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?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una 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://www.bbc.com/mundo/noticias-56299627

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/2021/04/1-click-hack-found-in-popular-desktop.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

Respuestas (Grupo 3):

1- ¿Qué tipo de amenaza es?

Es un virus de tipo troyano apodado “Saint Bot”.

2- ¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con un correo electrónico de phishing con un archivo ZIP incrustado ("bitcoin.zip") que dice ser una billetera bitcoin cuando, en realidad, es un script de PowerShell bajo la apariencia de un archivo de acceso directo .LNK.

Este script de PowerShell luego descarga el malware de la siguiente etapa, un ejecutable de WindowsUpdate.exe, que, a su vez, suelta un segundo ejecutable (InstallUtil.exe).

El segundo ejecutable se encarga de descargar dos ejecutables más:
def.exe, que deshabilita Windows Defender, y putty.exe, que se conecta a un servidor de comando y control (C2) para una posterior explotación.

Esta mecánica permite a los operadores del malware explotar los dispositivos en los que fueron instalados sin llamar la atención.

3- ¿Hay más de una amenaza aplicada?

Sí. La lista de comandos soportada por el malware incluyen:

- descargar y ejecutar otras cargas útiles recuperadas del servidor C2
- actualizar el malware del bot, y
- desinstalarse de la máquina comprometida

Si bien estas capacidades pueden parecer muy pequeñas, el hecho de que Saint Bot sirva como descargador de otro malware lo hace lo suficientemente peligroso.