Tendencias 2022:
los ciberdelincuentes también se fortalecen con las innovaciones

mexis aggity

El 2021 ha sido otro año marcado por cambios continuos que empujaron a las empresas a adoptar nuevas estrategias para fortalecer la resiliencia. Del mismo modo, los ciberdelincuentes continuaron refinando sus métodos para trabajar de manera más inteligente y moverse más rápido para escalar los ataques, extenderse más profundamente en las cadenas de suministro y causar un mayor daño.

Especialistas han observado los primeros signos de la evolución de los atacantes. Cada uno tiene el potencial de alterar significativamente el panorama de la ciberseguridad en los próximos 12 meses. Aquí, las innovaciones más relevantes:

Empresas criminales clandestinas

DevOps –una combinación de los términos development (desarrollo) y operations (operaciones), cuya práctica automatiza y optimiza los procesos con tecnología– está cambiando la forma en que se hacen los negocios, y las empresas criminales no son la excepción.

Al igual que los proveedores de software legítimos, los atacantes están utilizando pipelines de CI / CD, infraestructura en la nube y otras tecnologías digitales para desarrollar y vender malware como servicio (MaaS), impulsada por la creciente demanda clandestina de herramientas populares como el malware de
robo de credenciales, que se puede configurar para recopilar contraseñas de los usuarios y saquear la información privilegiada de las víctimas.

Dicho malware no solo es poderoso, sino que también es fácil de usar desde el primer momento, empoderando a los ciberdelincuentes.

Los grupos de atacantes aprovechan el interés para monetizar estos servicios y hacer crecer sus operaciones. A medida que estos grupos criminales comienzan a aparecer cada vez más como negocios reales, también se abrirán a nuevos riesgos.

Los ciberdelincuentes automatizarán los ataques a la cadena de suministro

La economía digital se ejecuta en software de código abierto (OSS): es flexible, escalable y aprovecha el poder colectivo de la comunidad para generar innovaciones. Pero innumerables bibliotecas OSS abiertas y gratuitas también significan una superficie de ataque dramáticamente expandida y una forma para que los actores de amenazas automaticen sus esfuerzos, eludan la detección y hagan más daño.
La violación de Codecov de abril de 2021 nos dio una idea de cómo un ajuste sutil en una línea de código puede convertir una biblioteca completamente benigna en una maliciosa, poniendo en riesgo a cualquier organización que la use. Utilizando este método de infiltración altamente evasivo, los atacantes pueden apuntar y robar credenciales para llegar a miles de organizaciones a través de una cadena de suministro al unísono.

En los próximos 12 meses, los atacantes continuarán buscando nuevas formas de comprometer las bibliotecas de código abierto. Hemos visto a atacantes implementar ataques tipo typosquatting mediante la creación de paquetes de código que incluyen cambios sutiles en los nombres de los paquetes (es decir, atlas-client vs. atlas-client). Estas eran en realidad versiones troyanizadas de los paquetes originales, que implementan o descargan una funcionalidad de puerta trasera o de robo de credenciales.
En otro caso, un paquete NPM fue troyano para ejecutar scripts de criptominería y malware de robo de credenciales después de que los accesos de un desarrollador se vieron comprometidos.
Las organizaciones deben permanecer vigilantes, ya que estos ataques sutiles rara vez enviarán señales, lo que los hace extremadamente difíciles de detectar, especialmente porque las bibliotecas se implementan como parte de las operaciones diarias legítimas y, en muchos casos, pueden parecer benignas, ya que el código malicioso se descarga como una dependencia.
Además, dado que estos ataques automatizados son fáciles y rápidos de ejecutar con una firma muy limitada, se volverán aún más frecuentes, repentinos y dañinos.
Nuevos puntos ayudarán a ciberdelincuentes a esconderse a plena vista.

Como si no fuera suficientemente complicado, la seguridad será más desafiante gracias a los nuevos escondites introducidos por la nube, la virtualización y las tecnologías de contenedores.

Por ejemplo, a medida que la micro virtualización se vuelve cada vez más popular, los actores de amenazas pueden aislar el malware en estos sistemas virtuales mientras lo mantienen oculto de los controles de seguridad basados en host.

Si bien estas nuevas técnicas de ataque no se han visto mucho en la realidad aún, al menos no todavía, se han observado actores de amenazas financieramente motivados y criminales que prueban sistemas que aseguran los procesos de credenciales y autenticación, mientras buscan nuevas formas de comprometer las máquinas de punto final.

Fuente de información: www.forbes.com.mx