Entrypoint:	0x40373d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F81F631 [Sat Oct 10 17:58:09 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ace494ecc2c2c2c7ecf836ae6aa78574

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x560bd	0x56200	False	0.769466051343	data	7.58088224522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x58000	0x4934	0x4a00	False	0.375263935811	data	5.33760982074	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x5d000	0xe5c8	0xa400	False	0.0572599085366	data	0.737734182218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rojira	0x6c000	0x241	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6d000	0x1740	0x1800	False	0.68115234375	data	5.86467035041	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
Nepali	Nepal	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/05/21-00:08:44.385890	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49690	80	192.168.2.3	79.141.164.155

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2021 00:08:31.950422049 CET	192.168.2.3	8.8.8.8	0x9245	Standard query (0)	qucaiaregi.xyz	A (IP address)	IN (0x0001)
Dec 5, 2021 00:08:40.144551039 CET	192.168.2.3	8.8.8.8	0xf800	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Dec 5, 2021 00:08:40.184057951 CET	192.168.2.3	8.8.8.8	0x79c5	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2021 00:08:31.971618891 CET	8.8.8.8	192.168.2.3	0x9245	No error (0)	qucaiaregi.xyz		79.141.164.155	A (IP address)	IN (0x0001)
Dec 5, 2021 00:08:40.168299913 CET	8.8.8.8	192.168.2.3	0xf800	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2021 00:08:40.207129955 CET	8.8.8.8	192.168.2.3	0x79c5	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: 27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe PID: 3892 Parent PID: 3428

General

Start time:	00:08:21
Start date:	05/12/2021
Path:	C:\Users\user\Desktop\27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\27eeb225876a7859c31bc8b1e8a8bb1782e2302475836.exe"
Imagebase:	0x400000
File size:	421888 bytes
MD5 hash:	49ECF401F61B2856944B0603C2B56D3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.335006784.00000000022A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.335058089.00000000022F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.278919255.000000000070D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.335358845.00000000025B0000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis