ID: 551503
Sample Name: J5RBhmpBtw
Cookbook:
defaultmacfilecookbook.jbs
Time: 09:23:51
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

macOS Analysis Report J5RBhmpBtw

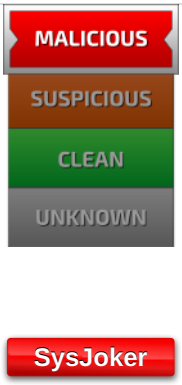
Overview

General Information

Sample Name:	J5RBhmpBtw
Analysis ID:	551503
MD5:	e06e06752509f9c.
SHA1:	554aef8bf44e7fa…
SHA256:	1a9a5c797777f37.
Infos:	

Most interesting Screenshot:

Detection

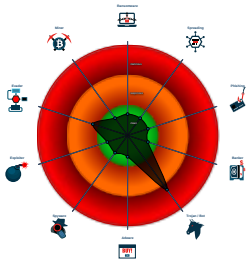


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Yara detected SysJoker
- Executes commands using a shell c…
- Reads the systems hostname

Classification



Analysis Advice

Exit code suggests that the sample could not be started, try looking at standard streams or writes to anonymous pipes for possible reason

Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551503
Start date:	12.01.2022
Start time:	09:23:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	J5RBhmpBtw
Cookbook file name:	defaultmacfilecookbook.jbs
Analysis system description:	Virtual Machine, High Sierra (Office 2016 16.16, Java 11.0.2+9, Adobe Reader 2019.010.20099)
Analysis Mode:	default
Detection:	MAL
Classification:	mal56.troj.mac@0/0@0/0
Warnings:	Show All

Process Tree

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 829, Parent: 753)
  - J5RBhmpBtw (MD5: e06e06752509f9cd8bc85aa1aa24dba2) Arguments: /Users/berri/Desktop/J5RBhmpBtw
    - sh New Fork (PID: 830, Parent: 829)
      - whoami (MD5: 24c45eb23e1aae68c572939d1a906018) Arguments: whoami
- **cleanup**

Copyright Joe Security LLC 2022

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
J5RBhmpBtw	JoeSecurity_SysJoker	Yara detected SysJoker	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000829.00000279.1.000000010409b000.00000001040b3000.r-x.sdmp	JoeSecurity_SysJoker	Yara detected SysJoker	Joe Security	
Process Memory Space: J5RBhmpBtw PID: 829	JoeSecurity_SysJoker	Yara detected SysJoker	Joe Security	

Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Stealing of Sensitive Information:

Yara detected SysJoker

Remote Access Functionality:

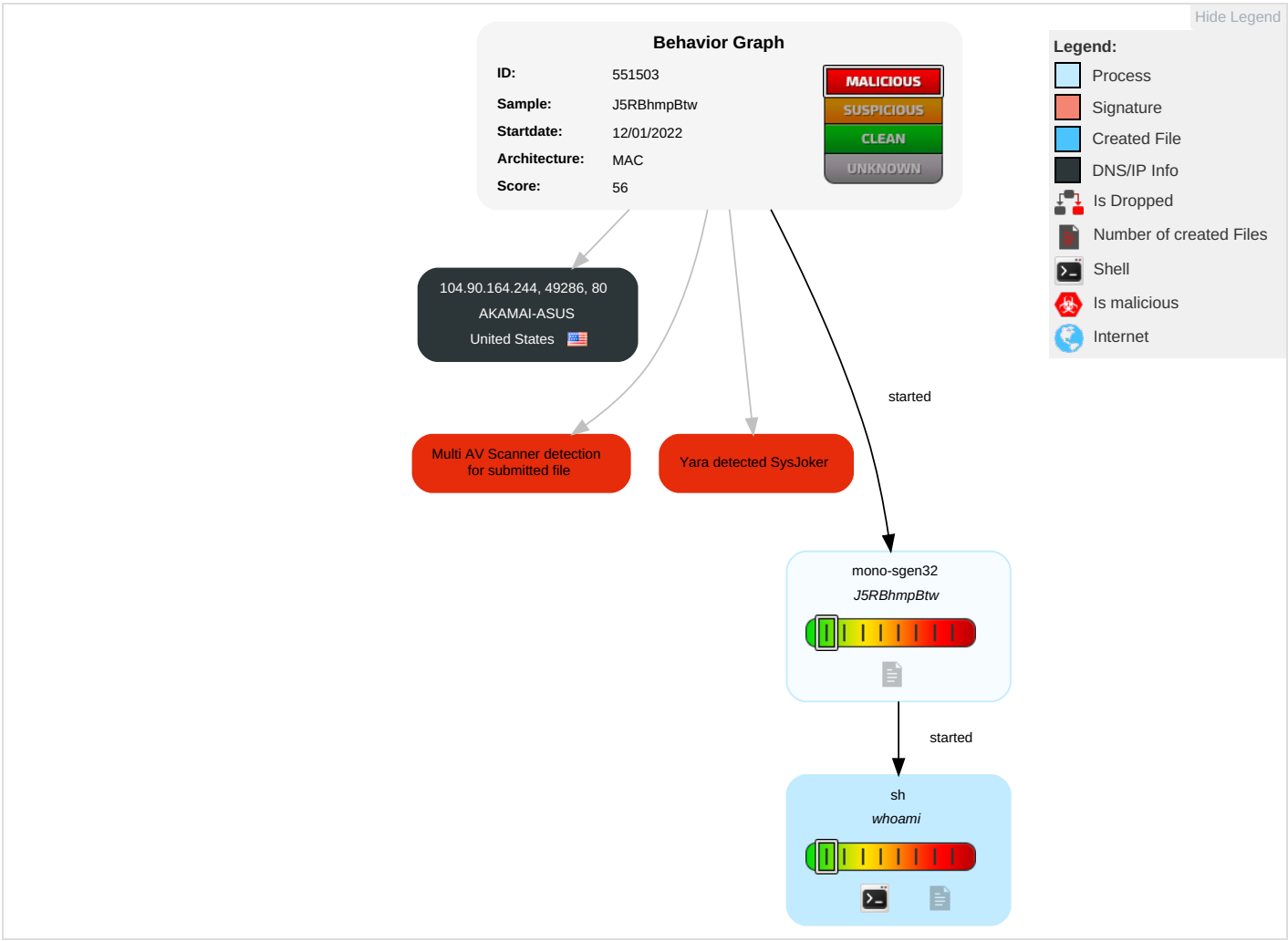
Yara detected SysJoker

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Path Interception	Path Interception	Scripting 1	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

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
J5RBhmpBtw	17%	Virustotal		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
J5RBhmpBtw	14%	ReversingLabs	MacOS.Backdoor.SysJoke	

Dropped Files

No Ant

Domains

No Ant

URLs

No Ant

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.90.164.244	unknown	United States		16625	AKAMAI-ASUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

Copyright Joe Security LLC 2022

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Runtime Messages

Command:	/Users/berri/Desktop/J5RBhmpBtw
Exit Code:	134
Exit Code Info:	SIGABRT (6) Abort signal from abort
Killed:	False
Standard Output:	
Standard Error:	dyld: lazy symbol binding failed: Symbol not found: __ZNSt3__14__fs10filesystem8__statusERKNS1_4pathEPNS_10error_codeE Referenced from: /Users/berri/Desktop/J5RBhmpBtw (which was built for Mac OS X 11.3) Expected in: /usr/lib/libc++.1.dylib dyld: Symbol not found: __ZNSt3__14__fs10filesystem8__statusERKNS1_4pathEPNS_10error_codeE Referenced from: /Users/berri/Desktop/J5RBhmpBtw (which was built for Mac OS X 11.3) Expected in: /usr/lib/libc++.1.dylib

Created / dropped Files

No created / dropped files found

Static File Info

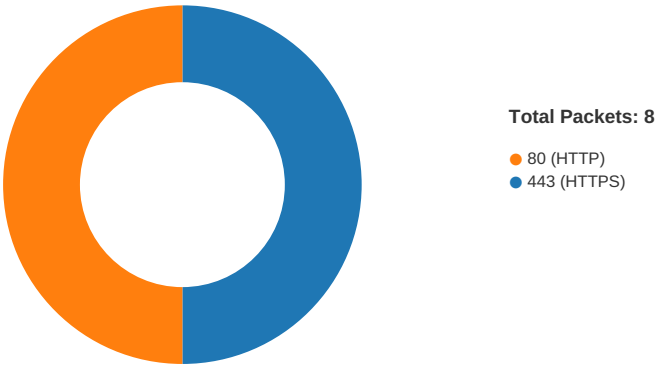
General

File type:	Mach-O universal binary with 2 architectures: [x86_64:Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>] [arm64:Mach-O 64-bit arm64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>]
Entropy (8bit):	4.67371613955121
TrID:	• Mac OS X Universal Binary executable (4004/1) 75.96% • HSC music composer song (1267/141) 24.04%
File name:	J5RBhmpBtw
File size:	360176
MD5:	e06e06752509f9cd8bc85aa1aa24dba2
SHA1:	554aef8bf44e7fa941e1190e41c8770e90f07254
SHA256:	1a9a5c797777f37463b44de2b49a7f95abca786db3977dcdac0f79da739c08ac
SHA512:	78a210c5fd1ac8c601fbb4ed226e7aaf1cc5bda187807ba3020997862fd54b59081f0b7f4fdc720acfa8e3d6a35dbe9309e0b2fe38088f493a02717a1057a56e
SSDEEP:	6144:5xw19koSAgvRyrnN5ft9A7pIHWhT5FixbxLZ:CvgMrnN51qaH+T5wl
File Content Preview:	.....@.....~..... ....

Static Mach Info

Network Behavior

Network Port Distribution



TCP Packets

UDP Packets

System Behavior

Analysis Process: mono-sgen32 PID: 829 Parent PID: 753

General

Start time:	09:24:44
Start date:	12/01/2022
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32
Arguments:	n/a
File size:	3722408 bytes
MD5 hash:	8910349f44a940d8d79318367855b236

Analysis Process: J5RBhmpBtw PID: 829 Parent PID: 753

General

Start time:	09:24:44
Start date:	12/01/2022
Path:	/Users/berri/Desktop/J5RBhmpBtw
Arguments:	/Users/berri/Desktop/J5RBhmpBtw
File size:	360176 bytes
MD5 hash:	e06e06752509f9cd8bc85aa1aa24dba2

Analysis Process: sh PID: 830 Parent PID: 829

General

Start time:	09:24:44

Copyright Joe Security LLC 2022

Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

Analysis Process: whoami PID: 830 Parent PID: 829

General

Start time:	09:24:44
Start date:	12/01/2022
Path:	/usr/bin/whoami
Arguments:	whoami
File size:	23248 bytes
MD5 hash:	24c45eb23e1aae68c572939d1a906018

File Activities

File Read

Copyright Joe Security LLC 2022