El ciber espionaje no es solo de película, también afecta tu dispositivo

Por staff de redacción Infosecurity Mexico

¿Qué es el ciber espionaje? Bueno, es el tipo de ciberataque en el que un usuario no autorizado intenta acceder a información sensible o clasificada, o propiedad intelectual de un tercero, para buscar un beneficio económico, ventaja competitiva, o motivado por razones políticas, aunque en algunos casos busca tan solo ocasionar un daño a la víctima exponiendo su información privada, o bien, dar a conocer prácticas de negocios cuestionables.

Aunque la mayoría de los ataques de ciber espionaje están motivados por ganancias monetarias, incluso también pueden ser desplegados en conjunto con operaciones militares o como actos de ciber terrorismo o ciber guerra. En este caso, su impacto, sobre todo cuando es parte de una campaña militar o política mayor, puede llevar a la disrupción de servicios públicos, infraestructura, así como a pérdida de vidas.

Los objetivos más comunes de los ataques de ciber espionaje son las grandes corporaciones, agencias de gobierno, instituciones académicas, institutos de investigación y otras organizaciones como las ONGs, que tienen valiosa propiedad intelectual o información técnica que puede darle una ventaja competitiva a otra organización o gobierno. Por otro lado, algunas veces las campañas pueden ser en contra de individuos, como prominentes líderes políticos, funcionarios de gobierno, ejecutivos corporativos y hasta celebridades.

Tácticas de ciber espionaje: La mayor parte de los ataques de ciber espionaje configuran una amenaza persistente avanzada (APT) en la que el intruso establece una presencia no detectada en la red para robar información sensible en cierto lapso. Este tipo de ataque requiere una cuidadosa planeación y diseño para infiltrar a una organización y evadir los sistemas de seguridad por largos periodos; exige un alto grado de sofisticación y los realizan equipos experimentados de cibercriminales, bien fondeados, cuyos objetivos son las organizaciones de alto valor. Además, invierten grandes cantidades de tiempo y recursos para investigar e identificar vulnerabilidades.

La mayoría de los ataques también se basan en la llamada ingeniería social para reunir la información necesaria del objetivo para realizar la intrusión. Estos métodos explotan emociones humanas como excitación, curiosidad, empatía o miedo para que las “víctimas” actúen rápido y, al hacerlo, los cibercriminales los engañan para obtener información personal dando clic en enlaces maliciosos, con lo que descargan malware o se les fuerza a pagar un rescate.

Otras técnicas de ataque incluyen el **watering-hole**, en el que los actores maliciosos infectan sitios legítimos que comúnmente usa la víctima o gente cercana para comprometer al usuario; el **spear-phishing**, en donde el agresor ataca a sus víctimas con correos, textos y llamadas fraudulentas para robar credenciales o información sensible; el **Zero-day exploits**, mediante el que los cibercriminales aprovechan alguna vulnerabilidad de seguridad o falla del software antes de que sea “parchada”; y las **amenazas internas**, en las que se convence a algún empleado o proveedor a compartir o vender información o acceso al sistema a usuarios no autorizados.

Cómo prevenir el ciber espionaje: Detectar a los ciber espías es uno de los retos más grandes para los equipos de seguridad de cualquier organización, ya que sus ataques son muy sofisticados y silenciosos en la red. Por ejemplo, el Reporte de Ciber Espionaje de Verizon encontró muchos ejemplos que comprometieron a sus usuarios en minutos, o incluso segundos, mientras que las organizaciones tardaron meses o años en descubrir el ataque.

Pero ante tales prácticas, existen algunas prácticas generales de ciber higiene que ayudan a protegerse; la principal es mantener el software actualizado, pero hay algunas consideraciones especiales que pueden ayudar a mitigar el riesgo del ciber espionaje:

Observar el comportamiento, acciones y anomalías: Los ciber espías pueden ser tan sofisticados que es difícil detectarlos con productos de seguridad, por lo que es mejor buscar anomalías en el comportamiento de usuarios y entidades a través de analíticos para detectar signos de ataques y robo de datos, ya que no se consideran registros de ataques anteriores; más bien

usan modelos de comportamiento que aprenden lo que es “normal” de cada usuario y dispositivo, y detectan amenazas potenciales por actividad inusual.

Utilizar contraseñas fuertes y autenticación multifactor: El robo de credenciales es redituable para los ciber espías porque no disparan alarmas. Por ello, las organizaciones con información confidencial o sensible deben tener políticas de bloqueo de contraseñas y monitoreo de cuentas para así detectar ataques, exitosos o no, y pueden ser críticos para conocer los movimientos del atacante luego de su intento inicial.

Control de acceso y principio de menores privilegios: Este principio puede ser muy efectivo contra las campañas de espionaje y robo de datos, y se basa en que los usuarios deben tener los menores privilegios posibles de acceso para realizar su trabajo dentro de la organización, tanto para que no pueda entrometerse en otras áreas como para que, si sus credenciales son robadas, no puedan tener acceso irrestricto a los sistemas de la empresa.

Educar a los empleados y construir cultura de seguridad: Los programas de ciberseguridad completos deben incluir el elemento humano para ser efectivos. El entrenamiento de consciencia de seguridad es la mejor defensa contra los ataques de ingeniería social, por lo que es esencial enseñar a los empleados a identificar signos de phishing, pretexting y carfishing para que los espías no puedan meter un pie en el sistema.

Implementar cero confianza: En este modelo todos los dispositivos y usuarios en una organización se consideran potencialmente comprometidos por los adversarios hasta que prueben lo contrario.

Hay que tener en cuenta que aún cuando muchos países han acusado a terceros por actividades de ciber espionaje, en la mayoría de los casos los atacantes se encuentran en otros países en donde no son sujetos a extradición, por lo que las agencias de hacer cumplir la ley no tienen poder para perseguirlos. Por esto, lo más conveniente es la prevención para evitar lo más posible ser víctima de estos delincuentes.

La invitación es a que usuarios y encargados de seguridad se protejan con herramientas e inteligencia, bajo el entendido de que los cibercriminales generalmente buscan ir uno o dos pasos delante de nosotros. Por eso vale la pena darse una vuelta a foros como Infosecurity Mexico para conocer la última tecnología en ciberseguridad y las prácticas más actualizadas.