Publicado en Madrid el 30/11/2023

El sector financiero ha sido uno de los más ciberatacados en 2023

Con motivo de la celebración del Día Internacional de la Seguridad de la Información, S2 Grupo ha destacado que uno de los sectores más ciberatacados en 2023 está siendo el financiero. Como principales amenazas, la empresa de ciberseguridad destaca los grupos APT, que a menudo trabajan en favor de los intereses de Estados soberanos, las bandas organizadas de cibercrimen que buscan el lucro por medio del fraude, y los grupos de hacktivistas que buscan promover ideas políticas, religiosas o sociales

En este contexto, desde la empresa S2 Grupo, especializada en ciberseguridad y gestión de entornos críticos, han destacado en un comunicado que "el sector financiero es uno de los objetivos más atacados en la actualidad y de que el cibercrimen vaya en aumento, las transformaciones digitales dentro del sector son una gran preocupación para las empresas a nivel mundial y hace que las posibilidades de ataque crezcan". Esto requiere conocer el comportamiento de los ciberdelincuentes para poder protegerse adecuadamente e impulsar la seguridad financiera digital, añaden.

Como ha explicado el equipo de expertos de esta compañía, los ciberdelincuentes para ejecutar sus ataques emplean las llamadas 'Técnicas, Tácticas y Procedimientos' (TTPs) que son comportamientos de ataque ejecutados contra las organizaciones víctimas.

"Los profesionales de ciberseguridad del sector financiero deben tener correctamente identificadas las TTPs que usan con mayor frecuencia los principales grupos hostiles que actúan contra las organizaciones del sector financiero porque es el único camino para poder implementar herramientas específicas que detecten estas amenazas e iniciar la mitigación del intento de intrusión o de respuesta de incidente", ha enfatizado José Rosell, socio director de S2 Grupo.

¿Quién amenaza la seguridad digital del sector financiero y cómo actúan?
Desde S2 Grupo se ha señalado que los principales actores hostiles del sector financiero son:

1. Grupos APT (amenazas persistentes avanzadas).
Estos tienen altos conocimientos técnicos, experiencia y gran cantidad de recursos que emplean para infiltrarse en las redes y sistemas de sus víctimas con el objetivo de acceder a información confidencial, sabotear las operaciones de sus contrincantes o establecer una persistencia para llevar a cabo estas acciones en el futuro. Las APT se caracterizan por la tenacidad en la búsqueda de sus objetivos a lo largo del tiempo, la capacidad de adaptarse a los esfuerzos defensivos de sus adversarios y la determinación para mantener un nivel continuo de interacción necesario para alcanzar sus metas .

A menudo, son agencias de inteligencia internas o externas que trabajan en favor de los intereses de un Estado, proporcionando inteligencia que ayude a sus dirigentes en la toma de decisiones estratégicas.

Sus objetivos son: atender a los intereses militares, políticos, económicos y de seguridad interna, la recopilación de información sobre inteligencia y seguridad nacional, además de inteligencia exterior, de objetivos militares, estratégicos, económicos, científicos y tecnológicos, de recopilación de información y robo financiero para financiar regímenes.

Algunas TTPs de estos grupos de ciberdelinciencia son:

- Explotación de vulnerabilidades poco tiempo después de ser publicadas por los fabricantes o, incluso, desconocidas por los propios fabricantes de un dispositivo.
- Empleo de ingeniería social para el acceso inicial o para la descarga de artefactos maliciosos.
- Empleo de servicios cloud legítimos como Yandex, Dropbox y Google Drive para diseminar malware y exfiltrar datos de las máquinas de sus víctimas.
- Uso de archivos con doble extensión para confundir al usuario.
- Crea servicios, tareas programadas y modificar claves de registro para establecer persistencia.

2. Cibercrimen

La mayoría de los delitos cibernéticos son cometidos por ciberdelincuentes o piratas informáticos que quieren ganar dinero. Sin embargo, en ocasiones el ciberdelito tiene como objetivo dañar ordenadores o redes por motivos distintos al lucro que podrían ser políticos o personales.

En este caso pueden desarrollarse diferentes tipos de actividades delictivas como ataques de ransomware, fraude por correo electrónico e Internet y fraude de identidad, así como intentos de robar información de cuentas financieras, tarjetas de crédito u otra información de tarjetas de pago. De hecho, el ransomware como servicio se ha convertido en una de la principales ciberamenazas a nivel global.

Algunas TTPs que se pueden destacar en este grupo son:

- Uso de exploits y vulnerabilidades de software sin parches para obtener acceso no autorizado a los sistemas.
- Phishing con archivos adjuntos o enlaces maliciosos.
- Uso de credenciales válidas.
- Firmas digitales para eludir medidas de seguridad específicas EDR (Endpoint Detection and Response).
- Robo de datos y doble extorsión (amenaza con publicación).
- Desactivar soluciones antimalware y de monitorización.
- Uso de WinRAR para comprimir los archivos.

3. Grupos hacktivistas

El hacktivismo consiste en la realización de ciberataques para promover unas ideas políticas, religiosas o sociales. El sector financiero es uno de los sectores más atacados por los grupos hacktivistas debido

a que una de sus principales motivaciones es crear disrupción en los sistemas de la víctima y tener impacto mediático. De este modo le generan un enorme desprestigio a la empresa u organización.

Algunas de las TTPs más utlizadas por grupos hacktivistas contra el sector financiero son:

Escaneo de vulnerabilidades basado en botnets con dispositivos IoT días antes de los ataques de denegación de servicio.
Uso del software DDoSIA para realizar ataques DDoS.
Servidores de comando y control distribuidos, que tienen la tarea de enviar objetivos para que sean atacados por los usuarios de la plataforma DDoSIA.
Uso de GodzillaBotnet para llevar a cabo sus ciberataques, botnet también asociada al grupo SkyNet.
Lanzamiento de ataques HTTP. Han enviado inundaciones de tráfico HTTP específicamente diseñadas para abrumar la infraestructura específica.
Especializados en DDoS, Hacking, Doxing y Defacement.
Ataques de diccionario de fuerza bruta.
Ataques DDoS en el modelo OSI.

Ante este contexto, el equipo de expertos de S2 Grupo ha resaltado que algunas recomendaciones básicas para la ciberprotección del sector financiero son llevar a cabo tareas de revisión proactiva como un servicio de threathunting, disponer de un proveedor de inteligencia que mantenga al cliente actualizado respecto a las nuevas TTPs usadas por los actores hostiles e integrar las reglas proporcionadas por el proveedor de inteligencia dentro del sistema perimetral de defensa de la entidad.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Finanzas Madrid Software Ciberseguridad