ID: 752916
Sample Name:
pwm_3.3.1.1_x86-64.dmg
Cookbook:
defaultmacfilecookbook.jbs
Time: 01:26:02
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

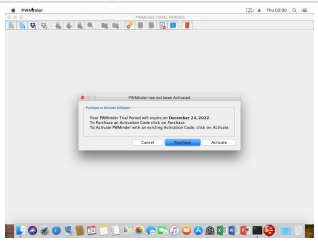
macOS Analysis Report

pwm_3.3.1.1_x86-64.dmg

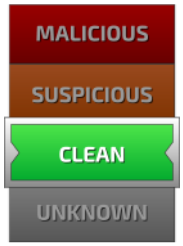
Overview

General Information

Sample Name:	pwm_3.3.1.1_x86-64.dmg
Analysis ID:	752916
MD5:	26e236876eb642.
SHA1:	5519ff231aedc73..
SHA256:	bd03a05dc21fa6..
Infos:	



Detection

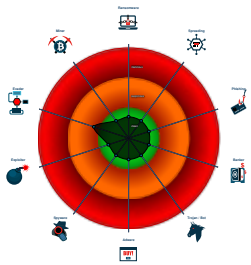


Score:	3
Range:	0 - 100
Whitelisted:	false

Signatures

- Reads the systems hostname
- Reads hardware related sysctl values
- Creates hidden files, links and/or dir…
- Reads the sysctl safe boot value (p…
- Reads the systems OS release and…
- Reads launchservices plist files

Classification



General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752916
Start date and time:	2022-11-24 01:26:02 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pwm_3.3.1.1_x86-64.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:	clean3.macDMG@0/24@2/0

Warnings

Runtime Messages

Command:	open "/Volumes/PWMinder_3.3.1.1/PWMinder.app"
PID:	900
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Process Tree

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 900, Parent: 812)
  - open (MD5: 40ed6d8f35c9f20484b97582d296398f) Arguments:
  - xpcproxy New Fork (PID: 901, Parent: 1)
  - PWMinder (MD5: 98e481ba3862913413a1ac1b7c00b45c) Arguments: /Volumes/PWMinder_3.3.1.1/PWMinder.app/Contents/MacOS/PWMinder
- **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

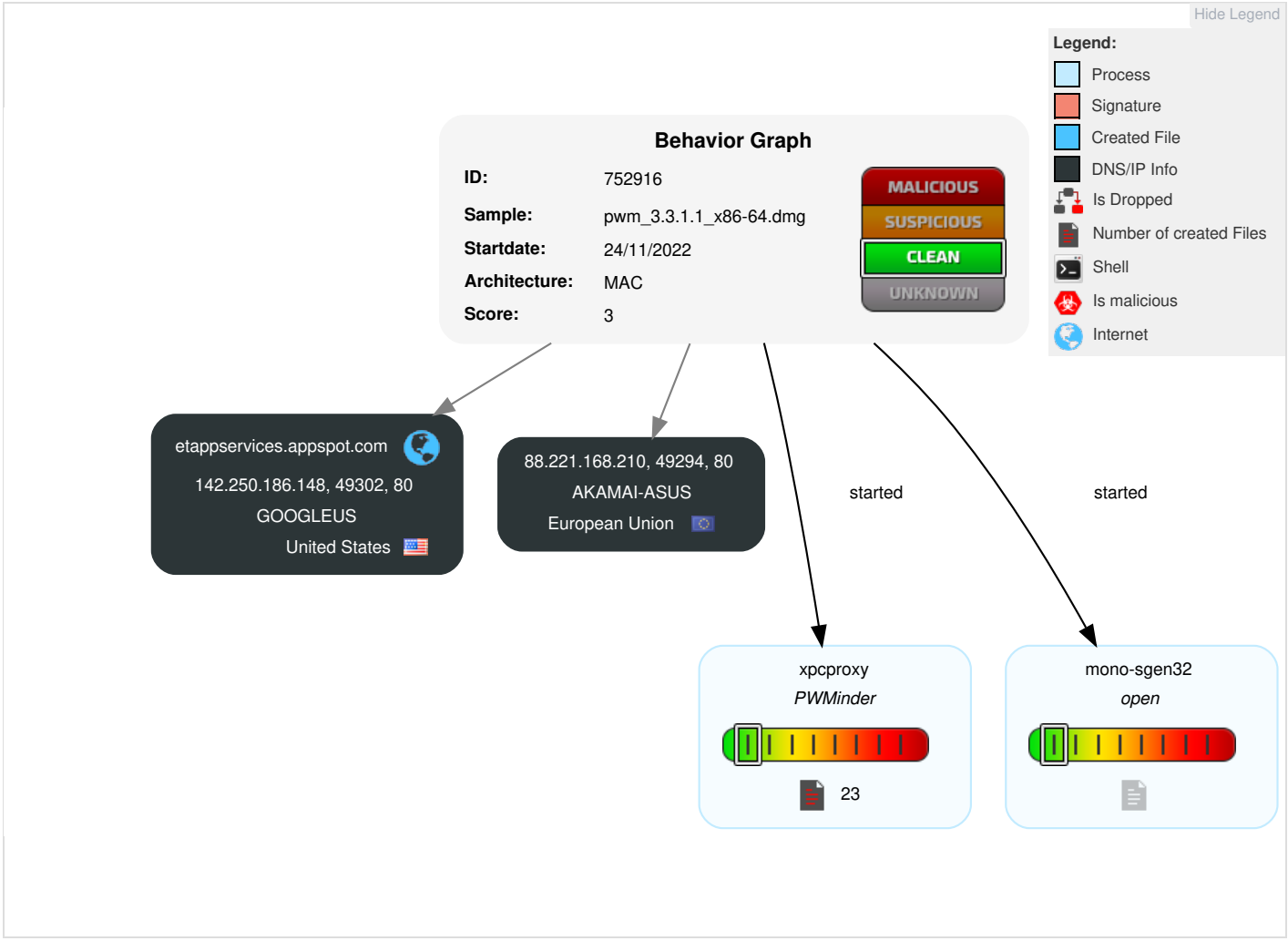
Joe Sandbox Signatures

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	5 1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	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	2 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Hidden Files and Directories	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

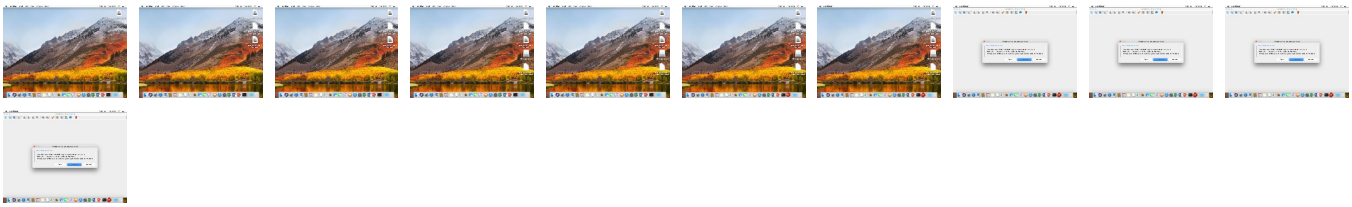
Behavior Graph

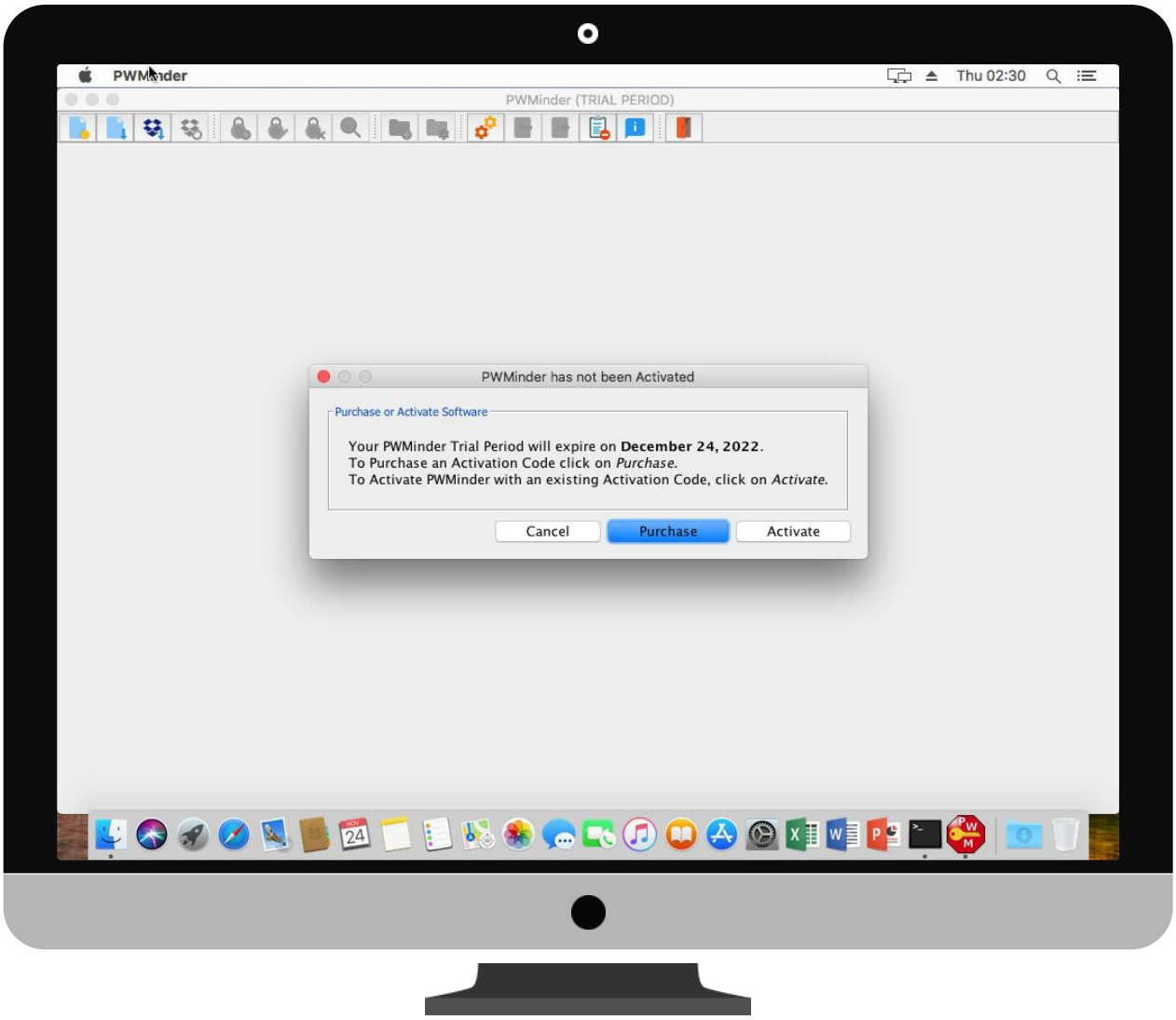


Screenshots

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_x86-64.dmg	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

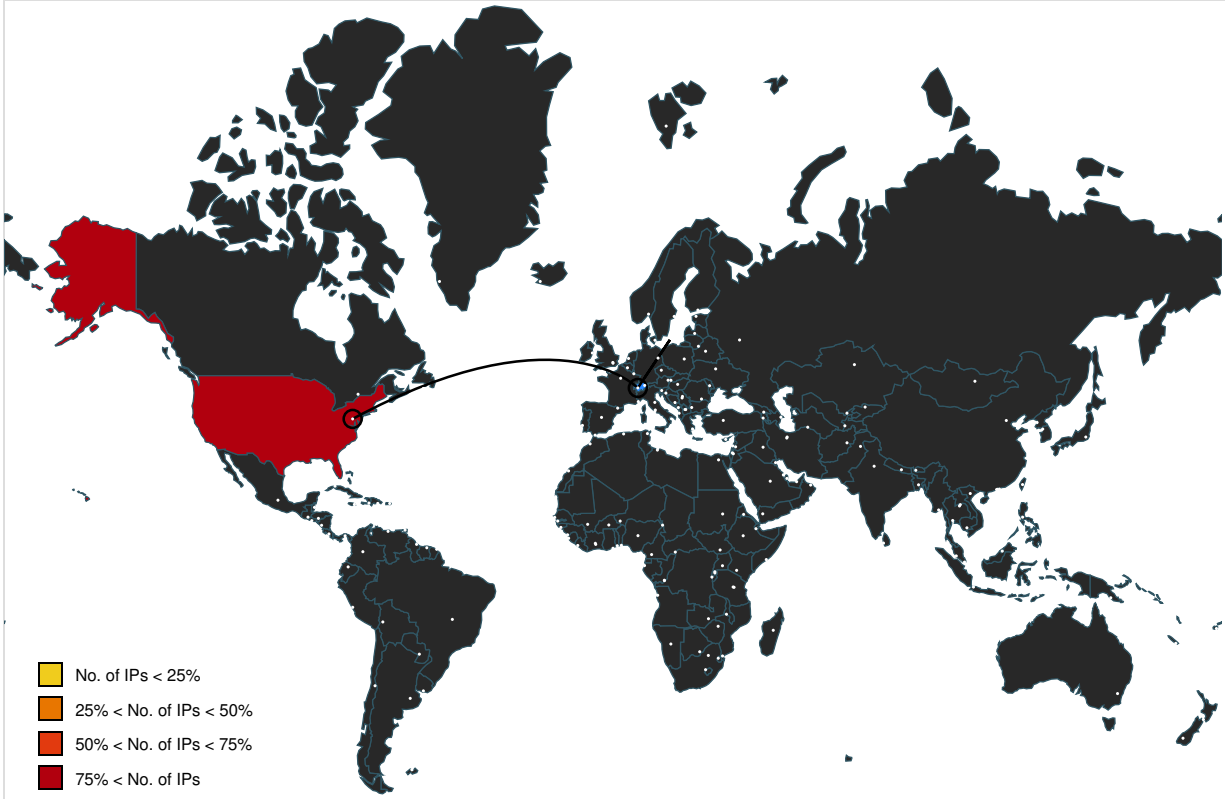
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
etappservices.appspot.com	142.250.186.148	true	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.221.168.210	unknown	European Union		16625	AKAMAI-ASUS	false
142.250.186.148	etappservices.appspot.com	United States		15169	GOOGLEUS	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

/Users/berri/.pwminder/log/PWMinder.log

/dev/null

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/hsperfdata_berri/901

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio10219926841058769522.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio10224466244630806701.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio10459773673903316017.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio12938241649503612607.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio13412971084950237612.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio13578127288510142521.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio16244522733088286171.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio20867146744837198l8.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio216252107100245977.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio22231709281746139l9.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio29996339748078696l2.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio3815422977875359551.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio5224863052943678154.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio5352537162059109128.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio6164943713436445280.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio6359674507834563537.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio66659064697009782l7.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio7103516844854627969.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio7212544972120051578.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio9716126586112586483.tmp

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/T/imageio9745765645810963695.tmp

Static File Info

General

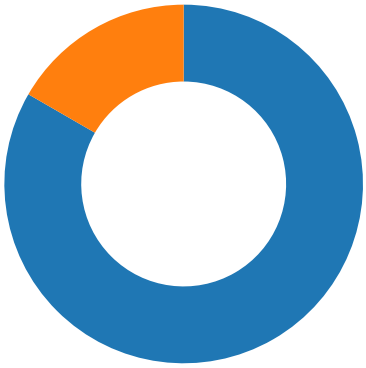
File type:	bzip2 compressed data, block size = 100k
Entropy (8bit):	7.999679567252431
TrID:	• Disk Image (Macintosh), bzip2 (12509/2) 80.61% • bzip2 compressed archive (3009/2) 19.39%
File name:	pwm_3.3.1.1_x86-64.dmg
File size:	72184045
MD5:	26e236876eb64279f77d118fbac3f06d
SHA1:	5519ff231aedc7394c5dd350b0b6058f253874c7

SHA256:	bd03a05dc21fa6ed0a3b35165df535896966f0f28279e07e7934d5e9e9ade8d8
SHA512:	ea476aa68f49632f0a4457b98549b9dbd881d1bc4d720c52734aaf6698176e1bc41f0b253808ee9a698900ae2b4cda07b135fefc9811bc223a3aea031ecd6fb3
SSDEEP:	1572864:7WAzO9n33sgIqk/kMl8TtlO1N2o/32H2avNZggwVJsYXZUk:KAIn33E/cMYQ1Mo/zavMHVJ9XZU
TLSH:	39F7337DA299A801CD958375E3DF1A264D110F73D5CAB98F167C3633A2F4279202AB37
File Content Preview:	BZh11AY&SY.z.V...F .....@.. .1...i...j:\.....N.$(....BZh11AY&SY+/.\.....P.@....BH..... .@... .u.=SA.....i...R..M.4....\g... (.^.d].\.*.....A..B.H.0H+.....=.4C.....~.I...A...R.W...)...Y}j.BZh91AY&SY.....x.Ib0.@P....@@...!.(..H.$..BL...*.j...

CodeSign Information

Network Behavior

Network Port Distribution



Total Packets: 12

- 53 (DNS)
- 80 (HTTP)

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 01:28:06.687371016 CET	192.168.11.11	1.1.1.1	0xbb2b	Standard query (0)	etappservices.appspot.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 01:28:06.687822104 CET	192.168.11.11	1.1.1.1	0x3951	Standard query (0)	etappservices.appspot.com	28	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 01:28:06.711705923 CET	1.1.1.1	192.168.11.11	0xbb2b	No error (0)	etappservices.appspot.com		142.250.186.148	A (IP address)	IN (0x0001)	false
Nov 24, 2022 01:28:06.711785078 CET	1.1.1.1	192.168.11.11	0x3951	No error (0)	etappservices.appspot.com			28	IN (0x0001)	false

HTTP Request Dependency Graph

- etappservices.appspot.com

System Behavior

Analysis Process: mono-sgen32 PID: **900**, Parent PID: **812**

General

Start time:	01:28:01
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: **900**, Parent PID: **812**

General

Start time:	01:28:01
Start date:	24/11/2022
Path:	/usr/bin/open
Arguments:	
File size:	105952 bytes
MD5 hash:	40ed6d8f35c9f20484b97582d296398f

File Activities

- File Read
- Directory Enumerated

Analysis Process: xpcproxy PID: **901**, Parent PID: **1**

General

Start time:	01:28:01
Start date:	24/11/2022
Path:	/usr/libexec/xpcproxy
Arguments:	n/a
File size:	43488 bytes
MD5 hash:	d1bb9a4899f0af921e8188218b20d744

File Activities

- File Read
- Directory Created

Analysis Process: PWMinder PID: **901**, Parent PID: **1**

General

Start time:	01:28:01
Start date:	24/11/2022
Path:	/Volumes/PWMinder_3.3.1.1/PWMinder.app/Contents/MacOS/PWMinder
Arguments:	/Volumes/PWMinder_3.3.1.1/PWMinder.app/Contents/MacOS/PWMinder
File size:	160464 bytes
MD5 hash:	98e481ba3862913413a1ac1b7c00b45c

File Activities

- File Created
- File Deleted
- File Read
- File Written
- Directory Enumerated
- Directory Attributes Enumerated Bulk
- Directory Created