LITORALPRESS

Fecha: 31-12-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: En 2025, prepárate para ciberataques más grandes y audaces

Pág. : 40
Cm2: 358,6

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Predicciones de amenazas

En 2025, prepárate para ciberataques más grandes y audaces

Por Derek Manky, Jefe de Estrategia de Seguridad y VP Global de Inteligencia de Amenazas en FortiGuard Labs de Fortinet.

Al tiempo que los actores maliciosos continúan confiando en muchas de las tácticas "clásicas" que han existido por décadas, el informe de predicción de amenazas que FortiGuard Labs de Fortinet preparó para 2025 se enfoca en los cibercriminales adoptando ataques más grandes, audaces y más eficientes. Desde grupos de cibercrimen como servicio (CaaS) cada vez más especializados, utilizando manuales (playbooks) más sofisticados que combinan amenazas tanto físicas como digitales, los cibercriminales están subiendo la apuesta para ejecutar ataques más dirigidos y dañinos.

En el reporte de predicciones de amenazas 2025, el equipo de FortiGuard Labs de Fortinet analiza los ataques que los ciberdelincuentes siguen ejecutando y cómo han evolucionado. Además, comparte nuevas tendencias de amenazas a tener en cuenta para este año y de cara al futuro y ofrece consejos sobre cómo las organizaciones de todo el mundo pueden mejorar su resiliencia frente a un panorama de amenazas cambiante.

Al tiempo que el cibercrimen evoluciona, anticipamos que estaremos viendo surgir tendencias sin precedente durante el 2025 y de cara al futuro. Acá un vistazo de lo que esperamos:

Surgen más expertos en la cadenas de ataque: En los últimos años, los cibercriminales han pasado más tiempo en las fases de reconocimiento y armamento de la cadena de ciberataque. Como resultado, los actores maliciosos pueden llevar a cabo ataques mucho más focalizados de un modo más rápido y preciso. En el pasado, habíamos observado muchos proveedores de cibercrimen como servicio (CaaS) actuando como expertos en todos los oficios: ofreciendo a los compradores todo lo necesario para ejecutar un ataque, desde kits de phishing hasta cargas útiles. Sin embargo, vemos que los grupos de CaaS están adoptando la especialización, con muchos grupos enfocándose en proveer ofertas que se focalicen en un solo segmento de la cadena de ataque.

Está "nublado" y con pronóstico de ciberataques: Si bien objetivos como los dispositivos de borde continúan captando la atención de los actores de amenazas, hay otra parte de la superficie de ataque a la que los defensores deberán poner mucha atención en los próximos años: sus ambientes de nube. Aunque la nube no es algo nuevo, está despertando gran interés en los cibercriminales. Debido a que muchas organizaciones confían en múltiples proveedores, no es de sorprenderse que estemos observando más vulnerabilidades específicas en la nube siendo aprovechadas por los atacantes, anticipando que esta tenencia crecerá de cara al futuro.

Las herramientas automatizadas para hacking se abren paso hacia el marketplace de la Dark Web: Un sinnúmero de vectores de ataque y códigos asociados están ahora disponibles a través del mercado de CaaS, como por ejemplo los kits de phishing, ransomware como servicio, DDoS como servicio y más. Si bien ya estamos viendo a algunos grupos cibercriminales apoyarse en el poder de la inteligencia artificial (IA) para impulsar sus ofertas de CaaS, esperamos que esta tendencia florezca. Anticipamos que los atacantes utilizarán los resultados automatizados para potenciar las ofertas de CaaS y hacer crecer el mercado, como el reconocimiento de redes sociales y la automatización de esa inteligencia en kits de phishing perfectamente empaquetados.

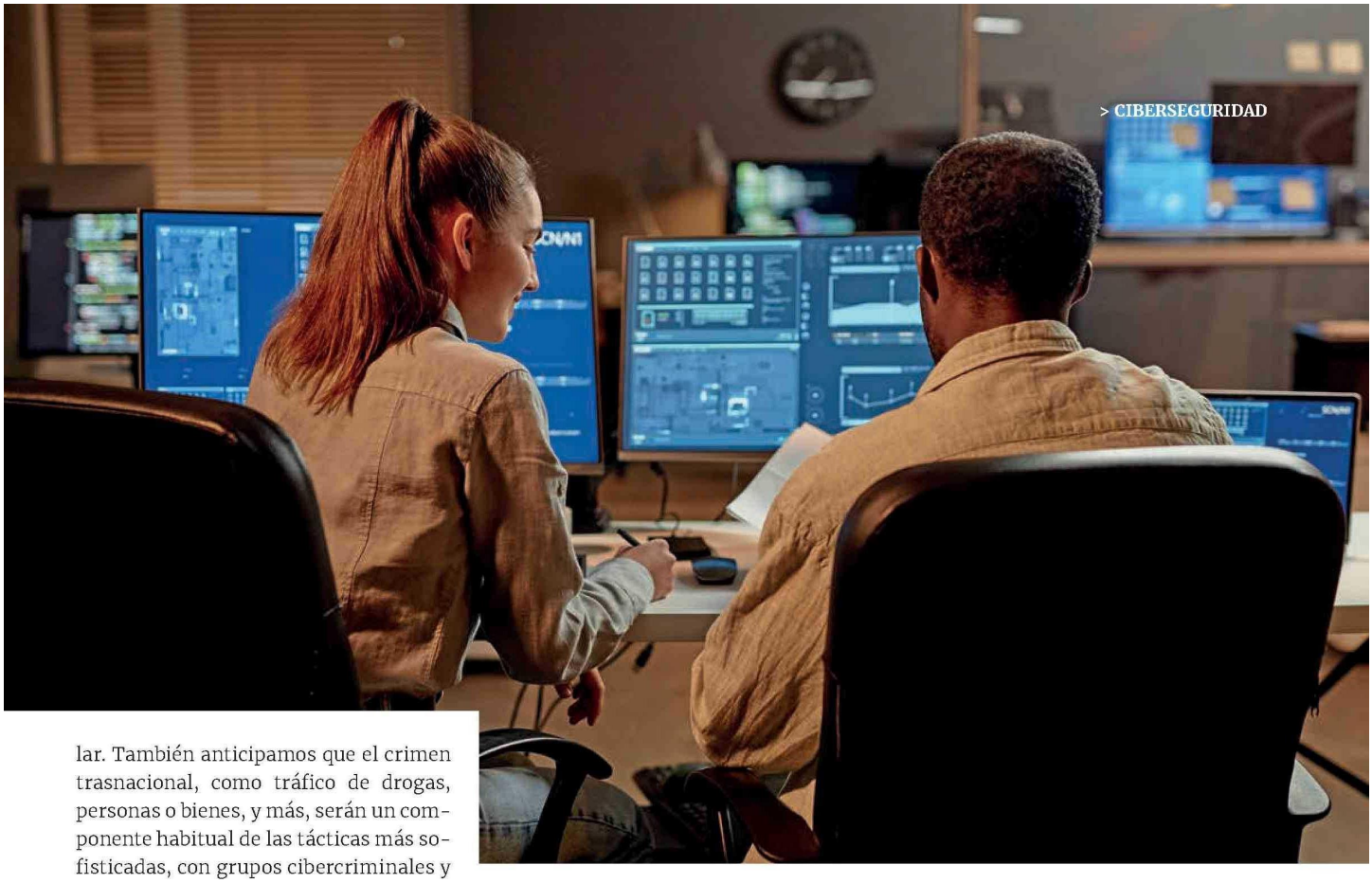
Las tácticas crecen para incluir amenazas de la vida real: Los cibercriminales continúan evolucionando sus tácticas, con ataques cada vez más agresivos y destructivos. Predecimos que los adversarios expandirán sus procedimientos para combinar ciberataques con amenazas físicas de la vida real. Ya estamos viendo que algunos grupos cibercriminales amenazan de manera física a los ejecutivos y empleados de las organizaciones en algunas instancias y anticipamos que esto formará parte de muchos manuales de manera regu-

LITORALPRESS

Fecha: 31-12-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: **En 2025, prepárate para ciberataques más grandes y audaces**

Pág. : 41
Cm2: 459,3

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



lar. También anticipamos que el crimen trasnacional, como tráfico de drogas, personas o bienes, y más, serán un componente habitual de las tácticas más sofisticadas, con grupos cibercriminales y organizaciones criminales trasnacionales trabajando en conjunto.

Se ampliarán los marcos anti adversarios: Al tiempo que los atacantes continúan evolucionando sus estrategias, la comunidad de la ciberseguridad en general puede hacer lo mismo en respuesta. Crear colaboraciones globales, sociedades público-privadas, y desarrollar marcos para combatir amenazas, es vital para impulsar nuestra resiliencia colectiva. Muchos esfuerzos relacionados, como la iniciativa Cybercrime Atlas del Foro Económico Mundial de la que Fortinet es miembro fundador, ya están en marcha y prevemos que surgirán más iniciativas de colaboración para desbaratar la delincuencia de forma significativa.

Impulsando la resiliencia colectiva en contra del panorama de amenazas evolucionado

Los cibercriminales siempre encontrarán nuevas formas para infiltrarse a las organizaciones. Sin embargo, existen numerosas oportunidades para que la comunidad de la ciberseguridad colabore para anticiparse a los siguientes movimientos de los adversarios y poder así interrumpir sus actividades de un modo significativo.

El valor de los esfuerzos a lo largo de todas las industrias, y las colaboraciones público-privadas no puede subestimarse y anticipamos que el número de organizaciones participando en estas colaboraciones crecerá de cara a los próximos años. Adicional a ello, las organizaciones deben recordar que la ciberseguridad es trabajo de todos, no solo responsabilidad de los equipos de seguridad y TI. Implementar programas de concientización y entrenamiento, a nivel de toda la organización, por ejemplo, es un componente vital para manejar el riesgo. Y, por último, otras entidades tienen la responsabilidad también de promover e incluir prácticas robustas de ciberseguridad, desde gobiernos hasta los proveedores que manufacturan los productos de seguridad en los que confiamos.

Al tiempo que los atacantes continúan evolucionando sus estrategias, la comunidad de la ciberseguridad en general puede hacer lo mismo en respuesta. Crear colaboraciones globales, sociedades público-privadas, y desarrollar marcos para combatir amenazas, es vital para impulsar nuestra resiliencia colectiva.

Ninguna organización o equipo de seguridad puede atacar al cibercrimen sola. Al trabajar en conjunto y compartir inteligencia en toda la industria estamos mejor posicionados de manera colectiva para poder combatir a los adversarios y proteger a la sociedad.

Descarga una copia de nuestro reporte de predicciones 2025 en **https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report_2025-threat-predictions.pdf** / ChN