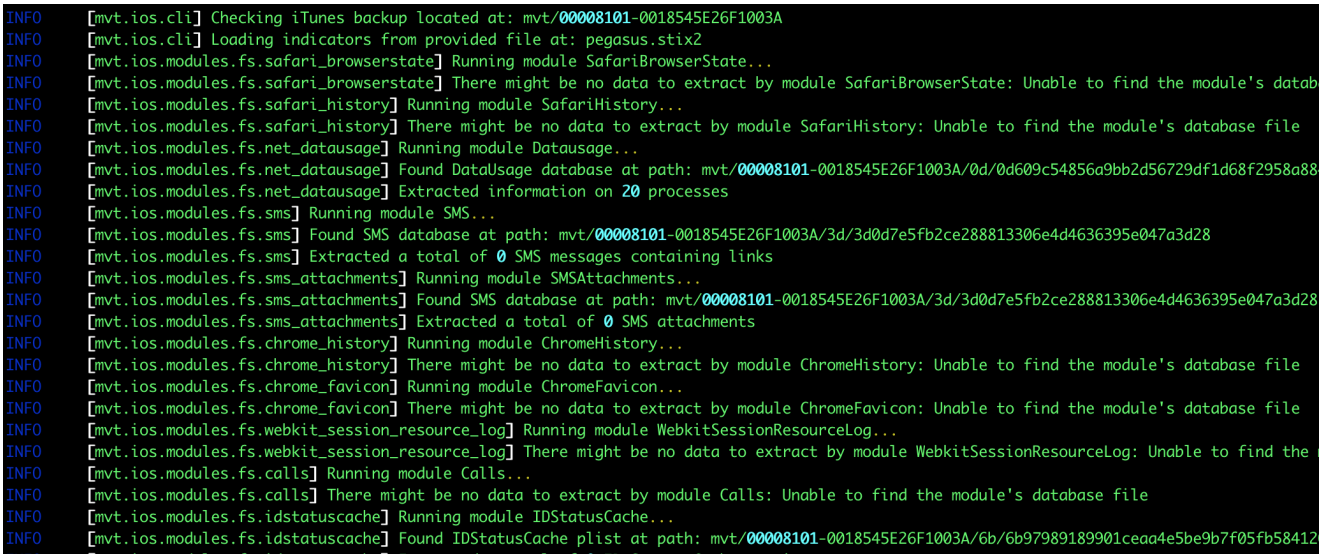
Scanning your iPhone for Pegasus, NSO Group's malware

arkadiyt.com/2021/07/25/scanning-your-iphone-for-nso-group-pegasus-malware/



Arkadiy Tetelman A security blog

Jul 25th, 2021 | 7 minute read

In collaboration with more than a dozen other news organizations The Guardian recently published an exposé about Pegasus, a toolkit for infecting mobile phones that is sold to governments around the world by NSO Group. It's used to target political leaders and their families, human rights activists, political dissidents, journalists, and so on, and surreptitiously download their messages/photos/location data, record their microphone, and otherwise spy on them. As part of the investigation, Amnesty International wrote a blog post with their forensic analysis of several compromised phones, as well as an open source tool, Mobile Verification Toolkit, for scanning your mobile device for these indicators. MVT supports both iOS and Android, and in this blog post we'll install and run the scanner against my iOS device.

Choosing your options

For iPhones, MVT can either run against a device backup or a full file system dump (which is only available from jailbroken devices). The device backup method has access to less forensic data than the filesystem dump but has the benefit that you don't need to jailbreak your device. MVT conveniently documents which forensic artifacts are available to which method - the following artifacts are not available when using the backup method:

- cache_files.json
- net_usage.json

- safari_favicon.json
- version_history.json
- webkit_indexeddb.json
- webkit_local_storage.json
- webkit_safari_view_service.json

The same documentation link also explains what data each file contains and where it's sourced from, and Amnesty's blog post describes in more detail how each data type is relevant for detecting Pegasus. For instance for the Safari favicon data (`safari_favicon.json`) they write:

> Although Safari history records are typically short lived and are lost after a few months (as well as potentially intentionally purged by malware), we have been able to nevertheless find NSO Group's infection domains in other databases of Omar Radi's phone that did not appear in Safari's History. For example, we could identify visits through Safari's Favicon.db database, which was left intact by Pegasus

So if you have a jailbroken device you will get more complete Pegasus detection with the filesystem dump approach, but since my device is not jailbroken I'll go with the device backup approach - it's better than nothing. In fact there is no publicly known jailbreak available for my iPhone model and version of iOS, so I don't have a choice.

Creating and checking your backup

To create and check your iPhone backup you can:

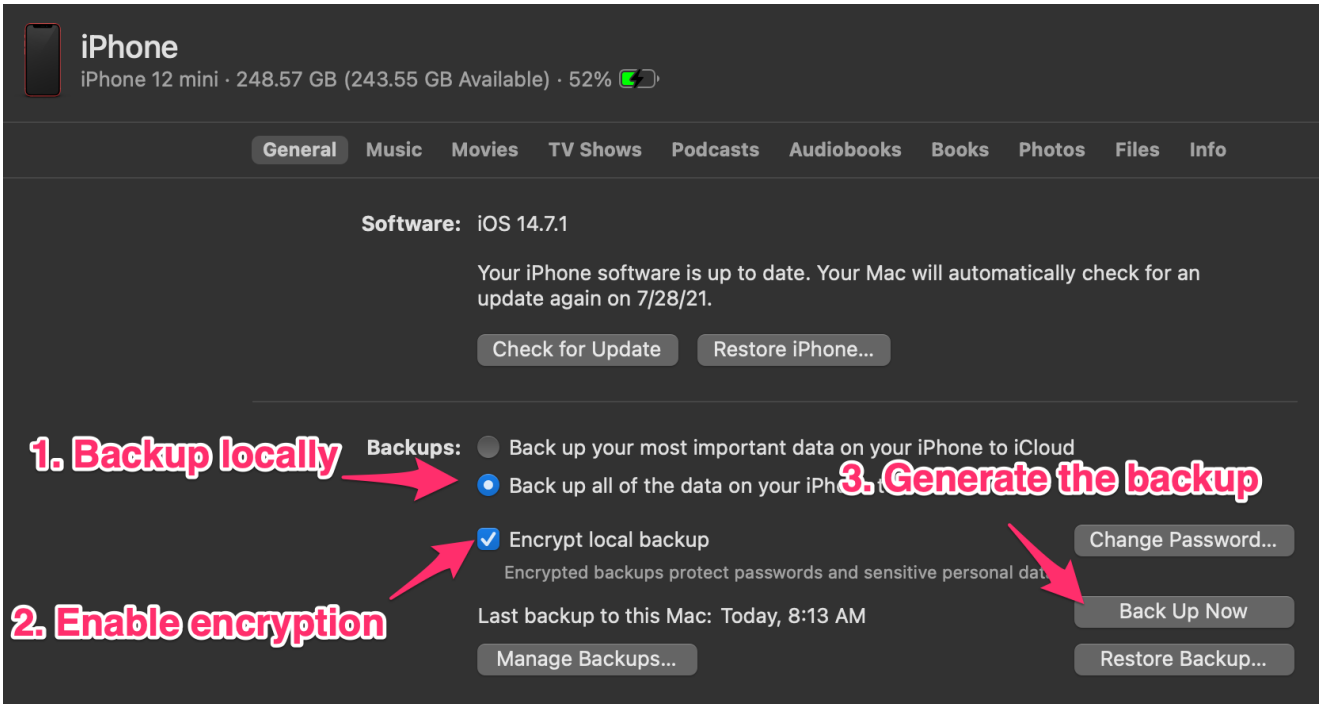
Build the MVT docker image:

```
git clone https://github.com/mvt-project/mvt.git
cd mvt
docker build -t mvt .
```

Create your backup:

The backup can be created either directly in Finder (prior to MacOS Big Sur this was done through iTunes), or using a library called libimobiledevice.

For the Finder approach plug your phone into your laptop, navigate to it in Finder, and click “Back Up Now” with these settings checked:



MVT only operates against decrypted backups so in the next step we’ll be decrypting everything anyway, but encrypted backups export more device data (such as your browsing history or wifi settings) so encrypting your backup will give you better detection.

After the backup is created click “Manage Backups”, then right click on your backup and select “Show In Finder”, and copy the folder to somewhere easily accessible (say, to your desktop).

Or, if you’d prefer to create a backup using libimobiledevice instead of Finder:

MVT automatically includes libimobiledevice in its Docker image but even with their instructions I couldn’t get it to recognize my iPhone from inside Docker, so I installed it on my MacOS host:

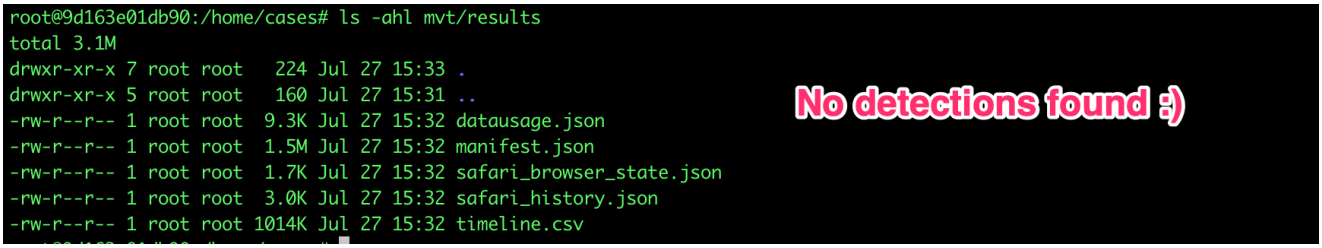
```
# Install latest libimobiledevice
brew install --HEAD libimobiledevice

# Make a working directory
mkdir -p ~/Desktop/mvt

# Enable backup encryption - you'll be prompted for a password
idevicebackup2 -i backup encryption on

# Backup the device
idevicebackup2 backup --full ~/Desktop/mvt/
```

Now we can scan our backup:

```
docker run \
  # Mount your desktop working directory into Docker
  -v ~/Desktop/mvt:/home/cases/mvt \
  # Run the MVT image
  -it mvt

# Download Amnesty International's indicators of compromise
wget https://raw.githubusercontent.com/AmnestyTech/investigations/master/2021-07-
18_nso/pegasus.stix2 -O pegasus.stix2

# We'll save our results here
mkdir mvt/results

# Decrypt the backup
mvt-ios decrypt-backup \
  # The backup password you created
  -p '<password>' \
  # The directory to save the decrypted backup to
  -d mvt/decrypted \
  # The encrypted backup to decrypt
  mvt/00008101-0018545E26F1003A/

# Scan the decrypted backup
mvt-ios check-backup \
  # Path to our downloaded IoCs
  --iocs pegasus.stix2 \
  # Where to save the results
  --output mvt/results \
  # Path to the backup to scan
  mvt/decrypted
```

And lastly we can interpret the results:

If everything ran successfully you should have a number of json files in the mvt/results folder on your desktop. Any filenames ending in `_detected.json` indicate that some trace of Pegasus was found, and all other json files contain debug data about your scan results. If you have no `_detected.json` files then there were no Pegasus indicators found:



P.S. If you enjoy this kind of content feel free to follow me on Twitter: @arkadiyt