CHANNEL News
Fecha: 30/05/2025 Audiencia: 18.000 Sección: ACTUALIDAD
Vpe: $528.695 Tirada: 6.000 Frecuencia: MENSUAL
Vpe pág: $783.027 Difusión: 6.000
Vpe portada: $783.027 Ocupación: 67,52%

La IA y nuevas técnicas surgen como armas

Revelan un aumento récord de ciberataques automatizados

El Reporte sobre el Panorama Global de Amenazas de FortiGuard Labs 2025 destaca un auge del ciberdelito como servicio en la "Dark Web", lo que impulsa un mercado lucrativo de credenciales, exploits y acceso.

El Reporte sobre el Panorama Global de Amenazas de FortiGuard Labs 2025 es una mirada hacia el actual panorama de amenazas y las tendencias de 2024, incluyendo un análisis integral de las tácticas utilizadas en los ciberataques, como se describe en el framework MITRE ATT&CK. Además, revela que los adversarios están utilizando de manera exponencial la automatización, las herramientas mercantilizadas, y la IA para erosionar de manera sistemática las ventajas antes sostenidas por los defensores.

"Los cibercriminales están acelerando sus esfuerzos, utilizando la IA y la automatización para operar a niveles sin precedentes de rapidez y escala", aseguró Derek Manky, Jefe de Estrategia de Seguridad, y VP Global de Inteligencia de Amenazas de FortiGuard Labs de Fortinet. "El manual tradicional de seguridad ya no es suficiente. Las organizaciones deben tomar una estrategia proactiva enfocada en inteligencia e impulsada por IA, confianza cero y manejo continuo de exposición a amenazas, para poder mantenerse a la vanguardia del panorama de amenazas actual que está cada vez más evolucionado".

Principales descubrimientos

En la edición 2025 del Reporte del Panorama de Amenazas Global de FortiGuard Labs incluyen:

- **El escaneo automatizado alcanza "peaks" récord al tiempo que los atacantes se desplazan a la izquierda para identificar objetivos expuestos con anticipación:** Para capitalizar las vulnerabilidades recién descubiertas, los cibercriminales están desplegando escaneo automatizado a escala global. El escaneo activo en el ciber espacio alcanzó niveles sin precedente en 2024, con un incremento de 16,7% año con año a nivel mundial, resaltando una colección masiva y sofisticada de información en infraestructura digital expuesta. FortiGuard Labs observó mil millones de escaneos mensuales -el equivalente a 36.000 escaneos por segundo-, lo que revela un foco en mapear servicios expuesto como SIP,

RDP y protocolos de IT/OT como ModbusTCP.

- **Los mercados de la "dark net" facilitan el acceso a kits de explotación cuidadosamente empaquetados:** en 2024, los foros de ciberdelincuentes funcionaron cada vez más como sofisticados mercados de kits de explotación, con más de 40.000 nuevas vulnerabilidades añadidas a la Base de Datos Nacional de Vulnerabilidades, un aumento del 39% con respecto a 2023. Además de las vulnerabilidades de día cero que circulan en la red oscura, los intermediarios de acceso inicial ofrecen cada vez más credenciales corporativas (20%), acceso RDP (19%), paneles de administración (13%) y shells web (12%). Asimismo, FortiGuard Labs observó un aumento del 500% durante el último año en los registros disponibles de sistemas comprometidos por malware de robo de información, con 1.700 millones de registros de credenciales robadas compartidos en foros clandestinos.
- **El cibercrimen impulsado por IA está escalando de manera rápida:** Los actores de amenazas están aprovechando la IA para mejorar el realismo del phishing y evadir los controles de seguridad tradicionales, lo que hace que los ciberataques sean más efectivos y difíciles de detectar. Herramientas como FraudGPT, BlackmailerV3 y ElevenLabs están impulsando campañas más escalables, creíbles y efectivas, sin las restricciones éticas de las herramientas de IA disponibles públicamente.
- **Se intensifican los ataques dirigidos a sectores críticos:** Industrias como manufactura, salud y servicios financieros continúan experimentando un aumento de ciberataques personalizados, con adversarios que despliegan exploits específicos para cada sector. En 2024, los sectores más atacados fueron manufactura (17%), servicios empresariales (11%), construcción (9%) y el comercio minorista (9%). Tanto los actores estatales como los operadores de ransomware como servicio (RaaS) concentraron sus esfuerzos en estos sectores, siendo Estados Unidos el más afectado (61%), seguido del Reino Unido (6%) y Canadá (5%).
- **Los riesgos en nube e IoT escalan:** Los ambientes de nube continúan siendo uno de los principales objetivos, con adversarios explotando debilidades persistentes como depósitos de almacenamiento abiertos, identidades con permisos excesivos y servicios mal configurados. En el 70% de los incidentes observados, los atacantes obtuvieron acceso mediante inicios de sesión desde ubicaciones desconocidas, lo que destaca el papel crucial de la monitorización de identidades en la defensa de la nube.
- **Las credenciales son la moneda de cambio del cibercrimen:** Durante 2024, los ciberdelincuentes compartieron más de 100.000 millones de registros comprometidos en foros clandestinos, un aumento interanual del 42%, impulsado principalmente por el auge de las "listas combinadas" que contienen nombres de usuario, contraseñas y direcciones de correo electrónico robadas. Más de la mitad de las publicaciones en la "dark net" involucraban bases de datos filtradas, lo que permitió a los atacantes automatizar ataques de robo de credenciales a gran escala. Grupos conocidos como BestCombo, BloddyMery y ValidMail fueron los grupos ciberdelincuentes más activos durante este periodo y continúan reduciendo la barrera de entrada al empaquetar y validar estas credenciales, lo que impulsa un aumento en el robo de cuentas, el fraude financiero y el espionaje corporativo. ChN

Para capitalizar las vulnerabilidades recién descubiertas, los cibercriminales están desplegando escaneo automatizado a escala global.

Artículo gentileza de Fortinet.
https://www.fortinet.com/lat