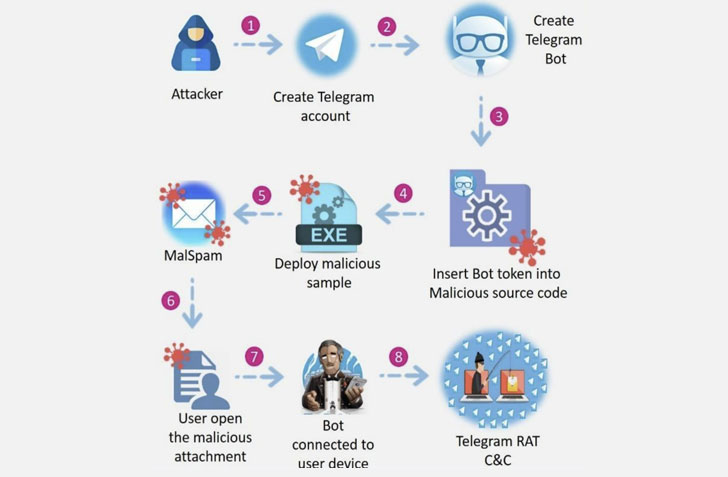
Práctica Integradora - Amenazas informáticas

Grupo 11

Cybercriminals Using Telegram Messenger to Control ToxicEye Malware

*Fuente: https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html*



* **¿Qué tipo de amenaza es?**

Es un troyano de acceso remoto multifuncional (RAT) llamado "ToxicEye".

* **¿Cómo comienza y cómo se propaga esta amenaza?**

ToxicEye utiliza Telegram para comunicarse con el servidor de comando y control (C2) y cargar datos en él. El malware cuenta con una serie de exploits que le permiten robar datos, transferir y eliminar archivos, terminar procesos, desplegar un keylogger, secuestrar el micrófono y la cámara del ordenador para grabar audio y vídeo, e incluso cifrar archivos para pedir un rescate.

1. Creación de una cuenta de Telegram y un bot “Telegram” exclusivo. Una cuenta de bot de Telegram es una cuenta remota especial en la que los usuarios pueden interactuar mediante el chat de la app, o agregándole a grupos de la misma, o enviando peticiones directamente desde el formulario de entrada escribiendo el nombre de usuario del bot y una consulta.
2. El bot (su identificación o token) se incorpora en el fichero de configuración del RAT ToxicEye y se compila en un fichero ejecutable.
3. El malware se propaga a través de campañas de spam como un archivo adjunto de correo electrónico. Un ejemplo de nombre de archivo encontrado por CPR (Check Point Research Technologies) fue ‘paypal checker by saint.exe’
4. La víctima abre el archivo adjunto malicioso que se conecta a Telegram. Cualquier víctima infectada con este payload malicioso puede ser atacada a través del bot de Telegram, que conecta el dispositivo del usuario con el C&C (Command and control) del ciberdelincuente a través de la app.
5. El ciberdelincuente se hace con el control total del dispositivo de la víctima y puede llevar a cabo una serie de actividades maliciosas.

* **¿Hay más de una amenaza aplicada ?**

Se utiliza como un sistema de "comando y control" para distribuir malware en organizaciones que luego podrían ser utilizadas para capturar información confidencial de sistemas específicos. Malware, Keylogger y uso de exploits.