ID: 752914
Sample Name:
pwm_3.3.1.1_aarch64.dmg
Cookbook:
defaultmacfilecookbook.jbs
Time: 01:14:52
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

macOS Analysis Report

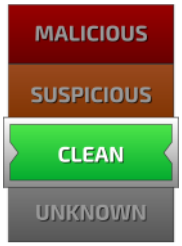
pwm_3.3.1.1_aarch64.dmg

Overview

General Information

Sample Name:	pwm_3.3.1.1_aarch64.dmg
Analysis ID:	752914
MD5:	860615adad871e.
SHA1:	462830c61a38b1..
SHA256:	8ad57fb0368aeb..
Infos:	

Detection

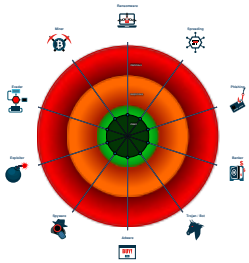


Score:	0
Range:	0 - 100
Whitelisted:	false

Signatures

Reads launchservices plist files

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752914
Start date and time:	2022-11-24 01:14:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pwm_3.3.1.1_aarch64.dmg
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:	CLEAN
Classification:	clean0.macDMG@0/0@0/0

Runtime Messages

Command:	open "/Volumes/PWMinder_3.3.1.1/PWMinder.app"
PID:	899
Exit Code:	1
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	LSOpenURLsWithRole() failed with error -10825 for the file /Volumes/PWMinder_3.3.1.1/PWMinder.app.

Process Tree

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 899, Parent: 812)
  - open (MD5: 40ed6d8f35c9f20484b97582d296398f) Arguments:
  - **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

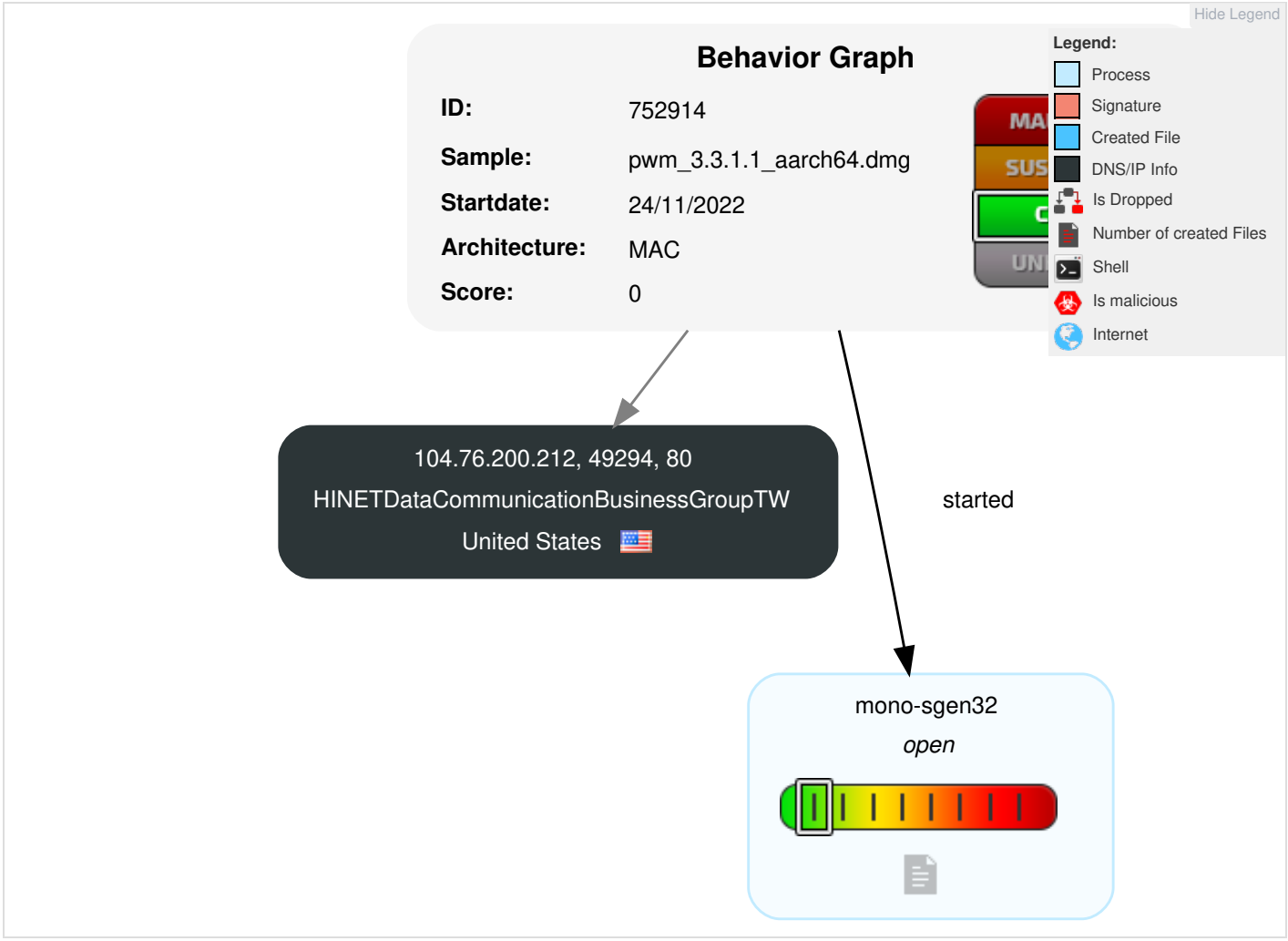
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	Path Interception	Path Interception	1 Invalid Code Signature	OS Credential Dumping	1 1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Code Signing	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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
pwm_3.3.1.1_aarch64.dmg	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

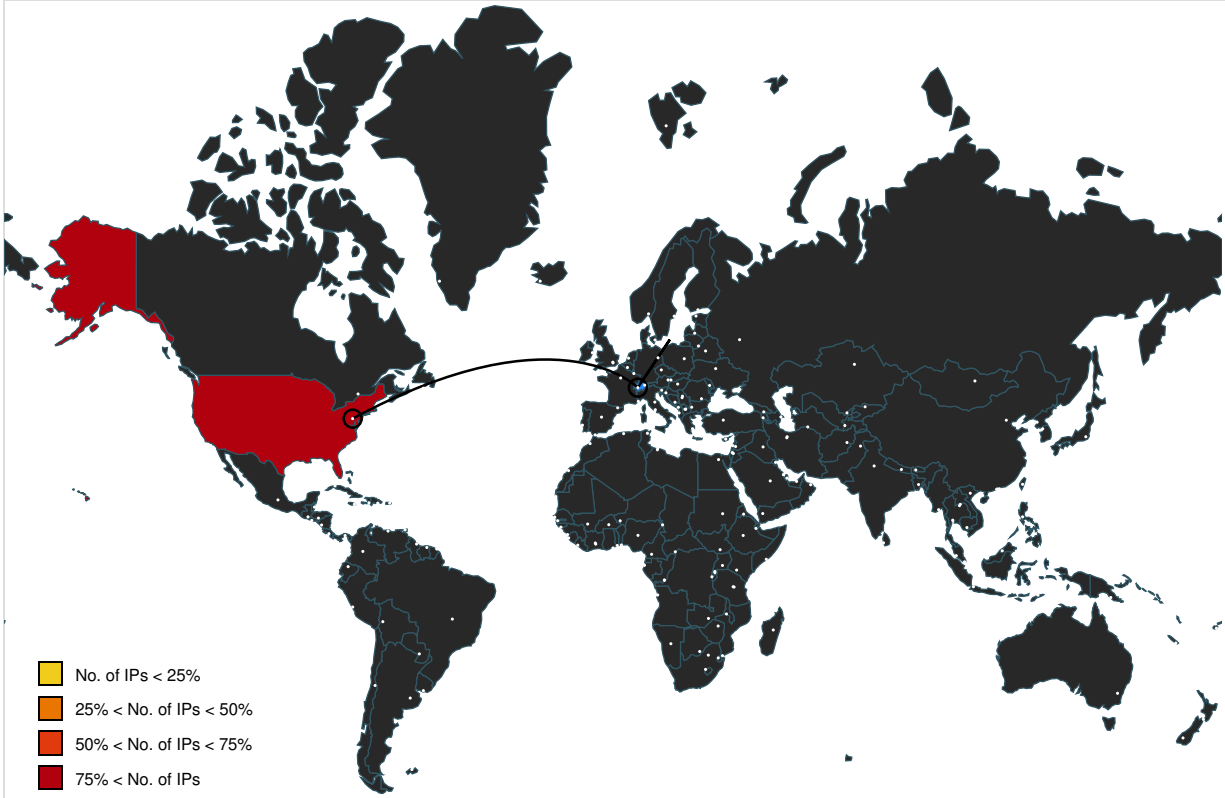
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.76.200.212	unknown	United States		3462	HINETDataCommunication BusinessGroupTW	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	bzip2 compressed data, block size = 100k
Entropy (8bit):	7.999667491831585
TrID:	• Disk Image (Macintosh), bzip2 (12509/2) 80.61% • bzip2 compressed archive (3009/2) 19.39%
File name:	pwm_3.3.1.1_aarch64.dmg
File size:	70962562
MD5:	860615adad871e67d0e2a362f7824b7b
SHA1:	462830c61a38b1d0c501b34bad200aec74ce3763
SHA256:	8ad57fb0368aeb7b73c4ef77da30bc9193f200a2c53b2b1cfa6d8dec6bdf0c8a
SHA512:	599faee0a185213f548362ed74f8a2f1c84593d2a82415911d202d015bb516e45080f1938d8da72c36c43a3d0e5ead8760bdb0d91b31672ea3ed1510f7167859
SSDEEP:	1572864:lZRFFYejQjasEfJNLPOWEtNOUF4txXp5Tm+UWuBgWPkW/:Zf5QjasEfvLIEL9F8xXLq2ugWJ
TLSH:	86F73376A59DA8D3CBC6573781CB17409DA04E37B9DF88480391FB8E283D61A7A14CBD
File Content Preview:	BZh11AY&SY..0....F ......@... .1...i...j:\.....N.$;'.;.BZh11AY&SY5|.........P.@....BH.........@... .u.=SA.....i...R..M.4....\g... (.^.d].\.*.....A..B.H.0H+.........=.4C.....~.I...A...R.W...).....BZh91AY&SY..|...........it"@@.@h .B@..... ..... @M.....MF.d

CodeSign Information

Network Behavior

TCP Packets

UDP Packets

System Behavior

Analysis Process: mono-sgen32 PID: 899, Parent PID: 812

General

Start time:	01:16:49
Start date:	24/11/2022
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32
Arguments:	n/a
File size:	3722408 bytes
MD5 hash:	8910349f44a940d8d79318367855b236

Analysis Process: open PID: 899, Parent PID: 812

General

Start time:	01:16:49
Start date:	24/11/2022
Path:	/usr/bin/open
Arguments:	
File size:	105952 bytes
MD5 hash:	40ed6d8f35c9f20484b97582d296398f

File Activities

File Read

Directory Enumerated