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.

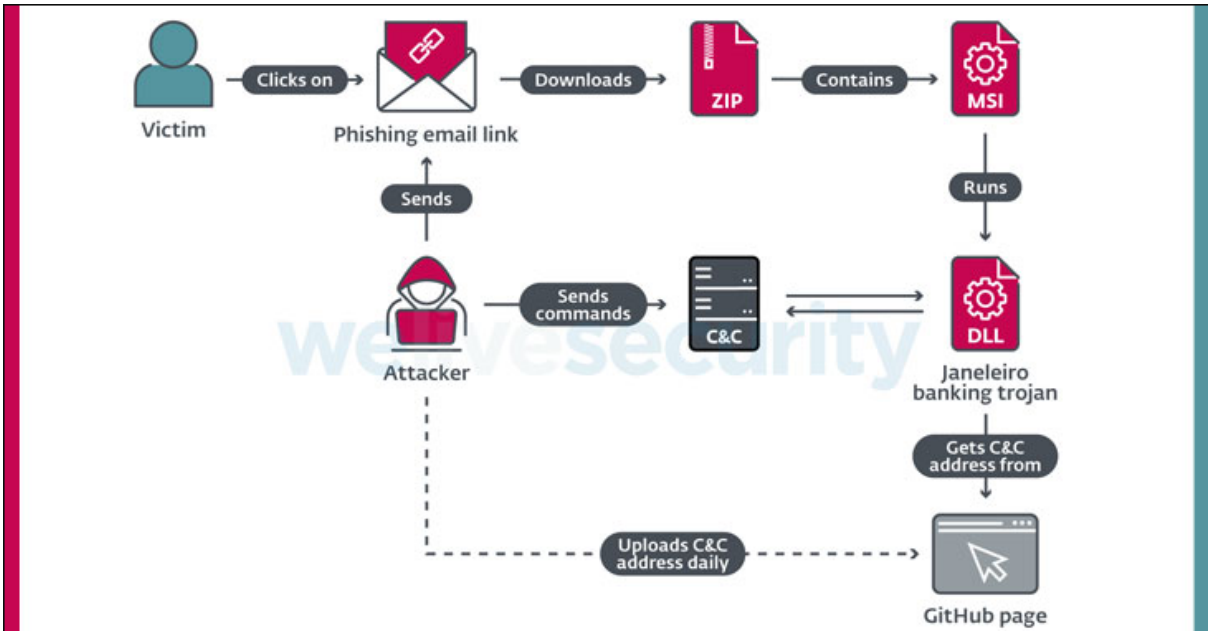
- ¿Qué tipo de amenaza es?

Es una amenaza de tipo troyano.

TROYANOS: No causan daño en sí mismos, pero tienen una estructura para cargar dentro virus, gusanos y demás malwares. Por lo general vienen en los programas sin licencias y cracks. Requieren de la ejecución del usuario, ya que no pueden replicarse a si mismos.

- ¿Cómo comienza y cómo se propaga esta amenaza?

Ya que se disfraza a través de un link que llega por correo electrónico y al clickear sobre este descarga un archivo ZIP con un instalador. Luego de ejecutarse el instalador crea un repositorio local que a través de comandos remotos que el atacante puede controlar. Además, con estos comandos logra que cuando la victima visita los sitios web de bancos le muestra al pop-up's con formularios que al completarlos captura la información sensible.



- ¿Hay más de una amenaza aplicada?

Si, se afirma este troyano reutiliza código de otro troyano denominado NjRAT

Backdoor: es como una puerta trasera para que el dispositivo pueda ser controlado de manera remota por otro usuario. También pueden utilizarlo como un servidor proxy para ocultar ataques. O lo más común, para introducir spam a nuestro equipo.

Spywares: O software espía, no daña el dispositivo pero roba información de contraseñas, información bancaria, puede acceder a la cámara del dispositivo, etc.

Phishing es un tipo de ataque de ingeniería social típicamente utilizado para robar datos del usuario, como credenciales o información de tarjetas de crédito. Ocurre cuando un atacante, disfrazándose de una entidad confiada, engaña a una víctima para que abra un mail, mensaje o chat.

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