

# Scenari reali di **DFIR**: Tips&Tricks per una corretta analisi



@samaritan\_o



<http://bit.ly/2fL3nM5>



[alessandro.dicarlo@protonmail.com](mailto:alessandro.dicarlo@protonmail.com)

Alessandro Di Carlo

30 Maggio 2020

# \$WHOAMI

- **CTO** at BIT4LAW
- National and International speaker
- SANS **Lethal Forensicator**
- **GCFA** - GIAC Certified Forensic Analyst
- **GASF** – GIAC Advanced Smartphone Forensics
- **Qualche altra certificazione che non frega a nessuno :)**



**\$Zoom Meeting**



**<https://bit.ly/3gAEgr5>**

**Meeting ID: 789 0262 2815**

**Password: XXXXXXXXXXXXXXXX**

**\$DISCLAIMER!**



Le slides sono pensate per far da 'guida'  
alla risoluzione dello scenario.

NON spiegano e NON approfondiscono  
concetti particolari

# \$Scenario

## HACK IN BO® Safe Edition

2020

14<sup>a</sup> EDIZIONE



Un utente **macOS** lamenta un'intrusione informatica:

1. E' realmente accaduta?
2. La minaccia è ancora in essere?
3. Quali artefatti sono utili per svolgere una corretta investigazione?
4. ...



L'**attaccante** è stato scoperto!!

1. Che tipo di macchina ha utilizzato per effettuare l'attacco?
2. È riuscito ad ottenere persistenza?
3. ...



# \$macOS artifacts - Sysdiagnose



- Non pensato per scopi di security e/o incident response
- Presenta al suo interno grandi quantità di informazioni
  - Processi attivi
  - Configurazioni network
  - Log di sistema
  - Versione di sistema operativo
  - Volumi montati
  - ...
- Avviabile premendo i pulsanti **Control+Option+Command+Shift+Period**
- In alternativa, **sudo sysdiagnose**
- **~/private/var/tmp/sysdiagnose\_AAAA.MM.DD-HH:MM:SS\_XXXXXXXXXX**

## \$macOS artifacts – LaunchDaemons/LaunchAgents

- **launchd** → processo utilizzato da macOS per daemons e agents

Path	Descrizione
<Macintosh HD>/System/Library/LaunchDaemons	Daemons di sistema forniti da Apple
<Macintosh HD>/System/Library/LaunchAgents	Agenti forniti da Apple che vengono applicati a tutti gli utenti in base a ogni singolo utente
<Macintosh HD - Data>/Library/LaunchDaemons	Daemons di sistema di terze parti
<Macintosh HD - Data>/Library/LaunchAgents	Agents di terze parti che vengono applicati a tutti gli utenti in base a ogni singolo utente
~/Library/LaunchAgents	Agents di terze parti che vengono applicati solo all'utente che ha effettuato l'accesso

# \$Windows Timeline



- **mmls** /path/immagine →

Usato per visualizzare la lista delle partizioni presenti

- **fls.exe** -r (ricorsivo) -m (mount point) "C:\\" -o (offset) 1187840 -f (file system) ntfs /path\_to\_image > bodyfile →

Usato per generare la timeline

- **mactime** -b (bodyfile) bodyfile 2020-03-01..2020-05-30 > timeline.csv →

Usato per convertire il bodyfile in csv e, volendo, selezionare un range temporale ben definito



# \$Chocolatey Package Manager

- Gestore di pacchetti
- Una quantità imbarazzante di log
- C:\ProgramData\chocolatey\lib\...



# \$Prefetch

- Cosa sono esattamente?
- Introdotti a partire da Windows XP
- Ad ogni avvio del sistema operativo, Windows registra diverse informazioni
  - modalità di avvio del computer
  - Quali sono i programmi aperti con maggiore frequenza



# \$Prefetch










- I file di prefetch contengono numerose informazioni utili in ambito forense
  - Il nome dell'eseguibile
  - Il **path assoluto** dell'eseguibile
  - Il **numero** di volte che il programma è stato lanciato
  - **L'ultima volta** che l'applicazione è stata eseguita
  - ...

# \$Prefetch



- Path
  - **C:\Windows\Prefetch**
- Vediamo ora come è composto il nome
  - Nome dell'eseguibile
  - -
  - **Hash di 8 cifre** che identifica univocamente l'eseguibile
  - Estensione **.pf**

 CALCULATOR.EXE-EE2573DF.pf	13/03/2019 09:09
 CHROME.EXE-5349D2D7.pf	19/03/2019 09:07
 CHROME.EXE-5349D2D8.pf	19/03/2019 11:37
 CHROME.EXE-5349D2DE.pf	19/03/2019 09:07
 CHROME.EXE-5349D2DF.pf	19/03/2019 09:07
 CMD.EXE-0BD30981.pf	19/03/2019 09:38
 CMD.EXE-6D6290C5.pf	19/03/2019 08:51