



Certified Tech Developer

The Ultimate Degree

Práctica Integradora

Objetivo

Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán 10 grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.



Micro desafíos

Deberán leer cada una de las noticias asignadas y responder en un documento (ustedes deben abrirlo) las siguientes consignas:

- ¿Qué tipo de amenaza es?
Spyware. Dos grupos de piratas informáticos patrocinados por el estado que operan desde Palestina. Asociado a PSS (Servicio de Seguridad Preventiva), y Arid Viper
- ¿Cómo comienza y cómo se propaga esta amenaza?
Usaron Facebook como trampolín (operadores del Arid Viper) y luego utilizaron ingeniería social para llegar a miles de personas, lograr que les den permisos de administrador, descarguen apps, y estos roben su información.
- ¿Hay más de una amenaza aplicada ?
El grupo implementó otro malware de Android llamado SpyNote que venía con la capacidad de monitorear llamadas y acceder de forma remota a los teléfonos comprometidos. Por otro lado, se observó que Arid Viper incorporaba un nuevo software de vigilancia iOS personalizado denominado "Phenakite" en sus campañas específicas, que Facebook notó que era capaz de robar datos confidenciales de usuarios de iPhones sin liberar los dispositivos antes del compromiso.

Link a nota:

<https://thehackernews.com/2021/04/facebook-busts-palestinian-hackers.html>