ID: 492126
Sample Name: sb.exe
Cookbook: default.jbs
Time: 11:48:03
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

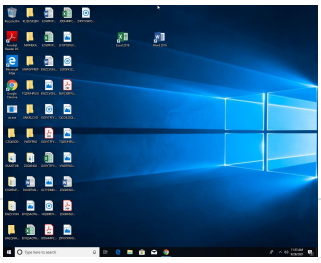
Windows Analysis Report sb.exe

Overview

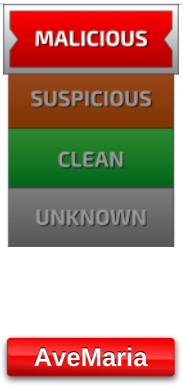
General Information

Sample Name:	sb.exe
Analysis ID:	492126
MD5:	e310cb3185d95e..
SHA1:	c20c8aa953f7df7..
SHA256:	82867648313483..
Tags:	arostetelemacca exe
Infos:	

Most interesting Screenshot:



Detection

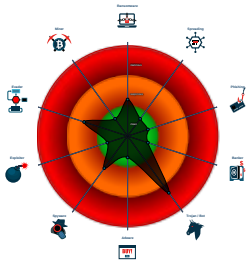


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected AveMaria stealer
- C2 URLs / IPs found in malware con…
- Contains functionality to hide user a…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- Installs a raw input device (often for …
- Contains functionality to check if a d…
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- sb.exe (PID: 6404 cmdline: 'C:\Users\user\Desktop\sb.exe' MD5: E310CB3185D95E3DDA42F0230B569D84)
  - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "cachepallioniwarznpa.icu",
  "port": 5200
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.374825576.00000000031F6000.00000002.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.374825576.00000000031F6000.00000002.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000000.00000002.374727716.00000000027E0000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.374727716.00000000027E0000.00000040.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
Process Memory Space: sb.exe PID: 6404	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.sb.exe.27e053f.1.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x16478:$a1: \Opera Software\Opera Stable\Login Data • 0x167a0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x160e8:$a3: \Google\Chrome\User Data\Default\Login Data
0.2.sb.exe.27e053f.1.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.sb.exe.27e053f.1.raw.unpack	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
0.2.sb.exe.27e053f.1.raw.unpack	AveMaria_WarZone	unknown	unknown	• 0x18520:$str1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x18274:$str2: MsgBox.exe • 0x18148:$str6: Ave_Maria • 0x177e8:$str7: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList • 0x16e08:$str8: SMTP Password • 0x160e8:$str11: \Google\Chrome\User Data\Default\Login Data • 0x177c0:$str12: \sqlmap.dll
0.2.sb.exe.27e053f.1.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x15878:$a1: \Opera Software\Opera Stable\Login Data • 0x15ba0:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x154e8:$a3: \Google\Chrome\User Data\Default\Login Data
Click to see the 7 entries				

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

Yara detected AveMaria stealer

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected AveMaria stealer

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

Stealing of Sensitive Information:

Yara detected AveMaria stealer

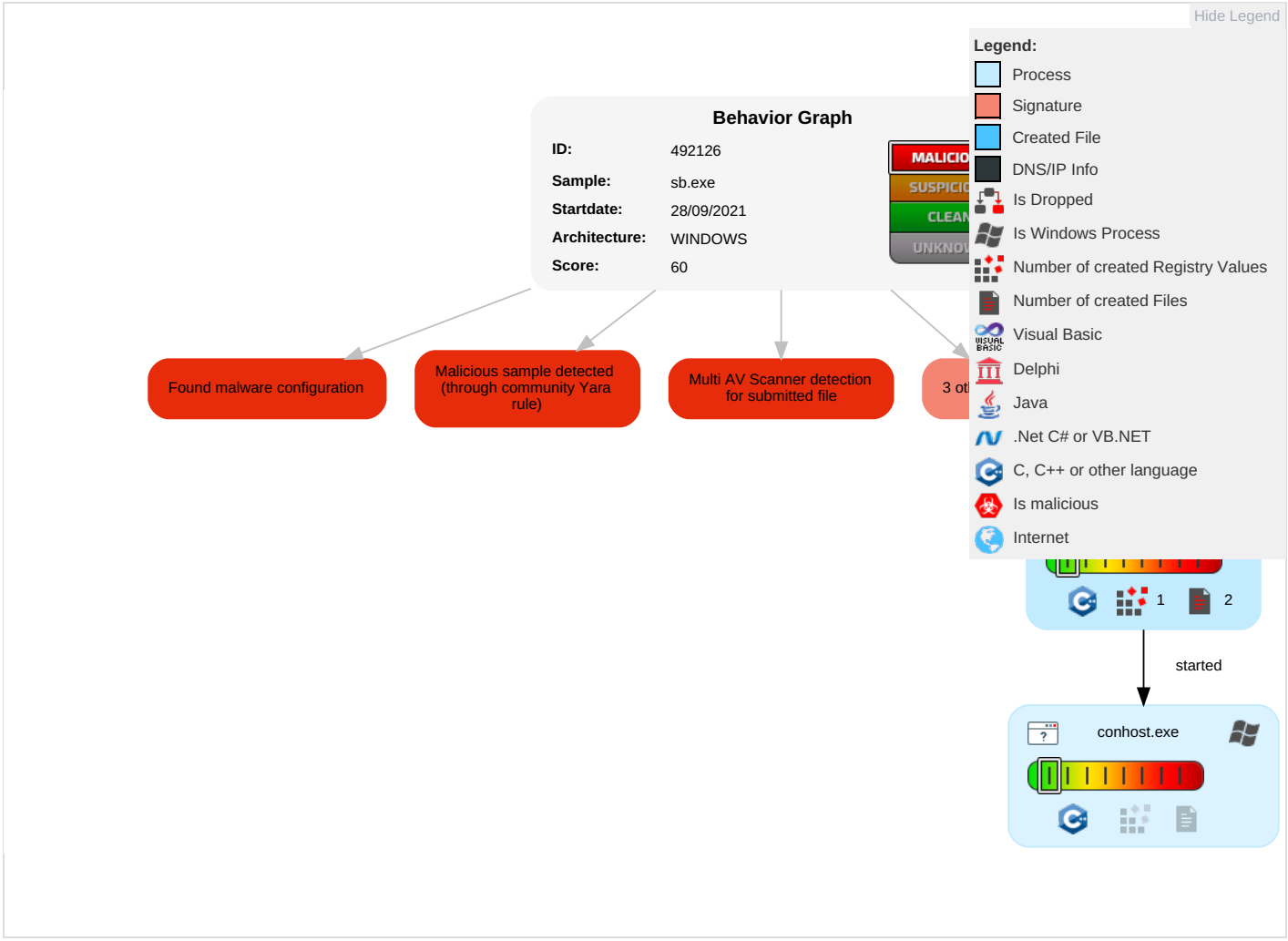
Remote Access Functionality:

Yara detected AveMaria 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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 2	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Information Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Users 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

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
sb.exe	38%	Virustotal		Browse
sb.exe	42%	ReversingLabs	Win32.Trojan.Streamer	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.sb.exe.31e0000.3.unpack	100%	Avira	TR/Downloader.Gen		Download File
0.2.sb.exe.27e053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
cachepallioniwarznpa.icu	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
cachepallioniwarznpa.icu	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cachepallioniwarznpa.icu	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492126
Start date:	28.09.2021
Start time:	11:48:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sb.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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.winEXE@2/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 91.8%) • Quality average: 76% • Quality standard deviation: 30.9%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
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 (console) Intel 80386, for MS Windows
Entropy (8bit):	3.7813426384094133
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:	sb.exe
File size:	1627136
MD5:	e310cb3185d95e3dda42f0230b569d84
SHA1:	c20c8aa953f7df7e9b117258a0d31530e23ffc55

General

SHA256:	82867648313483db4a6115e0cc2b34c06719ffdb6667e5(e625e2dc130adfbca
SHA512:	a0c4a70bc09ea2eb36a1a27af65891d866beec07a1c212 08e0b05e549d3d2f7619bef9012dab9e121e53a6a1a56d(42bfb5435520292dd879e30f4db71789bbd
SSDEEP:	12288:EjTG/NEiKx8FAuRg7Q7X/CRLL6/mkIHTydNNA F4B0laLpfqFR:EiAuRg7SFWlyFR
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$..... .....a.....r...T.....T.+..... T.....Rich.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40eb3e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6147C4FD [Sun Sep 19 23:17:17 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	9d3536f958f133fe568939841471fa60

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 9/7/2021 5:00:00 PM 9/8/2022 4:59:59 PM
Subject Chain	• CN=SAN MARINO INVESTMENTS PTY LTD, O=SAN MARINO INVESTMENTS PTY LTD, S=Victoria, C=AU
Version:	3
Thumbprint MD5:	5F47B0139E6B49D14882A7ABD4026C5A
Thumbprint SHA-1:	D877BC4EA5A61864AA45BCB3F7EBDCD8ACBC5D5D
Thumbprint SHA-256:	72A2371C9873A8CF56E98A6EACB267DEC076593AC0A6917DC10B479F19B9EA6F
Serial:	00D79739187C585E453C00AFC11D77B523

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4c3fa	0x4c400	False	0.454738729508	data	6.61929420007	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4e000	0x107c4	0x10800	False	0.418604995265	data	5.4012865504	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	0x5f000	0x12b554	0x12a200	False	0.175606001048	data	2.35283899818	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18b000	0x1e0	0x200	False	0.53125	data	4.71229819329	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x18c000	0x3914	0x3a00	False	0.747306034483	data	6.62483061725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: sb.exe PID: 6404 Parent PID: 4560

General

Start time:	11:49:08
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\sb.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\sb.exe'
Imagebase:	0xcb0000
File size:	1627136 bytes

MD5 hash:	E310CB3185D95E3DDA42F0230B569D84
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.374825576.00000000031F6000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.374825576.00000000031F6000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.374727716.00000000027E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.374727716.00000000027E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6408 Parent PID: 6404

General

Start time:	11:49:09
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis