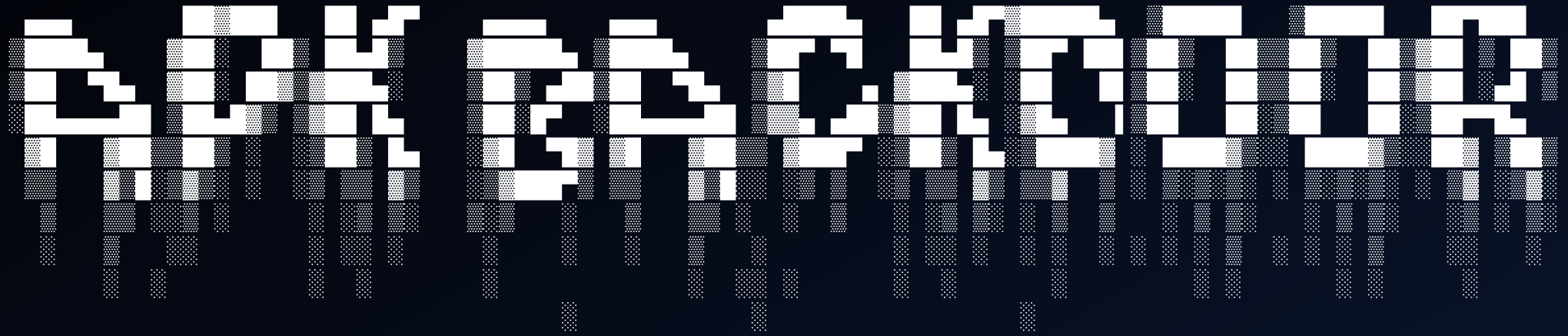
TriSec

PRESENTA

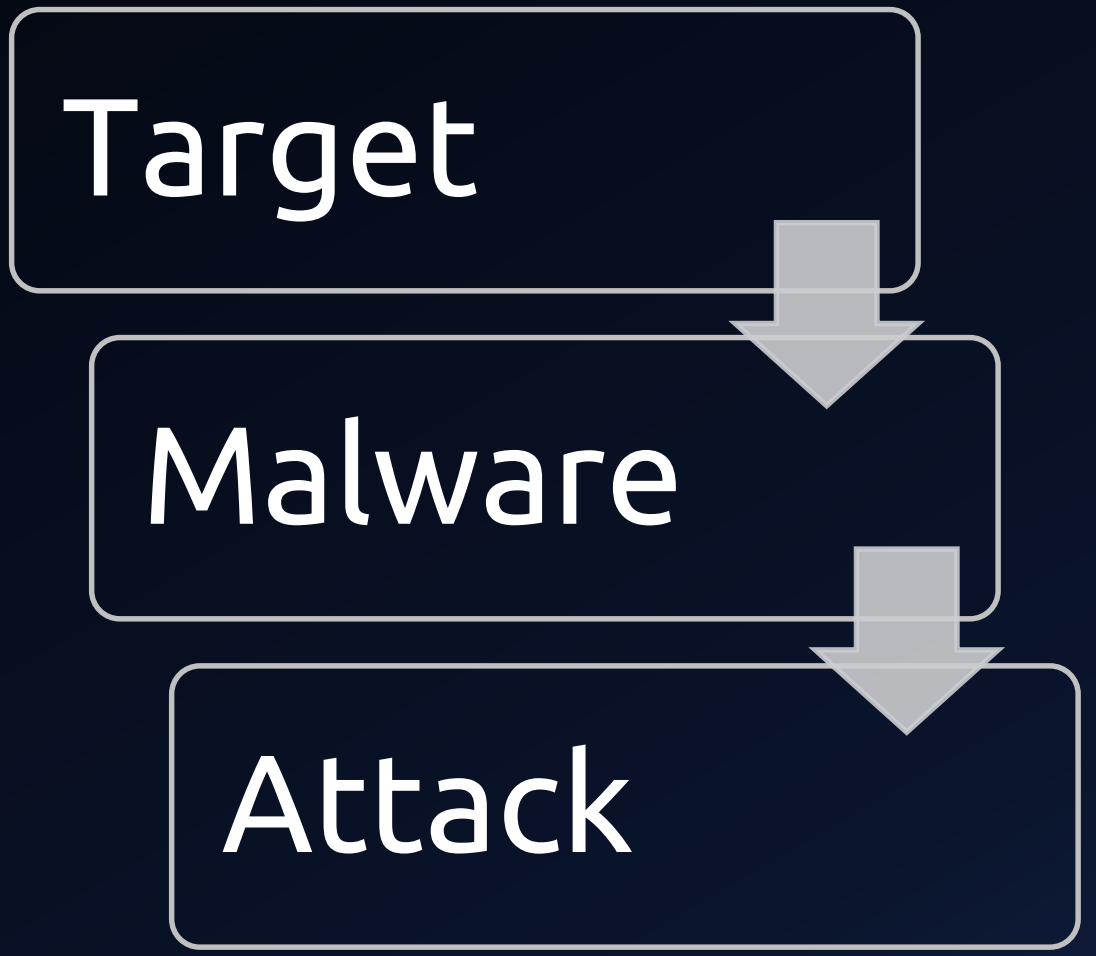


Un tool per generare applicazioni malevole

Alessandro Annese
Andrea Esposito
Graziano Montanaro

Le 7 fasi della KILLCHAIN

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploit
5. Installation
6. Command & Control
7. Action



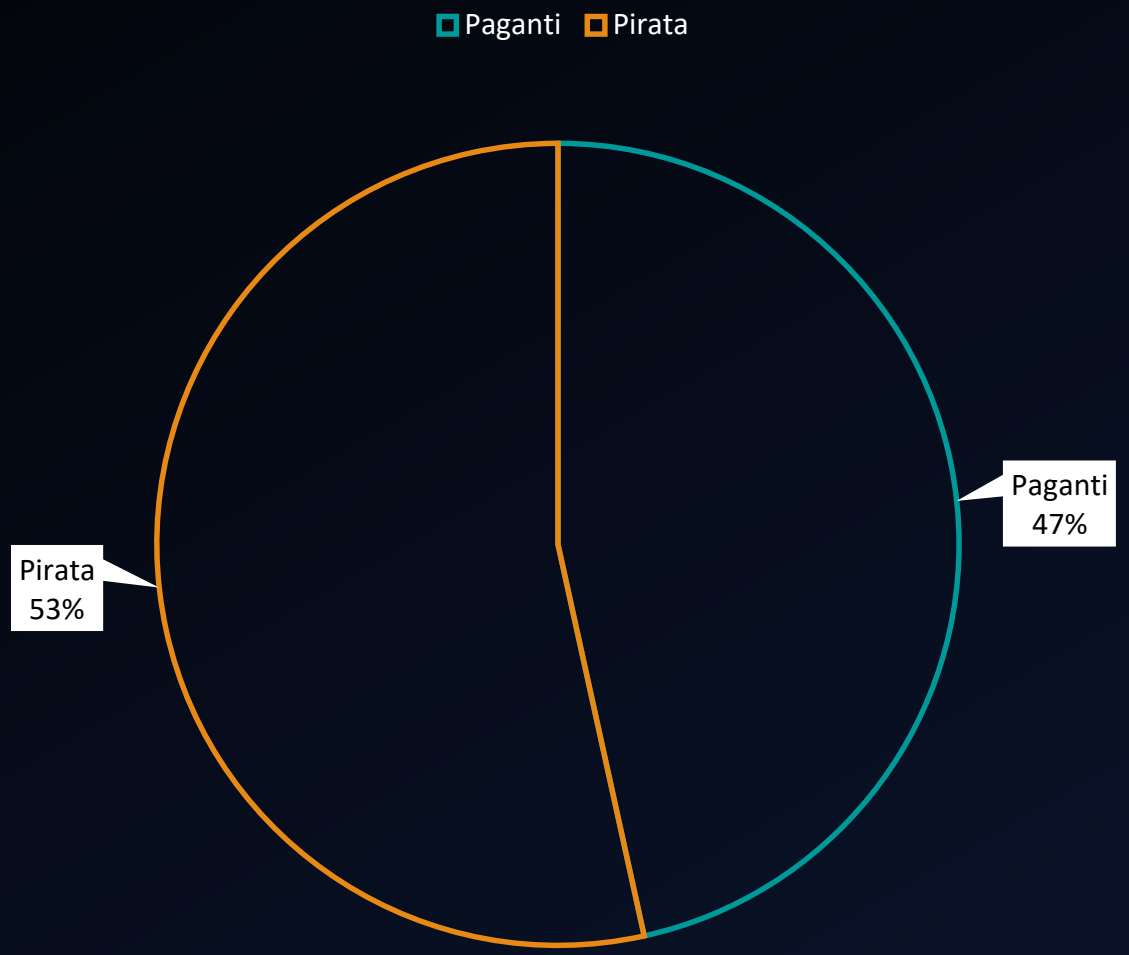
Reconnaissance

1°FASE

Reconnaissance

- L’intera fase di ricognizione in questo attacco è basata sul *social engineering*.
- Al fine di colpire il maggior numero di dispositivi possibili, la fase di ricognizione ha portato al riconoscere l’importanza di applicazioni legate all’ascolto di musica on-demand.
- Una di queste applicazioni è l’applicazione di **Spotify**, installata su diversi dispositivi e che conta numerose applicazioni pirata.

Utenti paganti vs Utenti pirata



Utenti totali: 232 Mln, Utenti non paganti: 124 Mln, Utenti paganti: 108 Mln
Fonte: rollingstone.it - Anno 2019

Weaponization

2°FASE

Weaponization

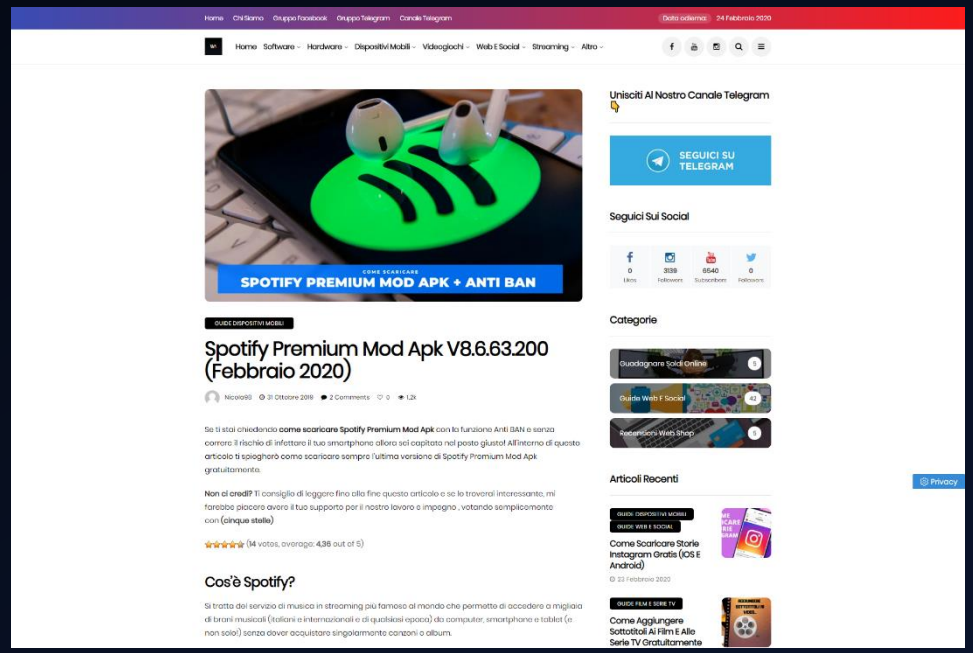
- Creazione di un tool per condurre un meta-attacco su Android mediante backdoor
- Il tool è capace di iniettare una backdoor all’interno di una qualsiasi applicazione
- Creazione di un app pirata di Spotify per testare il tool
- MITRE: T1444

Delivery

3°FASE

Delivery

- La consegna dell’apk malevolo avviene attraverso canali terzi come blog, gruppi o pagine social (Facebook, Telegram ecc…)
- MITRE: T1476



Exploit

4°FASE

Exploit

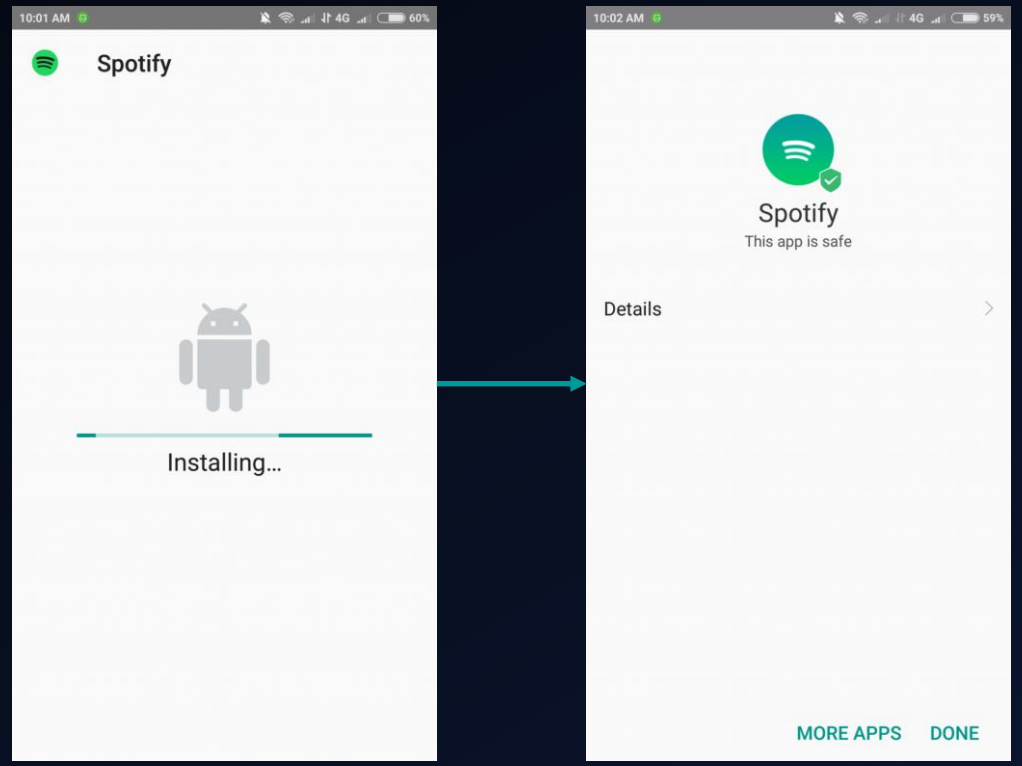
- Durante questa fase si attende che l’utente scarichi e installi l’applicazione malevola
- Questa fase non richiede ulteriori azioni da parte della squadra attaccante
- La backdoor viene avviata non appena viene eseguita l’app per la prima volta
- MITRE: Possibilità di applicare T1402

Installation

5°FASE

Installation

- In questa fase l’utente procede all’installazione dell’applicazione
- Durante questa procedura l’utente acconsente all’utilizzo da parte dell’applicazione di tutte le risorse richieste (comprese quelle del malware)
- MITRE: T1444

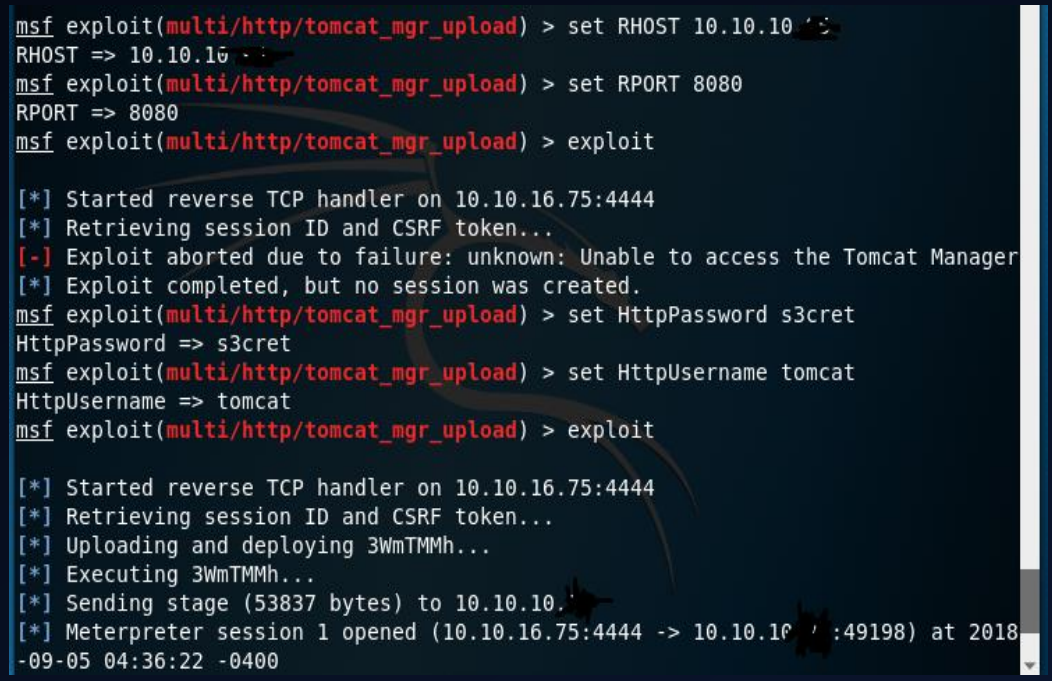


Command & Control

6°FASE

Command & Control

- L’attaccante utilizza una shell sulla propria macchina per controllare a distanza i dispositivi delle vittime attraverso la backdoor precedentemente creata
- Per attivare la shell vengono sfruttati i comandi forniti dal framework Metasploit
- MITRE: T1509

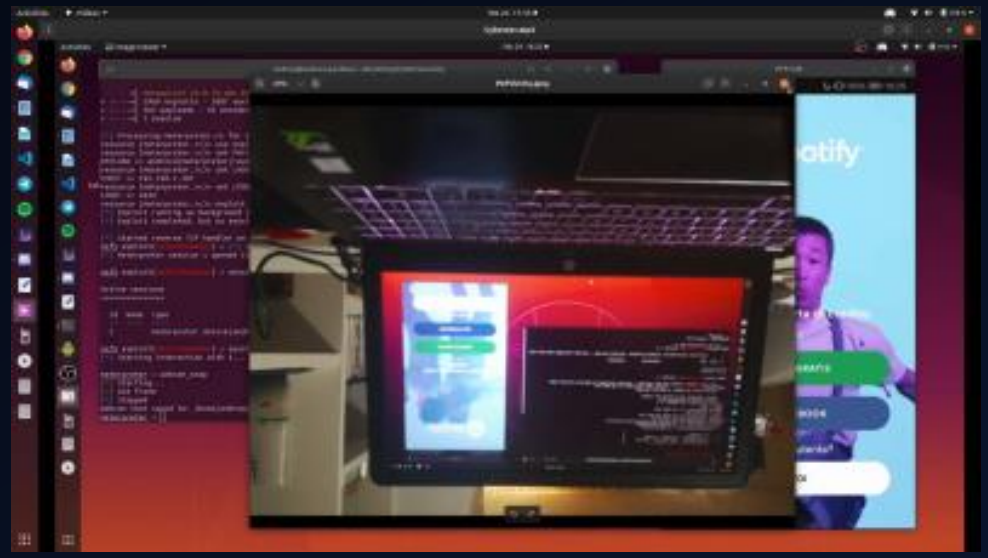


Action

7°FASE

Action

- Trattandosi di un meta-attacco i comandi dipendono strettamente dal tipo di attacco
- Grazie alla backdoor si ha completo accesso al dispositivo ed è quindi possibile effettuare qualsiasi operazione
- Alcuni esempi di attacco sono: Lettura/Invio SMS, Screenshot dello schermo, Utilizzo delle fotocamere, Utilizzo del modulo telefonico ecc…
- MITRE: Tattiche TA0034 e TA0035



Sei ancora convinto di vendere la tua privacy invece di pagare un servizio?

GRAZIE PER L’ATTENZIONE