ID: 756111
Sample Name:
Localizable.strings
Cookbook:
defaultmacfilecookbook.jbs
Time: 16:43:26
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

macOS Analysis Report

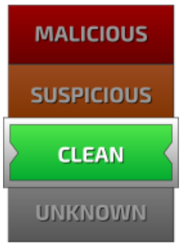
Localizable.strings

Overview

General Information

Sample Name:	Localizable.strings
Analysis ID:	756111
MD5:	2c6cc441ccdea7..
SHA1:	7968a661c4bf7f5..
SHA256:	41ecf6703414bb..
Infos:	

Detection

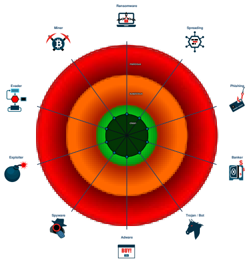


Score:	0
Range:	0 - 100
Whitelisted:	false

Signatures

Reads launchservices plist files

Classification



Analysis Advice

Sample could not be started, try setting a correct file extension or analyze on a different analysis machine.

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:	756111
Start date and time:	2022-11-29 16:43:26 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Localizable.strings
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.macSTRINGS@0/0@0/0

Warnings

Runtime Messages

Command:	open "/Users/berri/Desktop/Localizable.strings"
PID:	884
Exit Code:	1
Exit Code Info:	
Killed:	False

Copyright Joe Security LLC 2022

Standard Output:	
Standard Error:	No application knows how to open /Users/berri/Desktop/Localizable.strings.

Process Tree

- **System is macvm-highsierra**
  - mono-sgen32 New Fork (PID: 884, Parent: 811)
    - open (MD5: 40ed6d8f35c9f20484b97582d296398f) Arguments:
- **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

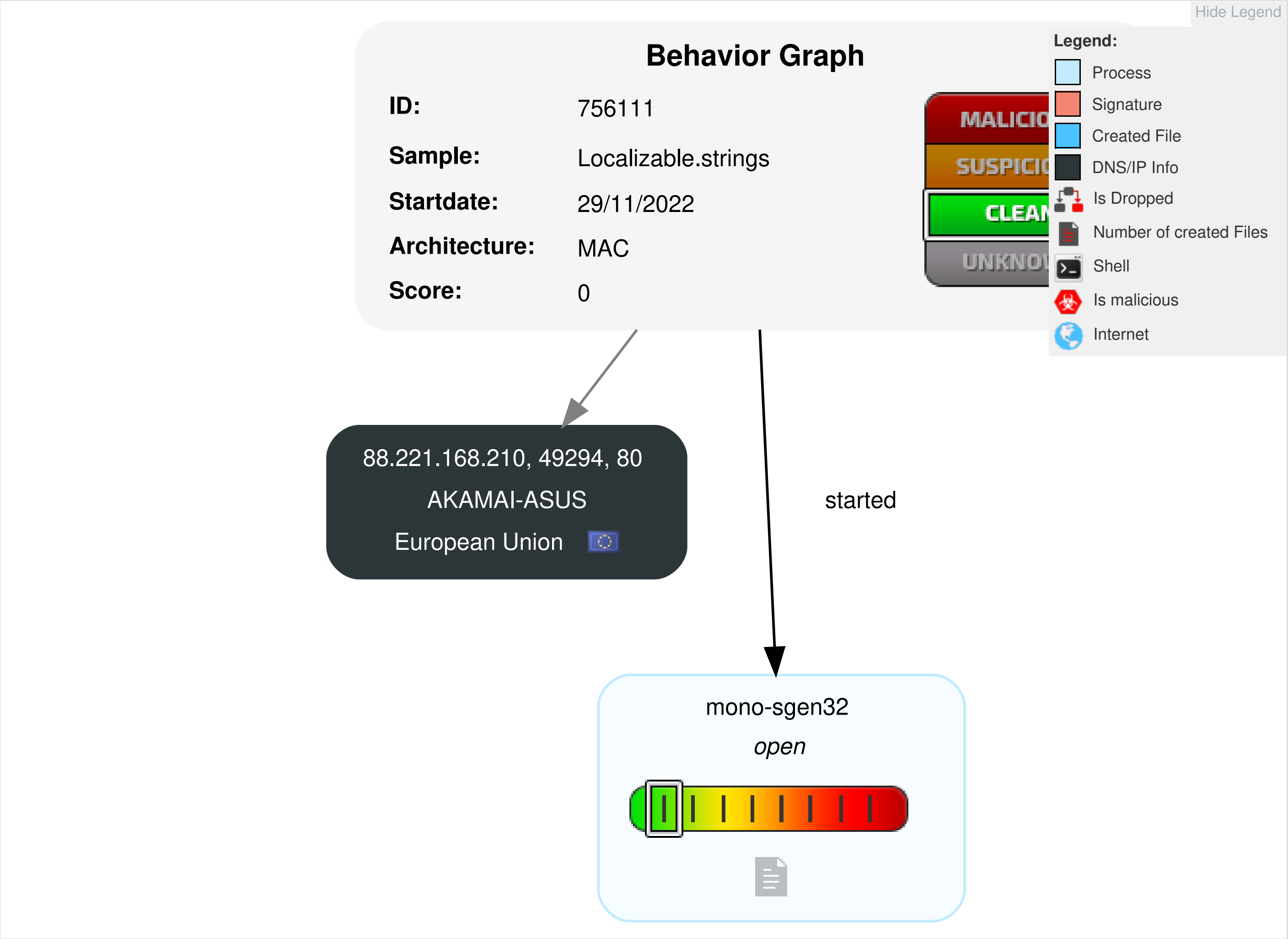
Joe Sandbox Signatures

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	Direct Volume Access	OS Credential Dumping	1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Behavior Graph



Behavior Graph

ID: 756111

Sample: Localizable.strings

Startdate: 29/11/2022

Architecture: MAC

Score: 0

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
Localizable.strings	0%	Virustotal		Browse
Localizable.strings	0%	ReversingLabs		

Dropped Files

⊘ **No Antivirus matches**

Domains

⊘ **No Antivirus matches**

URLs

⊘ **No Antivirus matches**

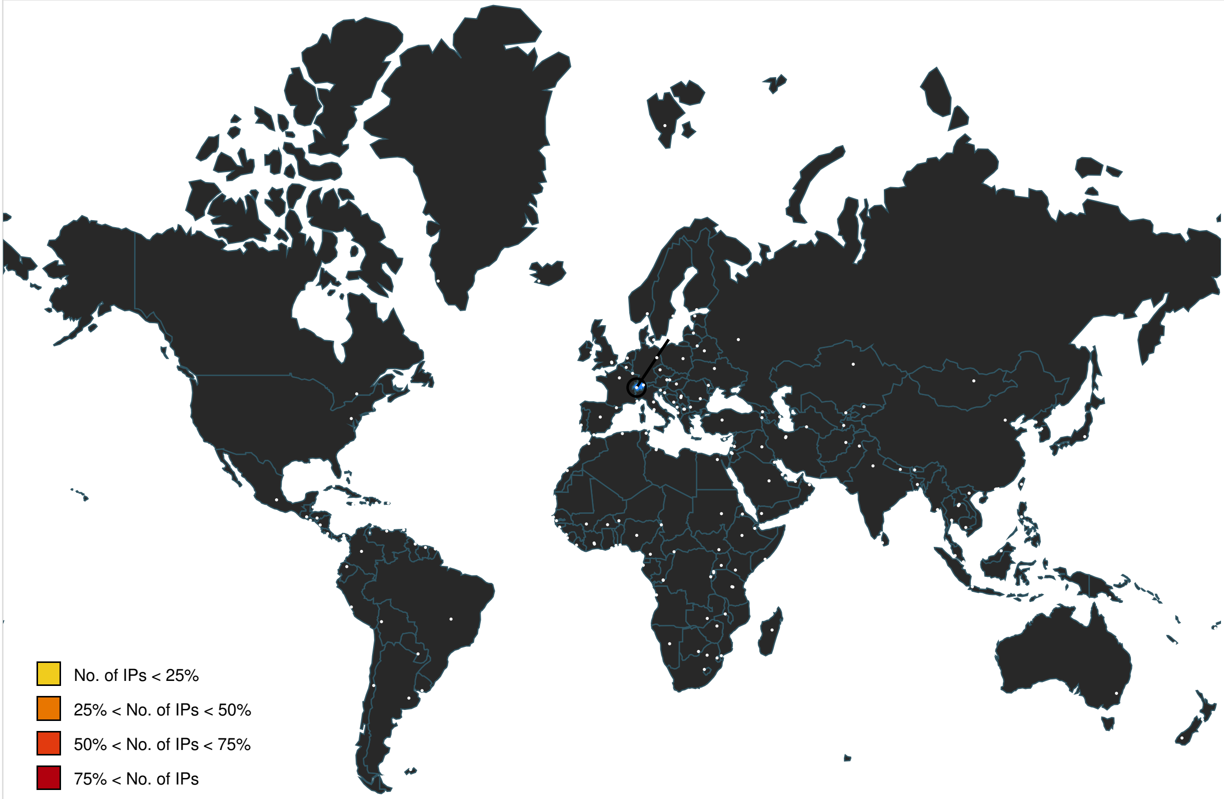
Domains and IPs

Contacted Domains

⊘ No contacted domains info

URLs from Memory and Binaries

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

Joe Sandbox View / Context

IPs

⊘ No context

Domains

⊘ No context

ASNs

⊘ No context

JA3 Fingerprints

⊘ No context

Dropped Files

⊘ No context

Copyright Joe Security LLC 2022

Created / dropped Files

No created / dropped files found

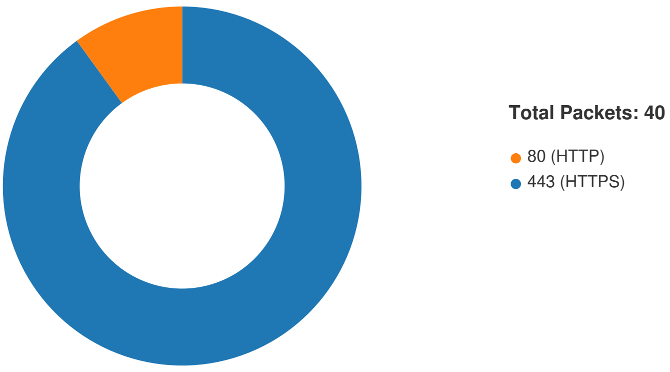
Static File Info

General

File type:	Unicode text, UTF-8 text, with very long lines (600)
Entropy (8bit):	4.936931280143745
TrID:	
File name:	Localizable.strings
File size:	11875
MD5:	2c6cc441ccdea763c0be634ab46ae0f6
SHA1:	7968a661c4bf7f54a8ed1ef501a083a337aacf6e
SHA256:	41ecf6703414bbee3cf309de7b3c3b94a8495f93118f260ab3d2299ab405bb62
SHA512:	173779861c98bff0ec239344af6b68c6ef26e5ed13d264297992a541d21ba5ae85a171ddbd1b02f34ac7551fffcb33a45a28e27b7eb39a33875443987847dc5e
SSDEEP:	192:zhQU06Mn7H7IE6Vy8WmMyzgOPsMzL4ekGX1Z3JXJy4LzmhW16Q7XaTs:zhQUzSbIPVy8WmsOkAwO1XXZIW16QzCs
TLSH:	4332A4BD4B40037C2952C3A1623FBF17FB108329662DA18E4D6FC55522DF90AE67BA53
File Content Preview:	"A newer version of DiskMaker X is available. Do you want to download it?" = "Uma vers..o mais recente do DiskMaker X est.. dispon..vel. Voc.. deseja fazer a transfer..ncia?" ;.."Not now, thanks" = "Agora n..o, obrigado";.."Get new version" = "Obter a nov

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: mono-sgen32 PID: **884**, Parent PID: **811**

General

Start time:	16:44:23
Start date:	29/11/2022
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: **884**, Parent PID: **811**

General

Start time:	16:44:23
Start date:	29/11/2022
Path:	/usr/bin/open
Arguments:	
File size:	105952 bytes
MD5 hash:	40ed6d8f35c9f20484b97582d296398f

File Activities

File Read ▼

Directory Enumerated ▼

Copyright Joe Security LLC 2022