INFORME

Predicciones de ciberamenazas para 2024

Una perspectiva anual de FortiGuard Labs

FORTINET

Contenido

La evolución de los viejos favoritos 3

Tendencias de ataques únicos a tener en cuenta a partir de 2024. 5

Estrategia a largo plazo (del atacante) 7

Mejorar nuestra resiliencia colectiva frente al panorama de amenazas en evolución 7

Acerca de FortiGuard Labs 8

Introducción

Los adversarios siempre descubren nuevas formas de comprometer redes; sin embargo, ejecutar ataques exitosos no siempre ha sido directo o rápido. Pero hoy, gracias al crecimiento del mercado del cibercrimen como servicio (CaaS) y al auge de la IA generativa, los ciberdelincuentes tienen más botones "fáciles" que nunca. ¿El resultado? Los atacantes ampliarán su enfoque de "trabajar de manera más inteligente, no más duro" frente al cibercrimen, confiando en gran medida en las nuevas funciones de sus respectivas cajas de herramientas.

El informe de predicciones de amenazas de este año examina una nueva era de cibercrimen persistente avanzado, analiza cómo la inteligencia artificial está cambiando el juego de los ataques, comparte nuevas tendencias para observar en 2024 y más. Aquí tenemos una semblanza de cómo esperamos que evolucione el panorama de amenazas y nuestros mejores consejos para proteger su organización.

La evolución de los viejos favoritos

Durante años, hemos hablado de muchas tendencias de ataques, incluso en nuestro Informe de predicciones de amenazas para 2023, señalando cómo esperamos que evolucionen estas tácticas favoritas de los fanáticos en los próximos días. Por ejemplo, hemos sido testigos de cómo el cibercrimen persistente avanzado es cada vez más sofisticado y dirigido, el aumento de guerras territoriales más intensas entre grupos de cibercrimen y un cambio en la forma en que se utiliza la IA para soportar los ataques. A continuación echamos una mirada retrospectiva a algunas predicciones clave para 2023 y nuestra opinión sobre cómo estas tendencias de larga duración cambiarán en el panorama de amenazas a partir de 2024.

Una nueva era de cibercrimen persistente avanzado

Durante los últimos años, hemos predicho que el crecimiento de nuevas vulnerabilidades combinado con una mayor actividad previa al ataque entre los adversarios allanaría el camino para la expansión del mercado del CaaS. Hoy, a medida que los ciberdelincuentes y los grupos de amenazas persistentes avanzadas (APT) continúan trabajando juntos (hay más en la *dark web* que nunca), podemos decir con seguridad que nuestra predicción se hizo realidad.

Desafortunadamente para los profesionales de la seguridad, esto es sólo la punta del iceberg. La actividad de APT va en aumento. En el primer semestre de 2023, presenciamos una actividad significativa entre los grupos APT, con 41 (alrededor del 30%) de los 138 grupos que MITRE rastrea estando activos durante este periodo. De ellos, Turla, StrongPity, Winnti, OceanLotus y WildNeutron fueron los más activos, según las detecciones de malware de nuestro FortiGuard Labs.

Mirando hacia el futuro, predecimos que aún más de estos grupos de APT se volverán más activos, incluso más allá de los 138 identificados por MITRE y aquellos que CISA describe con ciclos activos, y es probable que participen en actividades duales de cibercrimen y ciberespionaje. También esperamos ver una tendencia en la que más grupos APT pasarán a utilizar métodos aún más sigilosos e innovadores para iniciar ataques. Técnicas como el contrabando de HTML están ganando popularidad y prevemos que surgirán métodos novedosos adicionales durante el próximo año. Sus tácticas, técnicas y procedimientos (TTP) siguen evolucionando, evadiendo productos de seguridad con análisis obsoletos. Aunado a lo que seguramente será un año excepcional para las nuevas vulnerabilidades y exposiciones comunes (CVE), deberíamos esperar el crecimiento de los TTP y, por lo tanto, del marco MITRE ATT&CK.

Además de la evolución de las operaciones de APT, predecimos que los grupos de cibercrimen seguirán diversificando sus objetivos, buscando joyas ocultas (y muy lucrativas) entre una larga lista de organizaciones ya comprometidas. Por ejemplo, en el espacio de la tecnología operativa (OT), la industria manufacturera ha sido históricamente el principal objetivo de los ciberdelincuentes. Mirando hacia el futuro, anticipamos que los ataques a los sistemas operativos (OT) se extiendan rápidamente más allá del sector manufacturero, con actores maliciosos centrándose en industrias como la salud, servicios públicos, finanzas, petróleo y gas, y transporte. Estos ataques también irán más allá del cifrado de datos y se centrarán principalmente en la extorsión de sus objetivos. También seguirán dirigiendo ataques a la cadena de suministro, trabajando para alterar organizaciones y servicios críticos.

En nuestro informe de predicciones de amenazas para 2023, también dijimos que los ataques de borde se generalizarían y esperamos ver aún más de esta actividad en el futuro. No solo sucedió esto, sino que anticipamos que los atacantes trabajarán para diversificar sus objetivos más allá de lo que normalmente consideramos un dispositivo de borde. Con Flipper Zero y otras herramientas similares a su disposición, los intermediarios financieros o dispositivos podrían piratear dispositivos de IoT en persona mediante la clonación de tarjetas RFID o tarjetas de llaves de hotel y luego ejecutar comandos arbitrarios en dispositivos como teléfonos y computadoras portátiles. Recientemente, Flipper Zero ha permitido a los atacantes evitar conectar dispositivos USB en un ataque BadUSB. Solo se necesita que un empleado se conecte a través de Bluetooth antes de que se ejecuten comandos maliciosos. Con un exploit de día cero, es posible que ni siquiera sea necesaria la interacción del usuario.

Conclusión: La amplia gama de posibles objetivos y actividad más discreta en la cadena de ataque garantizan un flujo constante de víctimas y pagos lucrativos para los ciberdelincuentes.

Fuera de mi propiedad: Se intensifican las guerras territoriales del cibercrimen

Hace varios años predijimos que veríamos surgir guerras territoriales entre grupos de cibercrimen, con muchos adversarios centrándose en los mismos objetivos.

Hoy estamos viendo precisamente eso, mientras varios grupos de ciberdelincuentes intentan infiltrarse en el mismo objetivo en un período corto, a veces en cuestión de 24 horas o menos, implementando variantes de ransomware de AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum y Royal en diferentes combinaciones. Muchas organizaciones que experimentaron esto sufrieron ataques similares en pocos días, todos liderados por varios adversarios. Podemos suponer que otros ciberdelincuentes monitorean de cerca las comunicaciones en la *dark web* y luego ejecutan el mismo ataque o aprovechan los ataques ejecutados inicialmente por actores de amenazas rivales. El crecimiento de esta tendencia emergente llevó al FBI a emitir una advertencia a las organizaciones en septiembre de 2023, instando a los líderes de seguridad a revisar y mejorar sus defensas para protegerse contra incidentes de ransomware.

Vimos que aproximadamente dos tercios de todas las técnicas MITRE ATT&CK categorizadas se utilizaron activamente en ataques en la primera mitad de este año, siendo la evasión de defensa la táctica principal y la inyección de procesos que se utilizó en todos los ámbitos para la evasión en sistemas comprometidos. Las credenciales robadas son como un pase de acceso total para los delincuentes, permitiéndoles infiltrarse en su red para lanzar ransomware y otros ataques. Dado el valor que tienen las credenciales robadas para los actores de amenazas, predecimos que la tendencia emergente de ofertas de servicios de intermediarios de credenciales y acceso inicial crecerá en el futuro, facilitando a los ciberdelincuentes obtener las credenciales necesarias para llevar a cabo ataques exitosos (a veces contra el mismo objetivo). Es probable que este tipo de servicio madure y evolucione de la misma manera que se desarrolló el Ransomware-as-a-Service (RaaS) para cubrir un vacío en el mercado, con mayor disponibilidad comercial en lugar de estar disponible solo en la *dark web*.

Los servicios de lavado de dinero se quedan en el olvido

Anteriormente predijimos que los ciberdelincuentes utilizarían el lavado como servicio para lavar sus fondos mal habidos. Como era de esperar, muchos adversarios utilizaron estos servicios para obscurecer la propiedad de fondos ilegales, con ChipMixer, un ejemplo de un servicio de lavado que fue muy utilizado pero luego fue cerrado por las autoridades en marzo de 2023. Desde entonces, han aparecido en escena más mezcladores de criptomonedas. El grupo de amenazas Killnet, conocido por su actividad hacktivista pro-Rusia, también comenzó una casa de cambio de criptomonedas y ofrece servicios de mezcla.

Sin embargo, también parece haber un intento activo de acabar con muchos mezcladores de Bitcoin, además de que su popularidad parece estar disminuyendo. El resultado es que la mayoría de los grupos de hackers de Telegram está fomentando el uso de esquemas tradicionales de lavado de dinero en lugar de mezcladoras.

Aferrándose a las cadenas (de IA) para respaldar todas las etapas del ataque

El uso de la IA como arma está añadiendo combustible a un panorama de amenazas ya devastador: está permitiendo a los atacantes mejorar cada etapa de un ataque y hacerlo mejor y más rápido que antes. Como se predijo, estamos viendo que los ciberdelincuentes utilizan cada vez más la IA para reforzar muchas actividades maliciosas, que van desde frustrar los algoritmos que detectan la ingeniería social hasta imitar el comportamiento humano a través de actividades como la suplantación de audio de la IA y la creación de otros *deepfakes* (ultrafalsos).

Pero los adversarios no se detienen ahí. Anticipamos que los ciberdelincuentes aprovecharán la IA de otras formas que aún no hemos visto, por ejemplo:

- Los atacantes utilizarán la inteligencia artificial para llevar a cabo el perfilado generativo: recopilación de perfiles sociales y otros sitios web públicos en busca de información personal identificable, lo que fácilmente podría convertirse en un servicio ofrecido. Esta es otra forma más para que los actores maliciosos hagan investigaciones para ejecutar un ataque.
- Veremos surgir más ataques basados en IA, en los que los ciberdelincuentes utilizarán modelos ejecutables para hacer que sus cadenas de ataque sean más modulares. Por ejemplo, un atacante podría utilizar aprendizaje automático (ML) durante la fase de reconocimiento, encadenarlo a una carga útil armada basada en IA y encadenar eso a la implementación de la carga útil armada. Este enfoque de IA federada reduce su modelo de tiempo para comprometer.
- Los ciberdelincuentes utilizarán la IA para potenciar la pulverización de contraseñas. La fuerza bruta, el relleno y la pulverización de contraseñas son formas populares para que los atacantes identifiquen, roben y vendan credenciales. El uso de IA para identificar patrones y temas en las contraseñas aumentará esta posibilidad y acortará el tiempo necesario para que los atacantes tengan éxito.

- Los ataques de envenenamiento de IA (casos en los que los ciberdelincuentes manipulan intencionalmente los datos de entrenamiento de modelos de IA y los propios sistemas) se volverán comunes, con actores malintencionados probablemente utilizando kits de herramientas automatizadas para llevar a cabo estos ataques Los equipos de seguridad deberán empezar a protegerse contra estos ataques, confiando en un servicio de prevención de intrusiones y control de aplicaciones para proteger los activos de IA de una organización.

Tendencias de ataques únicos a tener en cuenta a partir de 2024

Los ciberdelincuentes seguirán confiando en tácticas específicas populares que les han permitido lograr una y otra vez sus objetivos. Sin embargo, los atacantes modernos tienen hoy más herramientas a su disposición que nunca, incluido un número creciente de ofertas de CaaS y tecnologías basadas en IA para ayudarles a trabajar de manera más inteligente y rápida en cada etapa de un ataque.

A medida que evolucione la industria del cibercrimen, veremos nuevas tendencias de ataque a partir de 2024. Aquí tenemos una semblanza de varios desarrollos anticipados que mantendrán alerta a los equipos de seguridad de todo el mundo.

El siguiente nivel de los libros de estrategias

Si hubiera un concurso de popularidad entre los tipos de ciberataques, el ransomware seguramente obtendría las mejores calificaciones. En los últimos años, el volumen de ataques de ransomware en todo el mundo se ha disparado, convirtiendo a todas las organizaciones, independientemente de su tamaño o industria, en un objetivo. De acuerdo con nuestro Informe sobre el panorama de amenazas de FortiGuard Labs del primer semestre de 2023, la actividad de ransomware fue 13 veces mayor a finales del primer semestre de 2023 que a principios de año. Y, a pesar de que el 78% de los líderes empresariales dijeron que se sentían preparados para defenderse contra el ransomware, la mitad fue víctima de un ataque.

Los atacantes continúan subiendo la apuesta al adoptar cepas más sofisticadas y complejas para infiltrarse en redes, incluido el malware de borrado de disco, altamente destructivo, que cubrimos en nuestro informe de predicciones para 2023, en gran medida gracias a la rápida expansión de las operaciones RaaS.. Sin embargo, a medida que un número cada vez mayor de ciberdelincuentes lanza ataques de ransomware con la esperanza de obtener un pago lucrativo, los grupos de cibercrimen están abandonando rápidamente objetivos más pequeños y fáciles de piratear.

Como resultado, anticipamos que los ciberdelincuentes se volverán más agresivos y ampliarán tanto sus listas de objetivos como sus estrategias. Veremos que los adversarios que buscan grandes pagos centrarán su atención en industrias críticas como la salud, servicios públicos, manufactura y finanzas, buscando objetivos que, si se interrumpen con éxito, tendrían un impacto sustancialmente adverso en la sociedad. Además de dirigir su atención a objetivos de mayor valor, los atacantes irán más allá de las tácticas que ya han utilizado. Sus estrategias se volverán más agresivas y destructivas, alejándose del cifrado y centrándose en la denegación de servicio y la extorsión.

A pesar de buscar objetivos de alto valor, en algún momento esta lista de objetivos se agotará. Esto plantea la pregunta de quién (o qué industria) serán los próximos en el radar de los ciberdelincuentes. A medida que los adversarios se ven obligados a ajustar sus estrategias, las aseguradoras cibernéticas pueden convertirse en atractivos objetivos. En los últimos años, hemos visto una tendencia en la que las organizaciones compensaban las brechas en su estrategia recurriendo a seguros cibernéticos. Pero a medida que el ransomware se intensifica, las aseguradoras cibernéticas están siendo más selectivas en cuanto a cuándo y cómo realizan los pagos. Con el tiempo ese dinero será restringido a medida que las aseguradoras cibernéticas se vuelvan cada vez más estrictas y los pagos de rescate sean menos frecuentes. Hasta ahora no hemos observado que las compañías de ciberseguros sean un objetivo directo para los atacantes, pero es posible que la industria sea considerada un objetivo de alto valor en el futuro, especialmente a medida que las compañías de seguros restrinjan esos pagos.

Un nuevo (y más lucrativo) día para los días cero

A medida que las organizaciones sigan ampliando el número de plataformas, aplicaciones y tecnologías en las que confían para respaldar las operaciones diarias del negocio, los ciberdelincuentes tienen nuevas y amplias oportunidades para descubrir y aprovechar vulnerabilidades de software. Un buen ejemplo: Hemos observado un número récord de vulnerabilidades día cero y nuevos CVE en 2023, y esa cifra sigue aumentando. Esta extensa lista incluye el MOVEit Transfer hack que afectó al menos a 60 millones de personas, y fue llamado el "mayor hackeo del año hasta ahora". Los nuevos días cero descubiertos son bastante rentables, pero como son tan valiosos, esperamos que muchos de ellos no se reporten. Los días cero no reportados son comprensiblemente más valiosos para los atacantes, ya que pueden ganar más dinero explotando un día cero del que la mayoría ni siquiera está al tanto, lo que significa que los equipos de seguridad deberán estar cada vez más atentos. Y no nos olvidemos del aumento de los días N, que consideramos días cero

con una vida útil prolongada. Estas vulnerabilidades podrían suponer un riesgo durante mucho tiempo, incluso varios años. Aunque los días N son vulnerabilidades conocidas, aún representan un riesgo para las organizaciones si no han sido parcheadas o no tienen un parche disponible.

Los ataques de día cero no disminuirán pronto; de hecho, esperamos ver agentes de día cero (grupos de cibercrimen que venden días cero en la *dark web* a múltiples compradores) surgir entre la comunidad CaaS. El auge de los agentes de día cero allanará el camino para que los ciberdelincuentes amplíen sus esfuerzos y alcancen una superficie de ataque más extensa a través de campañas más coordinadas. Veremos este cambio debido a una superficie de ataque en crecimiento con productos no reforzados, lo que permite a los atacantes poner en funcionamiento exploits para las decenas de miles de CVE que están destinados a ser descubiertos.

Existen muchas medidas que pueden tomar las organizaciones para protegerse contra las vulnerabilidades de día cero, como el uso de firewalls de próxima generación, la realización de análisis de vulnerabilidades y la implementación de una estrategia de administración inteligente de parches. Sin embargo, todas estas herramientas y actividades están diseñadas para proteger contra las vulnerabilidades sólo después de que se descubren. Los equipos de ingeniería tienen la oportunidad de ayudar a frenar el crecimiento de los exploits de día cero mejorando sus metodologías del ciclo de vida de desarrollo de software (SDL). Mientras que los ciberdelincuentes utilizan fuzzing (una técnica de prueba de software automatizada diseñada para descubrir errores de software) para encontrar nuevas vulnerabilidades que explotar, los equipos de desarrollo también pueden usar fuzzing para vencer a los atacantes en su propio juego. Los desarrolladores deberían considerar incorporar fuzzing en sus procesos SDL, lo que puede ayudar a fortalecer los productos y mejorar la seguridad y encontrar y corregir errores potenciales antes de que lo hagan los adversarios.

El juego al interior

En respuesta al panorama de amenazas en evolución, muchas empresas están fortaleciendo sus controles de seguridad y adoptando nuevas tecnologías y procesos para reforzar sus defensas. Estos controles mejorados dificultan que los atacantes se infiltren en una red desde el exterior, lo que obliga a los ciberdelincuentes a buscar nuevas formas de llegar a sus objetivos.

Dado este cambio, predecimos que los atacantes continuarán con un enfoque 'shift left' en sus tácticas, reconocimiento y armamentización, con grupos que comenzarán a reclutar desde dentro de las organizaciones objetivo con fines de obtener el acceso inicial. Por ejemplo, los ciberdelincuentes podrían utilizar fácilmente la IA generativa para clonar las voces de ejecutivos o personas de confianza, utilizando esas grabaciones para obligar a un objetivo desprevenido a ejecutar comandos, revelar contraseñas o datos e incluso liberar fondos. Podríamos ver fácilmente que el reclutamiento como servicio evoluciona como la siguiente fase de esta tendencia, permitiendo a los atacantes obtener acceso a más información para perfilar sus objetivos.

Si bien algunos objetivos pueden, sin saberlo, ser víctimas de un plan de cibercrimen, otros empleados pueden ver una colaboración única con los ciberdelincuentes como una forma de aumentar sus salarios con dinero rápido.

Ataques de "nosotros, el pueblo"

En 2024, esperamos ver a los atacantes aprovechar oportunidades más personalizadas e impulsadas por eventos, como las elecciones estadounidenses de 2024 y los juegos de París 2024. Si bien los adversarios han trabajado para interrumpir acontecimientos importantes en el pasado o aprovechar los acontecimientos geopolíticos, los ciberdelincuentes ahora tienen nuevas herramientas a su disposición, particularmente la IA generativa, para ayudarles en sus esfuerzos. Las autoridades ya están emitiendo advertencias sobre la amenaza de la IA en las próximas elecciones, hablando sobre el papel que esta tecnología probablemente desempeñará en acelerar la propagación de la desinformación en línea. Los asistentes y espectadores de los próximos juegos de París pueden esperar ser bombardeados con estafas dirigidas a la lealtad de los fanáticos. Y a medida que los juegos dependen cada vez más de la tecnología para cronometrar, gestionar y transmitir eventos, existe una probabilidad cada vez mayor de que esos sistemas se conviertan en objetivos.

Pero existen más oportunidades de provocar caos que sólo estos acontecimientos importantes. Si bien los gobiernos estatales y locales con recursos limitados han sido durante mucho tiempo blanco de ataques cibernéticos, predecimos que los actores maliciosos también encontrarán nuevas formas de infiltrarse en estas entidades. Por ejemplo, los ciberdelincuentes podrían utilizar fácilmente el aprendizaje automático (ML) y la inteligencia artificial (IA) para regionalizar los ataques, traduciendo las comunicaciones asociadas a los idiomas locales mediante modelos de lenguaje extensos.

Reducir el campo de juego del TTP

Anticipamos que los atacantes inevitablemente seguirán ampliando la colección de TTP que utilizan para comprometer sus objetivos. Sin embargo, al reducir el campo de juego y encontrar formas de interrumpir esas actividades, los defensores pueden obtener una ventaja.

Si bien la mayor parte del trabajo diario realizado por los defensores de la ciberseguridad está relacionado con el bloqueo de indicadores de compromiso, resulta muy valioso observar más de cerca los TTP que los atacantes utilizan habitualmente para mejorar

sus estrategias y encontrar puntos en los que podamos interrumpir sus modelos de ataque. Si bien los atacantes pueden tener un amplio conjunto de herramientas para ejecutar ransomware o campañas de phishing, sus técnicas suelen ser similares. Como defensores, podemos mapear lo que están haciendo los atacantes, compartir esa inteligencia entre la comunidad de seguridad y mitigar técnicas específicas.

El proyecto Attack Flow, dirigido por el Centro MITRE Engenuity para la defensa informada contra amenazas en colaboración con varios socios, incluido Fortinet, ofrece a los profesionales de la seguridad la oportunidad de reducir el campo de juego de TTP. Los contribuyentes del proyecto están creando un modelo de datos diseñado para ayudar a la comunidad de seguridad a encontrar puntos críticos en el tablero de ajedrez documentando los pasos que toma un actor malintencionado como parte de un ataque. A medida que los ciberdelincuentes avancen en sus operaciones y se vuelvan más hábiles para evadir las medidas de detección tradicionales, identificar dónde podemos potencialmente interrumpir sus actividades será de vital importancia.

Estrategia a largo plazo (del atacante)

Los dispositivos perimetrales, como los sistemas OT, alguna vez se consideraron objetivos no tradicionales para los ciberdelincuentes. Sin embargo, durante la última década, hemos visto un aumento en la sofisticación y el volumen de los intentos de ataques contra estos objetivos. Muchos años atrás, predijimos que los actores de amenazas usarían cada vez más troyanos de acceso perimetral para atacar entornos perimetrales, y hemos vimos varios ejemplos de cómo esto se ha hecho realidad.

Con Lynk Global, 5G, la conectividad directa al dispositivo es ahora una realidad. Además, el espacio satelital de órbita terrestre baja se está saturando, lo que significa que hay más conectividad con dispositivos que antes no estaban en línea. En pocas palabras, más dispositivos conectados ofrecen a los atacantes una mayor superficie de ataque y esto presenta oportunidades infinitas de compromiso. Un ataque exitoso contra la infraestructura 5G podría fácilmente interrumpir industrias críticas como las de petróleo y gas, transporte, seguridad pública y atención médica.

Mejorar nuestra resiliencia colectiva frente al panorama de amenazas en evolución

Los ciberdelincuentes encontrarán constantemente formas nuevas y más sofisticadas de hackear organizaciones. Aun así, podemos tomar muchas medidas en la comunidad de seguridad para anticipar mejor sus próximos movimientos e interrumpir sus actividades. Desde una mayor colaboración público-privada hasta estándares más estrictos para reportar incidentes, aquí hay varias formas de luchar colectivamente contra el cibercrimen.

Las asociaciones son cruciales para luchar contra el cibercrimen

El cibercrimen nos afecta a todos y las consecuencias de una infracción suelen ser de gran alcance. Una de las acciones de mayor impacto que podemos tomar como industria es crear asociaciones para facilitar el intercambio de información.

Se están llevando a cabo muchos esfuerzos para compartir conocimientos y mejores prácticas entre los sectores público y privado con el fin de interrumpir a los actores de amenazas. Sin embargo, aún queda trabajo por hacer, y todos tenemos un papel que desempeñar. Fortinet invierte recursos significativos en diversas asociaciones globales y contribuye activamente a la Asociación contra el Cibercrimen del Foro Económico Mundial (WEF). Además, trabajamos con la WEF a principios de este año para lanzar el Atlas del cibercrimen, un proyecto diseñado para ayudar a la industria, las fuerzas del orden y las agencias gubernamentales a interrumpir a los atacantes proporcionando un nuevo nivel de visibilidad del ecosistema y la infraestructura global del cibercrimen.

Cambios de política en el horizonte

Las alianzas sólidas son sólo una pieza del rompecabezas para luchar eficazmente contra el cibercrimen. En 2024 y en el futuro, esperamos ver algunas propuestas de cambios de políticas, desde la obligación de mejorar las defensas cibernéticas en determinadas industrias hasta la implementación de estándares más sólidos para el reporte de incidentes.

A medida que los gobiernos de todo el mundo empiecen a entender mejor la fragilidad y la interconectividad de la infraestructura crítica, se espera ver más sistemas definidos como críticos. Dado que el sector privado opera la infraestructura más crítica, esperamos que se introduzcan requisitos nuevos y más estrictos, lo que obligará a los operadores de infraestructura crítica a mantener mejores defensas cibernéticas.

Además, nos alienta ver que las agencias gubernamentales reconocen la necesidad de informes de incidentes estandarizados y toman medidas para armonizar los requerimientos de los informes. A principios del próximo año, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) introducirá requisitos de informes de incidentes en virtud de la Ley de Informes de Incidentes Cibernéticos para Infraestructuras Críticas de 2022. Recientemente, el Departamento de Seguridad Nacional de EE.UU. (DHS) emitió un informe que

incluye una plantilla de trabajo sobre cómo las agencias gubernamentales podrían crear una plataforma de informes común utilizando terminología consistente, lo que facilitaría el intercambio de información. Estaremos atentos para ver cómo evolucionan las regulaciones y plantillas de informes y qué papel podría desempeñar el informe del DHS en los requerimientos finales de la CISA.

Es esencial implementar regulaciones que se centren en aspectos de la ciberseguridad, como la presentación de informes y la divulgación responsable, para interrumpir las operaciones de los ciberdelincuentes. Podemos señalar varios ejemplos en los que la falta de regulación permite a las empresas vender herramientas y servicios diseñados con fines nefastos. Por ejemplo, consideremos al NSO Group y su rival QuaDream, ambos venden software de vigilancia de alta gama a clientes de cualquier parte del mundo, incluidos aquellos que lo utilizan con fines nefastos.

Las organizaciones desempeñan un papel vital a la hora de alterar el ecosistema del cibercrimen

Si bien las asociaciones colaborativas y las regulaciones sólidas son vitales para combatir el cibercrimen a nivel mundial, cada organización desempeña un papel integral en la interrupción del ecosistema. Esto empieza creando una cultura de resiliencia cibernética, haciendo que la ciberseguridad sea responsabilidad de todos, mediante la implementación de iniciativas continuas, como programas de educación en ciberseguridad para toda la empresa y actividades más específicas, como ejercicios de simulación para ejecutivos. Encontrar formas de reducir la brecha de habilidades en ciberseguridad, como aprovechar nuevos grupos de talentos para cubrir puestos vacantes, puede ayudar a las organizaciones a enfrentar la combinación de personal de TI y seguridad sobrecargado, así como el creciente panorama de amenazas. Además, el intercambio de información sobre amenazas será aún más importante en el futuro, ya que ayudará a movilizar rápidamente protecciones.

Responder colectivamente a las amenazas como un ecosistema tiene un mayor impacto en la interrupción del cibercrimen y los ataques, y es vital que las organizaciones entiendan su importante papel en esta interrupción.

Acerca de FortiGuard Labs

Fundada en 2002, FortiGuard Labs es la organización de inteligencia e investigación de amenazas de ciberseguridad élite de Fortinet. FortiGuard Labs, pionera e innovadora en la industria de la seguridad, desarrolla y utiliza tecnologías de inteligencia artificial y aprendizaje automático de vanguardia para brindar a los clientes protección oportuna y consistente de primera calidad e inteligencia sobre amenazas. Los datos de FortiGuard Labs se recopilan a través de telemetría obtenida de los millones de sensores de Fortinet (más de 6 millones de dispositivos implementados a nivel mundial), lo que brinda a FortiGuard Labs visibilidad en las amenazas del mundo real que enfrentan las organizaciones en la actualidad.

enero 1, 2024 11:57 p. m.

2387910-0-0-EN