Mobile Malware Analysis

Self-Triage di alto livello di un dispositivo Mobile per l'identificazione di comportamenti sospetti correlati a attività malware

Perché mobile malware analysis?

Incremento continuo degli attacchi sui dispositivi mobile

Il 30% degli 0-day scoperti nel 2021 avevano come target il mobile

75% dei siti di phishing analizzati erano indirizzati a dispositivi mobile

2,034,217 nuovi malware samples scoperti nel 2021

Infettati più di 10 milioni di dispositivi in 214 paesi

Perché è importante parlarne?

La malware analysis richiede conoscenze verticali approfondite

1. Sistemi Operativi in adozione: iOS e Android

2. Tecniche di exploitation

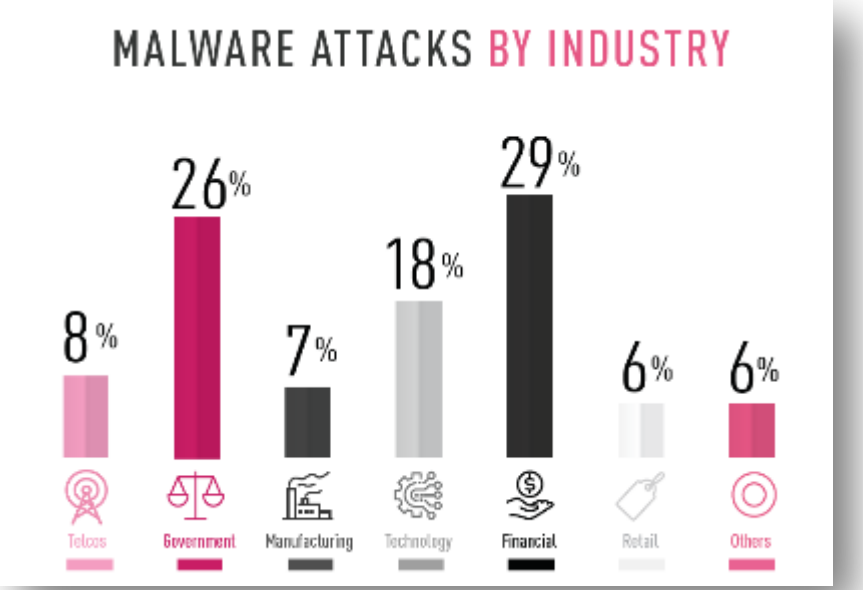
3. Setup di ambienti per l'analisi statica e dinamica

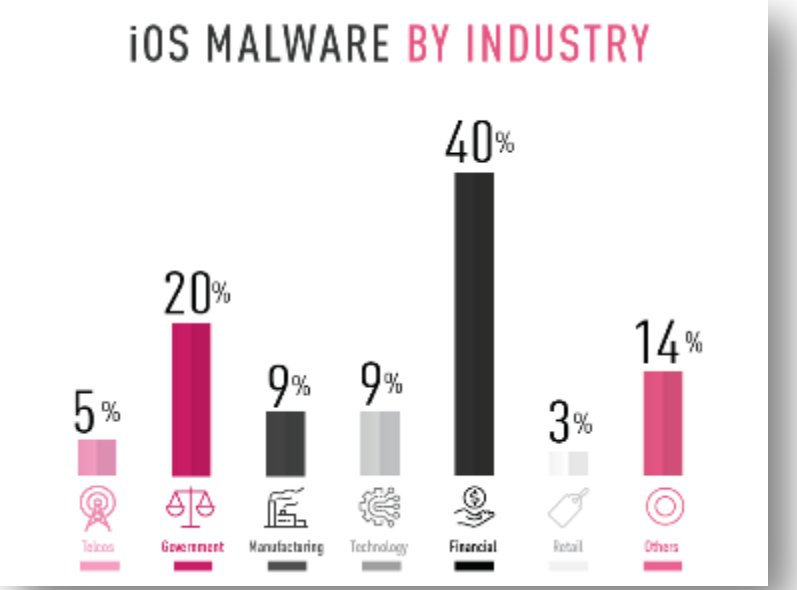
4. Tecniche di anti RE / anti forensics

Malware sui Dispositivi Mobili

Negli ultimi anni la sempre maggiore centralità dei dispositivi *mobile* nella vita delle persone ha portato a un incremento dei malware sviluppati per essi

*PurpleSec reported a **41% rise** in ransomware attacks in 2019 with 205,000 businesses losing access to their files. The company also identified **68,000 new ransomware trojans for mobile** in the same year, which highlights a new trend of criminals targeting mobile users with file-encrypting malware.*





L'incremento esponenziale della minaccia ha portato maggiore consapevolezza ma spesso non adeguate contromisure atte alla mitigazione del rischio

Disclaimer

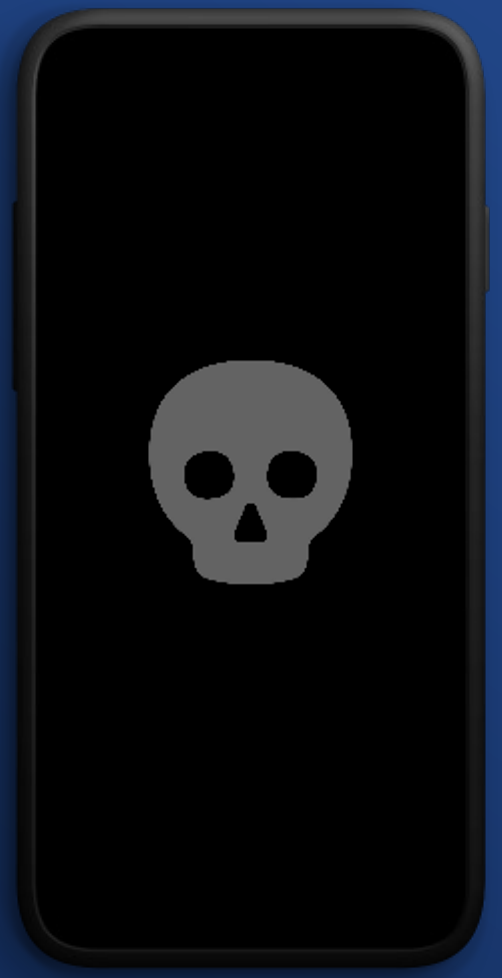
Ciò che vedremo non sostituisce una completa analisi del dispositivo…

Ma…

Potrebbe fornire informazioni utili per capire se sia veramente necessario procedere con analisi avanzata

"Alcune minacce informatiche possono prendere il controllo del vostro smartphone,
se gli fornite i permessi"

Identificazione IOC comuni



Riavvii improvvisi

Scaricamento Batteria

Problemi nell'uso di microfono e camera

Update non disponibili

- Crash applicazioni (browser)
- Impossibile spegnere
- App non conosciute
- Chiamate non presenti nel registro
- Switch continuo su connessioni meno sicure (2G-3G)
- Riscaldamento del dispositivo
- Tastiera lenta
- Bootloop
- SMS nuovi / chiamate in uscita sconosciute
- Profili sconosciuti / MDM
- Richiesta PIN random

Posso capire se il mio device è compromesso?

STEP 1: Analisi Antivirus

SOPHOS

Malwarebytes

KASPERSKY lab

eset

Norton

TREND MICRO

F-Secure

McAfee

zecOps

TOTAL AV

TRACE

Applicazioni e Permessi

STEP 2: Analisi Permessi

Affinché le app possano avere accesso ai componenti del sistema devono essere autorizzate (permesso di geolocalizzazione, accesso libreria foto, fotocamera, microfono, etc.)

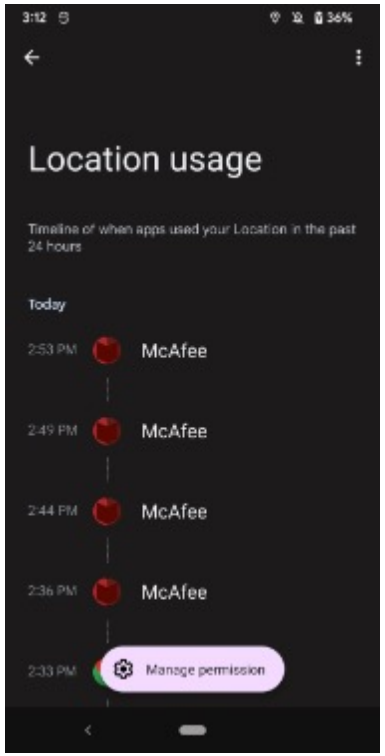
Reference: A Day in the Life of Your Data

iOS 15 privacy dashboard

Android 12 privacy dashboard

Analisi con Android / iOS Privacy Dashboard

- Ognuno di noi conosce l'utilizzo che fa proprio del proprio dispositivo
- Analisi dei permessi delle app
  - ✓ Perchè l'applicazione X richiede la geolocalizzazione ogni qualvolta sblocco il telefono?
  - ✓ Perchè l'applicazione Y ha attivato la camera mentre dormivo?
  - ✓ Perchè l'applicazione Z ha attivato il microfono mentre era aperta l'applicazione di home banking?



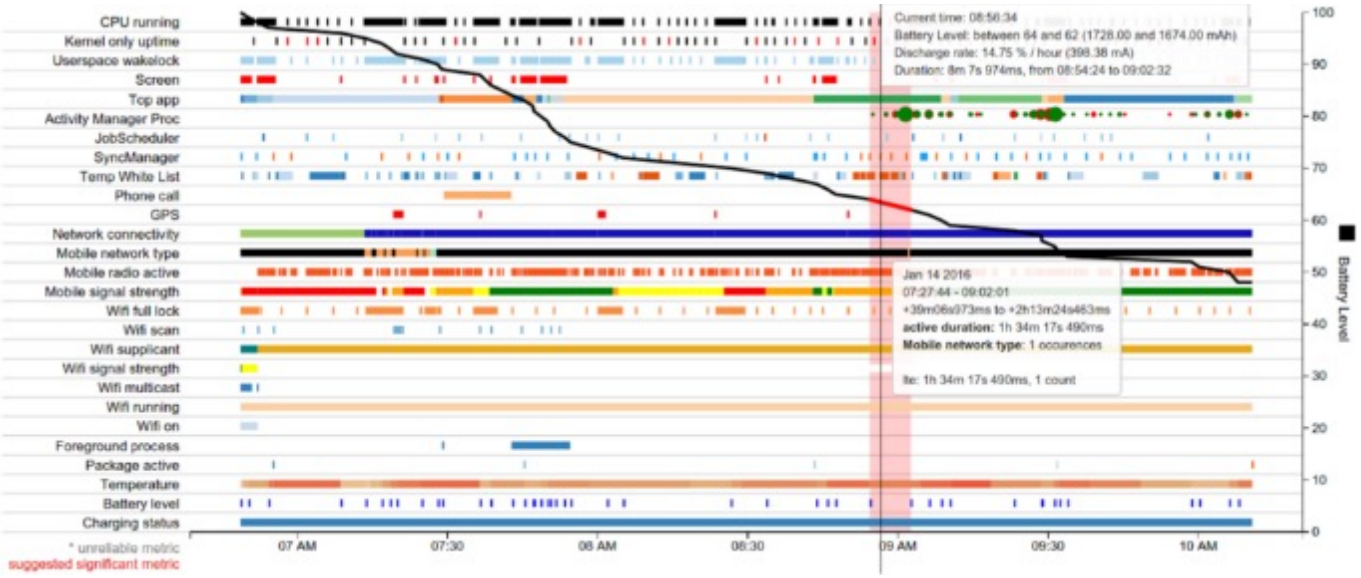
Analisi tramite ‘Battery Historian’

STEP 3: Analisi cicli di scarica batteria

Battery Historian consente di esaminare le informazioni e gli eventi relativamente all’utilizzo della batteria

Funzionalità:

1. Visualizzare eventi a livello di sistema
2. Visualizzare eventi a livello di applicazione
3. Visualizzare statistiche aggregate dall’ultima carica completa
4. Analizzare nello specifico una data applicazione



Analisi tramite APK / IPA – 1/2

STEP 4: Analisi App installate

Gli applicativi che installiamo nei nostri smarphone si presentano in due diversi formati:

- IPA: Sistema operativo iOS (e.g. Apple)
  - Può essere estratto tramite l'applicativo iTunes
- APK: Sistema operativo Android (e.g. Google)
  - Può essere estratto tramite ADB (richiede l'applicazione: "Android SDK")
  - **Nota**: Android richiede di attivare la *modalità sviluppatore*

Ricevere la lista degli applicative installati:

```
adb shell pm list packages
```

Recuperare il full path:

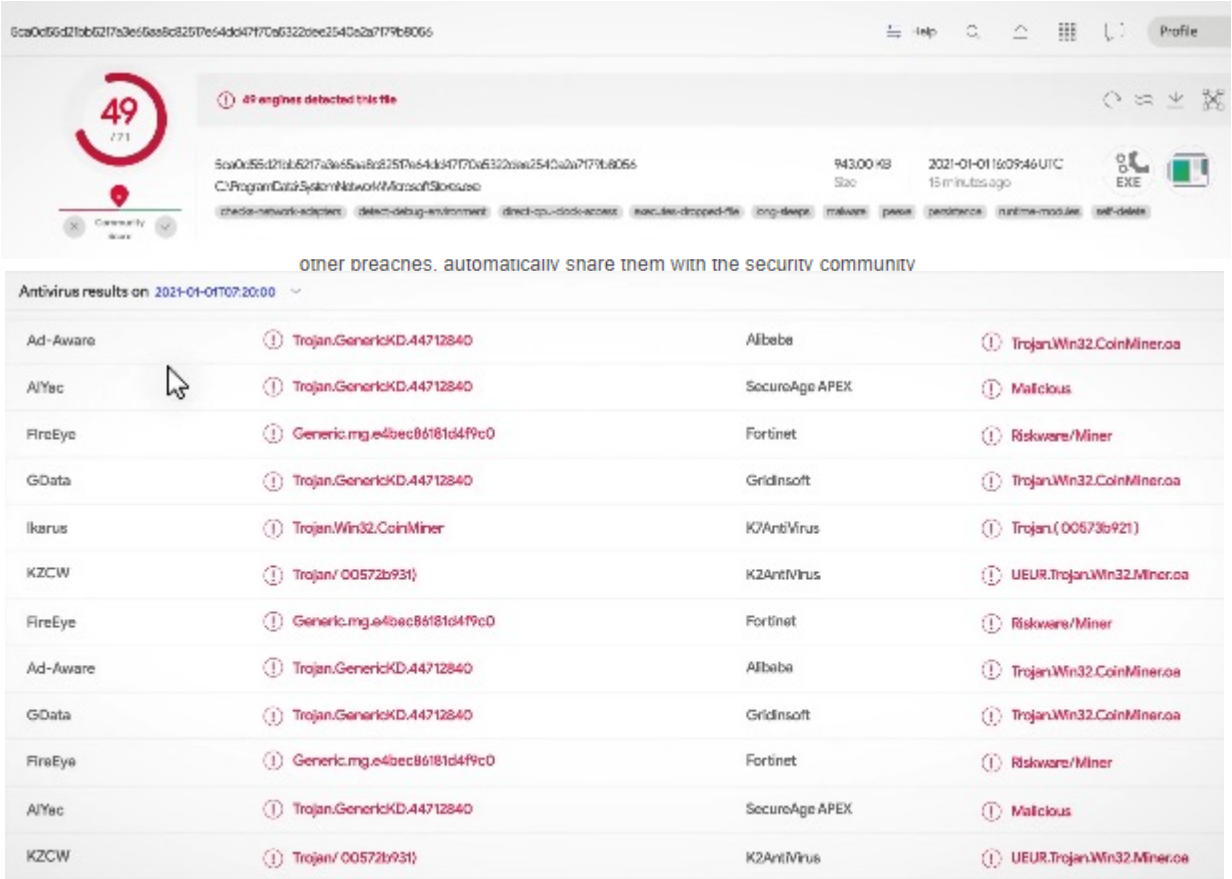
```
adb shell pm path com.example.app
```

Estrarre il pacchetto:

```
adb pull /data/app/com.example.app.apk
```

Analisi tramite APK / IPA – 2/2

1. Caricare la signature (e.g. hash) del package su **Virus Total** attraverso la funzione ‘Search’
2. Questo restituirà una serie di informazioni su tutto ciò che si conosce relativamente al file analizzato
    1. Sarà possibile avere uno ‘score’ complessivo (ed i relativi tag associati ad esso)
    2. Sarà possibile visualizzare come i diversi motori degli anti-virus / anti-malware riconoscono il file analizzato



Caso Pratico – Escobar Malware

Marzo 2022: il MalmwareHunterTeam individua per la prima volta una variante di un noto trojan bancario (Aberebot). Il nome del pacchetto è "com.**escobar**.**pablo**", quello dell'applicazione attraverso il quale si camuffa: McAfee.

Il malware è venduto sotto forma di Servizio a circa 3000$ / mese (in fase beta).

Automazione tramite prodotti commerciali XRY (MSAB©) 1/2

STEP 5 - Bonus: Automatizzare

XRY offre ai suoi utenti la possibilità di accedere ai contenuti dei file .XRY (un contenitore sicuro di prove digitali) tramite API Python. Questo ha reso possibile l'integrazione e l'automazione dell'analisi appena vista all'interno del prodotto.

I <u>requisiti per il corretto funzionamento sono</u>:
- PC connesso a Internet
- chiave API di Virus Total (Free / Personale)

<u>Come funziona</u>?

Attraverso lo script python, XRY esegue:

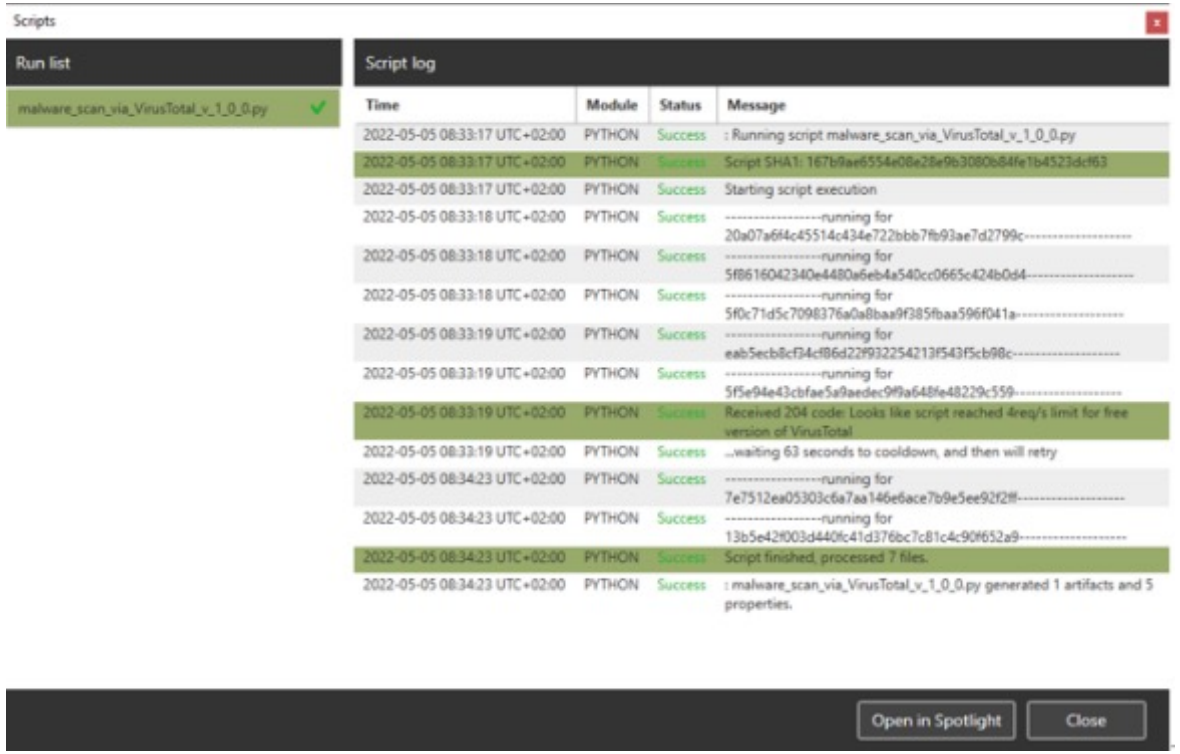
1. Calcolo dell'hash sull'applicazione desiderata
2. Interroga successivamente Virus Total
3. Fornisce tre possibili risultati:
   - Malware 🔴
   - Unknown 🟠
   - Negative ✅

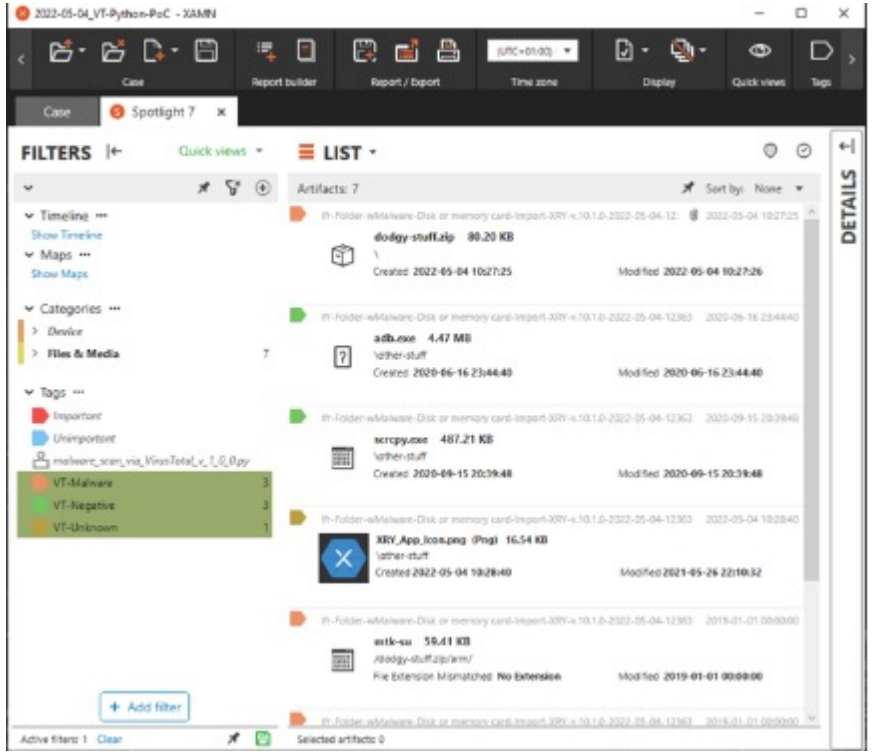
```python
import xry
import json
import time
import sys
```

```python
## Important: Paste your VirusTotal API key here:
vtApiKey = ''
```

```python
    # Initiate "VT-Deteciton" tags
    tagScrPos = image.create_tag("VT-Malware", xry.tag_icons.dark_salmon)
    tagScrNeg = image.create_tag("VT-Negative", xry.tag_icons.mantis)
    tagScrUnk = image.create_tag("VT-Unknown", xry.tag_icons.roti)
```

Automazione tramite prodotti commerciali XRY (MSAB©) 2/2





Cyber Act Forum 2023

TRACE