Certified Tech Developer
The Ultimate Degree

Práctica integradora

Objetivo

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

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

- ¿Qué tipo de amenaza es?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada?
- ¿Qué solución o medida recomendarían?

Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.

https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/

1. **¿Qué tipo de amenaza es?**

   Es un backdoor junto con un troyano.

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

   Los atacantes han estado distribuyendo sus herramientas a través de correos electrónicos maliciosos (“malspam”) con enlaces que conducen a un archivo malicioso.

   Con frecuencia, los enlaces que conducen a un archivo ejecutable se disfrazan como enlaces a un PDF. El archivo ejecutable es un WinRAR auto extraíble cuyo nombre e icono son modificados para parecerse a un archivo PDF y así engañar al usuario. Una vez que se ejecuta, está configurado para desempaquetar su contenido, abrir el PDF utilizado como señuelo para evitar cualquier sospecha y ejecutar silenciosamente BalkanRAT o BalkanDoor.

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

   Sí, el backdoor y el troyano al desempaquetar sus componentes instalan además un rootkit, un keylogger, scripting. Lo que permite:

   - Control remoto de la computadora
   - Espionaje y robo de información
   - Concede permisos privilegiados para realizar cualquier tipo de acciones sobre el dispositivo

4. **¿Qué solución o medida recomendarían?**

   - No descargar archivos sospechosos desde el correo electrónico.
   - Comprobar la procedencia de los archivos.

- Si ya se ha descargado el malware, desconectar el cable de red, wifi y realizar instalación de antivirus o cualquier herramienta de seguridad de pago.