Reflexionando sobre las tendencias emergentes de ciberamenazas

Tras finalizar el Mes de Concientización sobre Ciberseguridad 2021, celebrado en octubre, considero que es un excelente momento para reflexionar sobre dos cosas sumamente importantes hoy en día: la ciberseguridad y las tendencias clave y emergentes del año pasado.

La seguridad digital está en cada uno de nosotros, bien sea organización, gobierno o colaborador, todos podemos generar conciencia y es importante hacerlo no solo un mes al año, sino el año completo ya que está en constante movimiento y evolución.

Por su parte, en relación a las tendencias clave y emergentes del año pasado, es importante señalar que no ha habido escasez de titulares de seguridad sobre los cuales reflexionar, por lo que hablaré sobre tres cuestiones clave que me llamaron especialmente la atención.

Antes de 2021, se suponía que los ataques a la cadena de suministro eran exclusivamente una herramienta solo para actores de amenazas sofisticados patrocinados por el Estado. Se pensaba que los recursos y conocimientos necesarios para comprometer a un proveedor de software e integrar código malicioso estaban fuera del alcance de los actores de amenazas criminales, sin embargo, en julio de 2021 esta suposición fue desarticulada.

REvil es un ransomware que se distribuyó a través de la explotación de una vulnerabilidad previamente no identificada en el código del servidor de Kaseya VSA, herramienta utilizada para monitorear y administrar un gran número de sistemas en una amplia variedad de organizaciones. El impacto de este ataque fue más amplio de lo que podría imaginarse. Golpear los servidores dentro de los proveedores de servicios administrados se tradujo en un servidor violado que afectó a muchas organizaciones. Por su parte, detener muchas empresas significa más pagos de rescate potenciales, por lo tanto esta será una táctica tentadora para muchos otros atacantes en el futuro.

En muchos sentidos, los actores de APT actúan como líderes de pensamiento para el resto del panorama de amenazas, mostrando lo que un actor ambicioso y efectivo puede lograr. Es posible que los actores criminales que llevaron a cabo el ataque de Kaseya hayan tenido algún tipo de apoyo o protección estatal, o que hayan logrado el ataque completamente a través de sus propios esfuerzos. En cualquier caso, es probable que veamos más casos de cadenas de suministro que se utilizan para distribuir malware en el futuro.

Los actores de amenazas criminales están motivados por las ganancias y uno de los modelos de negocio más exitosos que han creado es el ransomware, donde un sistema puede detenerse cifrando datos y requiriendo un pago para que el sistema vuelva a la normalidad. Aunque es lucrativo, este modelo tiene debilidades para el atacante. El flujo de ingresos se basa en la búsqueda continua de nuevas víctimas, lo que requiere tiempo y recursos. Si el compromiso es solo un inconveniente menor para la víctima, y en ausencia de una copia de seguridad que funcione, la víctima puede optar por volver a imaginar el sistema.

La persistencia en un sistema comprometido puede ofrecer más oportunidades para extraer valor

que el enfoque de una sola toma del ransomware. Apropiarse de recursos de sistemas comprometidos fue una táctica implementada por muchas de las primeras botnets, donde el controlador robó recursos, incluido el ancho de banda de la red, mediante el envío de spam o el lanzamiento de ataques de denegación de servicio desde los sistemas de sus víctimas infectadas.

En los últimos años, los atacantes han desarrollado criptomineros para robar recursos informáticos de sistemas comprometidos. Este proceso requiere grandes cantidades de potencia informática para resolver los desafíos criptográficos necesarios para adquirir nuevos tokens. Desarrollar y operar las instalaciones informáticas legítimas para lograr los cálculos necesarios es costoso. Sin embargo, robar estos recursos es fácil por lo tanto, vemos el desarrollo de malware de criptominería como un proceso de fondo en sistemas comprometidos, robando recursos para ganar dinero.

Aunque el beneficio de un solo sistema es pequeño, los atacantes pueden persistir en sistemas comprometidos durante largos períodos de tiempo y controlar y afectar a un gran de ellos.

En los últimos dos años, durante la pandemia de COVID-19, hemos visto un aumento sin precedentes del trabajo remoto y del uso de servicios entregado en la nube. Con los usuarios y los sistemas a los que acceden fuera del entorno de oficina tradicional, la cuestión de cómo autenticar a los usuarios se ha vuelto cada vez más importante.

Los nombres y las contraseñas nunca han sido un mecanismo particularmente seguro para verificar las identidades de los usuarios, ya que estos son propensos a revelar sus datos en respuesta a las señales de ingeniería social de los ataques de phishing. Los estudios han demostrado que los usuarios incluso revelarán voluntariamente su contraseña a cambio de un chocolate. El uso continuo de sistemas heredados, las malas elecciones en la implementación del sistema o los malos algoritmos hash han permitido a los atacantes recopilar un gran número de nombres de usuario y pares de contraseñas de texto sin formato.

Es en este momento donde el uso de la autenticación multifactor es un factor fundamental porque ofrece una capa adicional de seguridad. Estos enfoques, requieren que los usuarios se autentiquen con un método de inicio de sesión adicional, como responder a una alerta en su dispositivo móvil ya que estos con frecuencia están protegidos por datos biométricos, como una huella digital.

Sin embargo, el reconocimiento biométrico se basa en una “cadena de custodia” segura. El dispositivo de lectura de la huella, el software que interactúa con el dispositivo de huellas dactilares y la conexión que transmite el resultado al sistema de autenticación debe ser seguro. Nada de esto puede darse por sentado.

Hemos demostrado que es posible imprimir en 3D una huella digital que engañará a los sistemas de lectura con equipos de impresión 3D de grado de consumidor y nada más que un escaneo de la huella dactilar del usuario. Esto significa que cualquier actor de amenazas con recursos adecuados podría desarrollar técnicas de clonación de huellas para engañar al reconocimiento biométrico. Si bien la biometría ofrece una vía adicional de autenticación, todos debemos ser conscientes del hecho de que el mundo de la biometría también abre la posibilidad de nuevos tipos de ataques.