JOeSandbox Cloud BASIC

ID: 546175
Sample Name: 2s8Gnp8xe2
Cookbook: default.jbs
Time: 08:10:10
Date: 29/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report 2s8Gnp8xe2

Overview

General Information

Sample Name:	2s8Gnp8xe2 (renamed file extension from none to exe)
Analysis ID:	546175
MD5:	1a8620af98d68f9..
SHA1:	1a39e1f41e89d55.
SHA256:	f593cd3e0a4ad34.
Tags:	32 exe trojan
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…

Is looking for software installed on th…

Uses 32bit PE files

Found a high number of Window / Us…

Queries the volume information (nam…

Classification
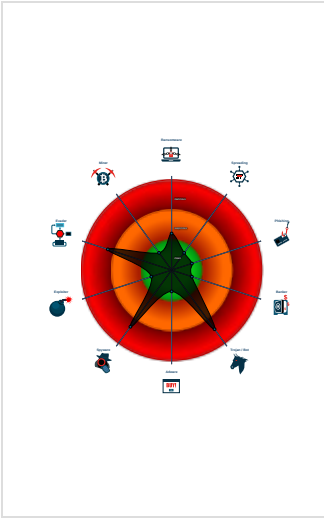
Process Tree

- **System is w10x64**
  - 2s8Gnp8xe2.exe (PID: 5936 cmdline: "C:\Users\user\Desktop\2s8Gnp8xe2.exe" MD5: 1A8620AF98D68F9CADB5916341AD1E71)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "188.119.112.82:28198"
  ],
  "Bot Id": "x0999123",
  "Message": ""
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
2s8Gnp8xe2.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
00000001.00000000.272540023.0000000000940 2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.321954678.0000000000940 2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.324131569.00000000031E 7000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: 2s8Gnp8xe2.exe PID: 5936	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.2s8Gnp8xe2.exe.940000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.0.2s8Gnp8xe2.exe.940000.0.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)
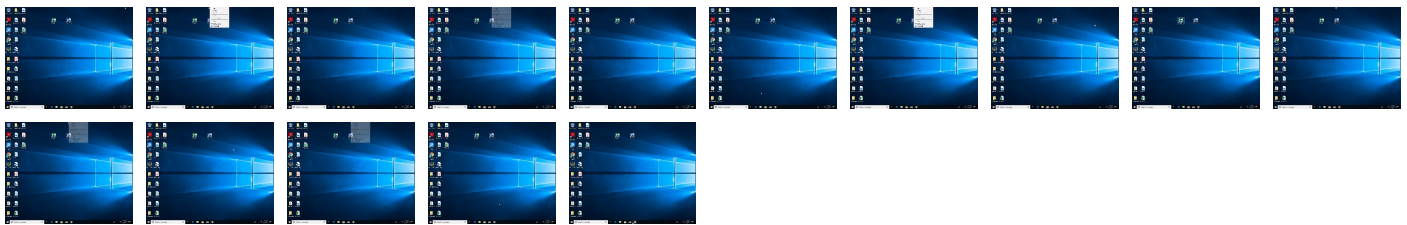
Remote Access Functionality:

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commur
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	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	Steganography	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur

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
2s8Gnp8xe2.exe	46%	Virustotal		Browse
2s8Gnp8xe2.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.Lazy	

Dropped Files

No Antivirus matches

Unpacked PE Files

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/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/Id46a	0%	Avira URL Cloud	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
188.119.112.82	unknown	Russian Federation		50673	SERVERIUS-ASNL	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546175
Start date:	29.12.2021
Start time:	08:10:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2s8Gnp8xe2 (renamed file extension from none 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:	23
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:	mal92.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	Failed
HDC Information:	- Successful, ratio: 0.2% (good quality ratio 0.1%) - Quality average: 24.2% - Quality standard deviation: 35.4%
HCA Information:	- Successful, ratio: 99% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:11:21	API Interceptor	12x Sleep call for process: 2s8Gnp8xe2.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\2s8Gnp8xe2.exe.log	
Process:	C:\Users\user\Desktop\2s8Gnp8xe2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHjHKdHAHDJn:vq5qXAqLqdqUqzcGYqhQnoPtIxHbqoL1
MD5:	B8B968C6C5994E11C0AEF299F6CC13DF
SHA1:	60351148A0D29E39DF51AE7F8D6DA7653E31BCF9
SHA-256:	DD53198266985E5C23239DCDDE91B25CF1FC1F4266B239533C11DDF0EF0F958D
SHA-512:	CFBCFCB650EF8C84A4BA005404E90ECAC9E77BDB618F53CD5948C085E44D099183C97C1D818A905B16C5E495FF167BD47347B14670A6E68801B0C01BC264F1(
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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.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\b219d4630d26b88041b59c21e8e2b95c\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):		5.892677990184514
TrID:		• 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:		2s8Gnp8xe2.exe
File size:		115712
MD5:		1a8620af98d68f9cadb5916341ad1e71
SHA1:		1a39e1f41e89d552bd1228f7dd79e553a8dbb22e
SHA256:		f593cd3e0a4ad34d16b48b9cdd344e486b42fbfc5bca0c25abb75b6cc03ac2d0
SHA512:		0824ade76adc9c5f6120775ce89d6e3b64d5814683dffa39adeab2a90131a7cf1d3be0a72546c0afeeb2fd72a510639a64fc37ef23dea8baeb9dbbc9c3b38de6
SSDEEP:		1536:9UVr85RhYuBGHDp8j468w4d8WD7u7HXhbYpfwxBRFovsSw00IniD:9UVwfUHD2868tiW0JX5BFsiD

General

File Content Preview:	MZ....................@...............................!..L.!Th is program cannot be run in DOS mode....$.......PE..L...g n...............0......0........... ....@.. ....@.............................

File Icon

Icon Hash:	a2a32b218bb8f08c

Static PE Info

General

Entrypoint:	0x4191ba
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:	0xE3096E67 [Thu Sep 14 04:21:59 2090 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	0x18d90	0x19000	False	0.4332421875	data	5.87898568602	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x2b24	0x2c00	False	0.313121448864	data	5.71292062675	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x400	False	0.025390625	data	0.0558553080537	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_DISCARDABL E, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: 2s8Gnp8xe2.exe PID: 5936 Parent PID: 6108

General

Start time:	08:10:59
Start date:	29/12/2021
Path:	C:\Users\user\Desktop\2s8Gnp8xe2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2s8Gnp8xe2.exe"
Imagebase:	0x940000
File size:	115712 bytes
MD5 hash:	1A8620AF98D68F9CADB5916341AD1E71
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: 00000001.00000000.272540023.0000000000942000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.321954678.0000000000942000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.324131569.00000000031E7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities   Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis