ID: 286
Sample Name: vpnkit-bridge
Cookbook:
defaultmacfilecookbook.jbs
Time: 12:33:41
Date: 08/02/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report vpnkit-bridge

Overview

General Information

Sample Name:	vpnkit-bridge
Analysis ID:	286
MD5:	97149225b26798..
SHA1:	3bc07891356fbde.
SHA256:	04fb8fb364cd2da..

Most interesting Screenshot:

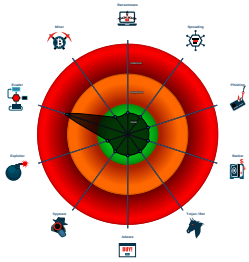
Detection

Score:	22
Range:	0 - 100
Whitelisted:	false

Signatures

- Contains symbols with suspicious n…
- Contains symbols with paths
- Contains symbols with suspicious n…
- Contains symbols with suspicious n…
- Reads hardware related sysctl values

Classification



Startup

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 570, Parent: 493)
  - vpnkit-bridge (MD5: 97149225b26798a9c2e958ff722c7df3) Arguments: /Users/berri/Desktop/vpnkit-bridge
- **cleanup**

Yara Overview

No yara matches

Signature Overview

- Cryptography
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Malware Analysis System Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

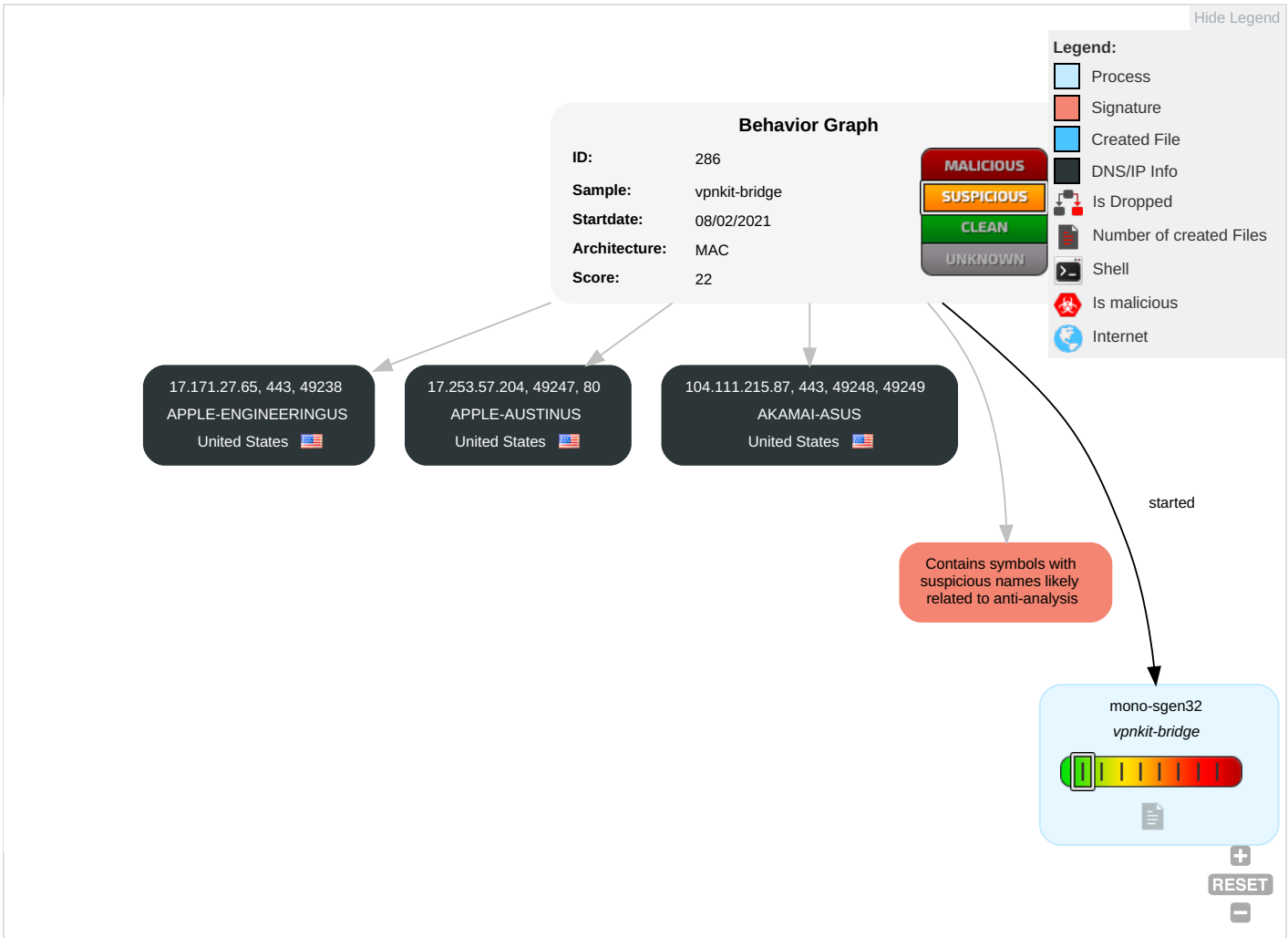
Malware Analysis System Evasion:

Contains symbols with suspicious names likely related to anti-analysis

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track De Without Authoriza
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Dat Without Authoriza

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
vpnkit-bridge	0%	Virustotal		Browse
vpnkit-bridge	0%	Metadefender		Browse
vpnkit-bridge	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

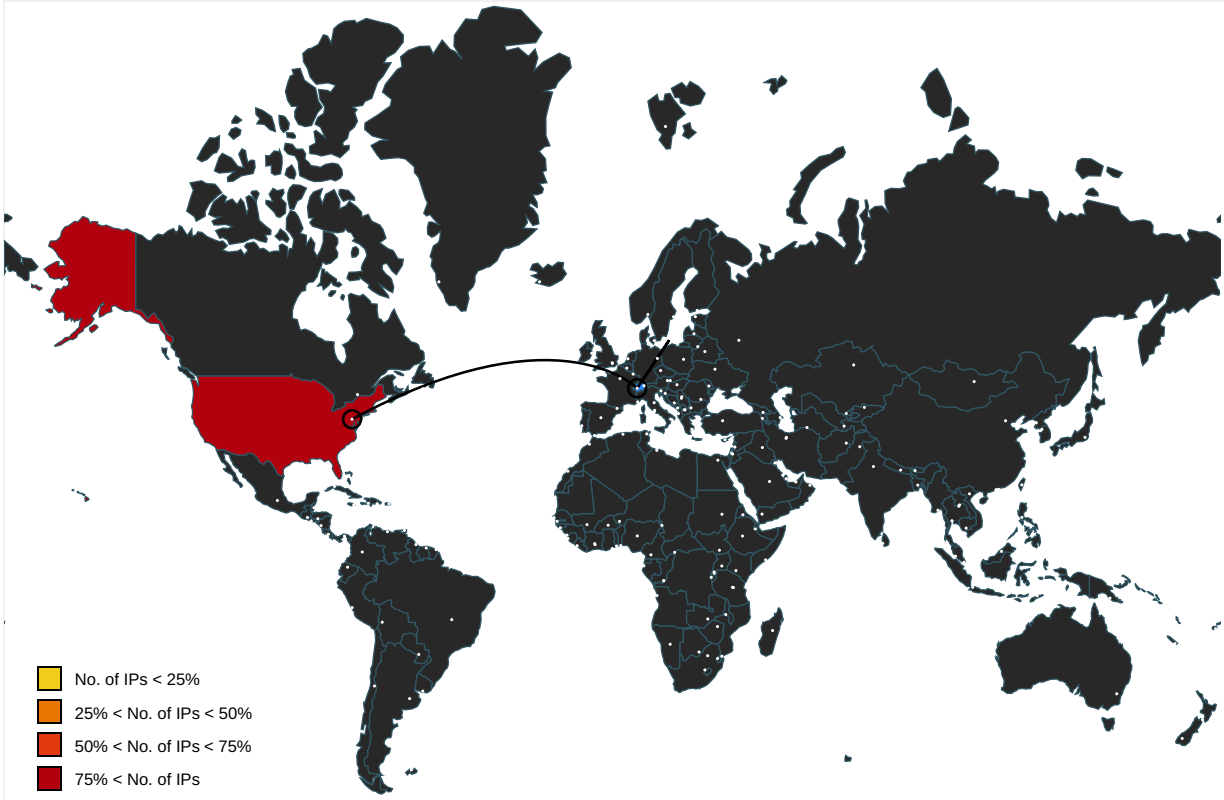
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
17.253.57.204	unknown	United States		6185	APPLE-AUSTINUS	false
17.171.27.65	unknown	United States		714	APPLE-ENGINEERINGUS	false
104.111.215.87	unknown	United States		16625	AKAMAI-ASUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	286
Start date:	08.02.2021
Start time:	12:33:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vpnkit-bridge
Cookbook file name:	defaultmacfilecookbook.jbs
Analysis system description:	Virtual Machine, High Sierra (Office 2016 v16.16, Java 11.0.2+9, Adobe Reader 2019.010.20099)
Analysis Mode:	default
Detection:	SUS
Classification:	sus22.evad.mac@0/0@0/0
Warnings:	Show All

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
17.253.57.204	bc20	Get hash	malicious	Browse	
	GPT.dmg	Get hash	malicious	Browse	
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	
	yz1D8IY8l2.bin	Get hash	malicious	Browse	
	4MTr61Qr8q	Get hash	malicious	Browse	
	flashInstaller copy.dmg	Get hash	malicious	Browse	
	dialog-ee-x-2.8.1.493.dmg	Get hash	malicious	Browse	
	Player.dmg	Get hash	malicious	Browse	
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	
17.171.27.65	bc20	Get hash	malicious	Browse	
	p	Get hash	malicious	Browse	
	in3.dmg	Get hash	malicious	Browse	
	http://https://billychemr324.github.io/santipxzic/index1.html?bbre=aod9435	Get hash	malicious	Browse	
	dialog-ee-x-2.8.1.493.dmg	Get hash	malicious	Browse	
	install.dmg	Get hash	malicious	Browse	
	Player.dmg	Get hash	malicious	Browse	
	http://help-servicee.ml	Get hash	malicious	Browse	
	http://owauth1tadsoh1itndereql1nysa1ier1rnrhnthaesinlp.us-east-2.elasticbeanstalk.com/#jdiaz@eversheds-sutherland.es	Get hash	malicious	Browse	
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	
	prescribe ,12.20.doc	Get hash	malicious	Browse	
	http://protesidenext.com/16dbc8c14acdb8703b.js	Get hash	malicious	Browse	
104.111.215.87	bc20	Get hash	malicious	Browse	
	Alfred_4.3.1_1214 (1).dmg	Get hash	malicious	Browse	
	GPT.dmg	Get hash	malicious	Browse	
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	
	yz1D8IY8l2.bin	Get hash	malicious	Browse	
	Installer.dmg	Get hash	malicious	Browse	
	oSolGjJEjL	Get hash	malicious	Browse	
	4MTr61Qr8q	Get hash	malicious	Browse	
	PAYMENT.dmg	Get hash	malicious	Browse	
	ExtendedSprint.service	Get hash	malicious	Browse	
	p	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
APPLE-ENGINEERINGUS	mozi.a.zip	Get hash	malicious	Browse	• 17.73.154.133
	bc20	Get hash	malicious	Browse	• 17.171.27.65
	p	Get hash	malicious	Browse	• 17.171.27.65
	xSf	Get hash	malicious	Browse	• 17.149.240.70
	Alfred_4.3.1_1214 (1).dmg	Get hash	malicious	Browse	• 17.149.240.70
	GPT.dmg	Get hash	malicious	Browse	• 17.149.240.70
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 17.209.148.6
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 17.149.240.70
	yz1D8IY8l2.bin	Get hash	malicious	Browse	• 17.149.240.70
	Installer.dmg	Get hash	malicious	Browse	• 17.149.240.70
	4MTr61Qr8q	Get hash	malicious	Browse	• 17.149.240.70
	fil1	Get hash	malicious	Browse	• 17.173.212.16
	PAYMENT.dmg	Get hash	malicious	Browse	• 17.149.240.70
	ExtendedSprint.service	Get hash	malicious	Browse	• 17.149.240.70
	p	Get hash	malicious	Browse	• 17.149.240.70
	i	Get hash	malicious	Browse	• 17.120.249.110
	REP er0005147.doc	Get hash	malicious	Browse	• 17.149.240.70
	svchost.exe	Get hash	malicious	Browse	• 17.48.42.214

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BetterTouchTool.zip	Get hash	malicious	Browse	• 17.149.240.70
	Alfred_4.3_1205.dmg	Get hash	malicious	Browse	• 17.149.240.70
APPLE-AUSTINUS	bc20	Get hash	malicious	Browse	• 17.253.57.204
	p	Get hash	malicious	Browse	• 17.253.55.203
	xSf	Get hash	malicious	Browse	• 17.253.55.205
	Alfred_4.3.1_1214 (1).dmg	Get hash	malicious	Browse	• 17.253.57.203
	GPT.dmg	Get hash	malicious	Browse	• 17.253.57.204
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 17.253.57.204
	yz1D8IY8l2.bin	Get hash	malicious	Browse	• 17.253.57.204
	Installer.dmg	Get hash	malicious	Browse	• 17.253.57.208
	oSolGjJEjL	Get hash	malicious	Browse	• 17.253.55.203
	4MTr61Qr8q	Get hash	malicious	Browse	• 17.253.57.204
	PAYMENT.dmg	Get hash	malicious	Browse	• 17.253.57.208
	ExtendedSprint.service	Get hash	malicious	Browse	• 17.253.57.207
	p	Get hash	malicious	Browse	• 17.253.57.203
	REP er0005147.doc	Get hash	malicious	Browse	• 17.253.57.202
	BetterTouchTool.zip	Get hash	malicious	Browse	• 17.253.57.208
	Alfred_4.3_1205.dmg	Get hash	malicious	Browse	• 17.253.55.207
	http://https://among-modded.com/app.mobileconfig	Get hash	malicious	Browse	• 17.253.57.208
	my420.dmg	Get hash	malicious	Browse	• 17.253.57.203
	flashInstaller copy.dmg	Get hash	malicious	Browse	• 17.253.57.204
	in3.dmg	Get hash	malicious	Browse	• 17.253.57.208
AKAMAI-ASUS	Curriculo Laura Sperandio.xlsm	Get hash	malicious	Browse	• 92.122.33.192
	bc20	Get hash	malicious	Browse	• 104.111.215.87
	SecuriteInfo.com.Generic.mg.fc2ec506b712be50.dll	Get hash	malicious	Browse	• 2.18.68.31
	SecuriteInfo.com.Generic.mg.78deebcff2e21343.dll	Get hash	malicious	Browse	• 2.21.140.74
	Alfred_4.3.1_1214 (1).dmg	Get hash	malicious	Browse	• 104.111.215.87
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 23.210.249.140
	GPT.dmg	Get hash	malicious	Browse	• 104.111.215.87
	davay (2).exe	Get hash	malicious	Browse	• 23.49.13.33
	davay.exe	Get hash	malicious	Browse	• 23.49.13.33
	boom5.dll	Get hash	malicious	Browse	• 95.100.196.29
	mon22.dll	Get hash	malicious	Browse	• 95.100.196.29
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 23.56.220.205
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 104.111.215.87
	yz1D8IY8l2.bin	Get hash	malicious	Browse	• 104.111.215.87
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 104.79.90.110
	Mecca_Bingo_App_v1.8_www.9apps.com_.apk	Get hash	malicious	Browse	• 92.122.32.206
	Installer.dmg	Get hash	malicious	Browse	• 104.111.215.87
	oSolGjJEjL	Get hash	malicious	Browse	• 104.111.215.87
	4MTr61Qr8q	Get hash	malicious	Browse	• 104.111.215.87
	VFe7Yb7gUV.exe	Get hash	malicious	Browse	• 95.100.74.51

JA3 Fingerprints

No context

Dropped Files

No context

Runtime Messages

Command:	/Users/berri/Desktop/vpnkit-bridge
Exit Code:	0
Exit Code Info:	
Killed:	False

Standard Output:	Usage:
	  vpnkit-bridge [command]
	
	Available Commands:
	  guest Establish connection to the host and setup service bridges as the guest
	  help Help about any command
	  host Establish connection to the guest and setup service bridges as the host
	  kill Kill running instance of vpnkit-bridge
	
	Flags:
	  --addr string Can be connect://vmid/serviceid or listen://vmid/serviceid. On Windows IDs are Guids; on Unix they are integers
	  -h; --help help for vpnkit-bridge
	  --pid-file string file in which to put the pid
	  -v; --verbose Enable verbose mode
	  --wsl-distro string WSL distribution to run in
	
	Use 'vpnkit-bridge [command] --help' for more information about a command.

Standard Error:	

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL>
Entropy (8bit):	6.017802967361337
TrID:	• Mac OS X Mach-O 64bit Intel executable (20004/1) 100.00%
File name:	vpnkit-bridge
File size:	5435232
MD5:	97149225b26798a9c2e958ff722c7df3
SHA1:	3bc07891356fbded338d1ea881414327eac0f037
SHA256:	04fb8fb364cd2da2544b662d15853852d4b14a09981f3593cc1fdf1b2764d1f8
SHA512:	25289828a6fa5075ca3ea1924b61f5b0a9f6ed44229d3b454237836a0545e44880bc111e965171f2b28b4aff63d66624285b5de0c238908a0318b2858c4efbf3
SSDEEP:	49152:W+G/6IZcXQOvcXzBIbsrGqmm/B7zJVLPCoHYr4XyUm/UhswaqLv/8q2gSGXhOj5j:U37Qqme1VbCoOUmfwPvVSGxTgFlN
File Content Preview:	.....H...__PAGEZERO..... .....__TEXT.....PI..... PI.....__text.....__TEXT.....&.....5.!.....& .....

Static Mach Info

Network Behavior

Network Port Distribution

Total Packets: 13

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

UDP Packets

System Behavior

Analysis Process: mono-sgen32 PID: 570 Parent PID: 493

General

Start time:	12:34:32
Start date:	08/02/2021
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32
Arguments:	n/a
File size:	3722408 bytes
MD5 hash:	8910349f44a940d8d79318367855b236

Analysis Process: vpnkit-bridge PID: 570 Parent PID: 493

General

Start time:	12:34:33
Start date:	08/02/2021
Path:	/Users/berri/Desktop/vpnkit-bridge
Arguments:	/Users/berri/Desktop/vpnkit-bridge
File size:	5435232 bytes
MD5 hash:	97149225b26798a9c2e958ff722c7df3

File Activities

File Read