Amenazas Informáticas Grupo 2

BackdoorDiplomacy es también un grupo multiplataforma dirigido a sistemas Windows y Linux. El grupo apunta a servidores con puertos expuestos a Internet, probablemente explotando la seguridad de carga de archivos mal ejecutada o vulnerabilidades sin parchear.

Un subconjunto de víctimas fue atacado con ejecutables de recopilación de datos que fueron diseñados para buscar medios extraíbles (probablemente unidades flash –USB). El implante busca de forma rutinaria dichas unidades y, al detectar la inserción de un medio extraíble, intenta copiar todos los archivos que contienen en un archivo protegido con contraseña. BackdoorDiplomacy es capaz de robar la información del sistema de la víctima, tomar capturas de pantalla y escribir, mover o eliminar archivos.

● ¿Qué tipo de amenaza es?

Spywares no causan daños los dispositivos, su objetivo es permanecer oculto para robar todo tipo de datos, "ROBO DE INFORMACION BANCARIA" entra en forma de troyano.

Pueden crear backdoors, que es una puerta trasera para que un dispositivo pueda ser controlado de forma remota por alguien más. Pueden usarlo como un servidor proxy para ocultar ataques o para introducir span.

● ¿Cómo comienza y cómo se propaga esta amenaza?

Su modo de ataque es permanecer oculto para robar los datos, pueden ingresar desde las cámaras de los dispositivos y pueden ingresar al sistema por medio de troyanos o por medio de instalaciones de programas que se instalan sin pensar que harán daño.

● ¿Hay más de una amenaza aplicada?

Ransomware Sofware de secuestro.

● ¿Qué solución o medida recomendarían?

- Antivirus inicialmente, eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación.
- También podemos recurrir a otros programas de limpieza, como CCleaner o Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.
- Implementa la seguidad activa y pasiva
- Implementar seguridad física y lógica.

- Hacer auditoria para detectar las vulnerabilidades, prevenir ante próximos ataques.