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:

GRUPO 1: https://thehackernews.com/2021/05/new-stealthy-rootkit-infiltrated.html

- ¿Qué tipo de amenaza es?

  Amenaza del tipo rootkit

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Un rootkit es un software diseñado para permanecer oculto en su equipo mientras proporciona acceso y control remotos. Los hackers utilizan los rootkits para manipular un equipo sin el conocimiento ni el consentimiento del propietario.

En el caso de MORIYA, originalmente se infectó un servidor de correo de la víctima para comenzar a mapearlo y luego comenzar a propagarse en entidades diplomáticas asiáticas y africanas y otras organizaciones de alto perfil para hacerse con el control de sus redes y mantener la persistencia durante meses sin ser detectado. El agente de modo de usuario de Moriya se instaló explícitamente usando una línea de comando ejecutada en el servidor de destino de esta manera.
Las víctimas más destacadas fueron dos grandes organizaciones diplomáticas regionales en Asia Sudoriental y África, mientras que todas las demás fueron víctimas en Asia Meridional.

- ¿Hay más de una amenaza aplicada ?

  No, solo fue una sola amenaza aplicada.

Una vez resueltas volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros.

1	https://thehackernews.com/2021/05/new-stealthy-rootkit-infiltrated.html
2	https://thehackernews.com/2021/04/experts-uncover-new-banking-trojan.html
3	https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html
4	https://thehackernews.com/2019/10/42-adware-apps-with-8-million-downloads.html
5	https://thehackernews.com/2020/03/android-apps-ad-fraud.html
6	https://thehackernews.com/2021/02/first-malware-designed-for-apple-m1.html
7	https://thehackernews.com/2021/04/passwordstate-warns-of-ongoing-phishing.html
8	https://thehackernews.com/2021/04/hackers-threaten-to-leak-stolen-apple.html
9	https://thehackernews.com/2021/04/facebook-busts-palestinian-hackers.html
10	https://thehackernews.com/2021/02/chinese-hackers-using-firefox-extension.html
11	https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html

12	https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html