Anuncios

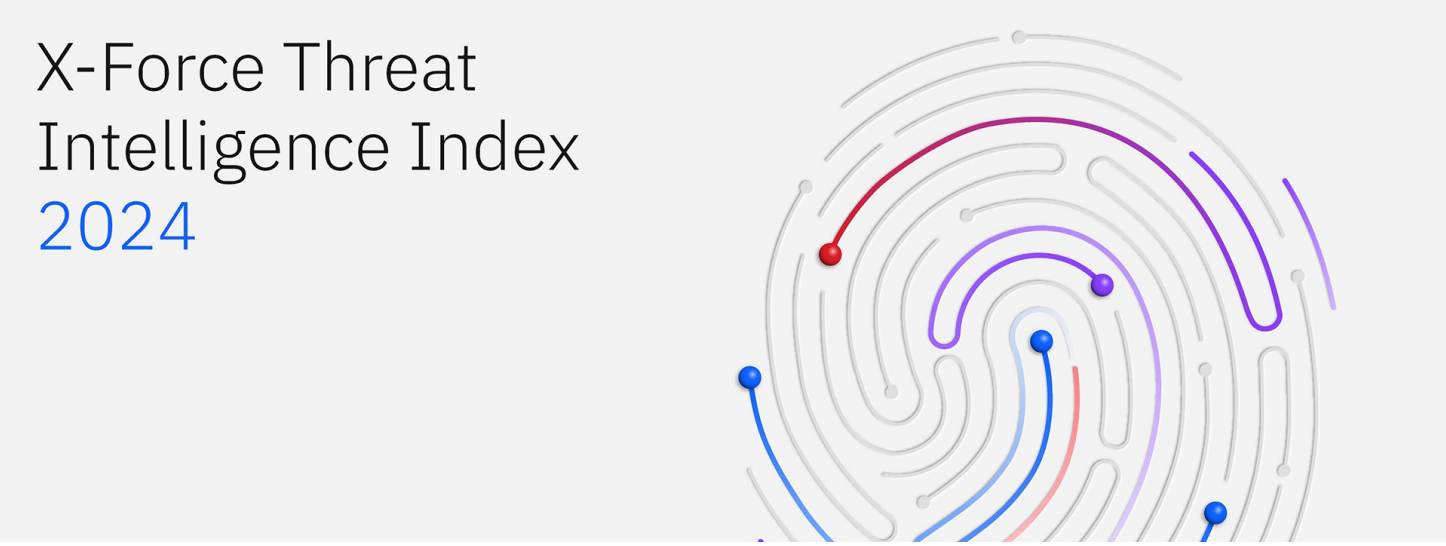
La identidad digital se convierte en el principal objetivo de los ciberataques en Europa dificultando los tiempos de recuperación tras una brecha de seguridad

• A nivel global, el informe registró un aumento del 71% de los ciberataques cuyo objetivo es la explotación de la identidad digital de los usuarios

• Se estima que una vez que la IA generativa se consolide con una cuota de mercado del 50%, podrían desencadenarse ataques cibernéticos a escala

• Casi el 70% de los ataques a nivel mundial en 2023 tuvieron como objetivo infraestructuras críticas

• Europa se ha convertido en la región más atacada en 2023, con un 32% de los incidentes a nivel mundial, subiendo desde el segundo puesto que ocupaba en 2022



CAMBRIDGE, Massachusetts, 21 de febrero de 2024 - IBM (NYSE: IBM) ha publicado hoy el IBM Security X-Force Threat Intelligence Index 2024, que destaca la existencia de una emergente crisis global que amenaza principalmente a la identidad digital, a medida que los ciberdelincuentes duplican la explotación de las identidades de los usuarios para comprometer la seguridad de las empresas de todo el mundo. Según IBM X-Force, la rama de servicios de seguridad ofensiva y defensiva de IBM Consulting, en 2023 los ciberdelincuentes vieron más oportunidades a través de tácticas que conllevan "iniciar sesión" que pirateando las redes corporativas a través de cuentas válidas, lo que convierte a este método en el arma preferida de los ciberdelincuentes.

El X-Force Threat Intelligence Index se basa en conocimientos y observaciones procedentes de la supervisión de más de 150.000 millones de eventos de seguridad al día en más de 130 países. Asimismo, los datos se recopilan y analizan en múltiples fuentes dentro de IBM, incluyendo IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services, y los datos proporcionados

"Si bien la preocupación por los 'ataques diseñados por IA' es comprensible, no debemos pasar por alto las amenazas existentes que continúan año tras año perturbando las empresas, como los ataques que explotan la identidad. Este problema sólo empeorará a medida que los adversarios aprovechen la IA para

por Red Hat Insights e Intezer, que contribuyeron al informe de 2024.

Resultados destacados para el continente europeo:

- Casi uno de cada tres ataques observados en todo el mundo tuvo como objetivo el continente europeo, una cifra de ataques sin precedentes en la región registrada por X-Force.
- Los eslabones más débiles para las organizaciones europeas fueron las identidades y los correos electrónicos, con el uso ilegítimo de cuentas válidas (30%) y phishing (30%).
- En toda Europa, X-Force observó un aumento interanual del 66% en los ataques causados por el uso ilegítimo de cuentas válidas.
- El malware fue la acción más observada, con un 44% de los incidentes, y el continente europeo fue la región que experimentó el mayor número de ataques de ransomware a nivel mundial (26%).
- Los tres tipos de incidentes más importantes para las organizaciones con sede en Europa han sido el robo de credenciales con un 28%, la extorsión con un 24% y las filtraciones de datos con un 16%.
- Por sectores, la industria manufacturera pasó a ser la más atacada con un 28% de incidentes y subiendo del segundo puesto que ocupaba en el informe de 2022.
- Los servicios profesionales, empresariales y de consumo se situaron en segundo lugar —con un 25% de los ataques—, seguido por el sector financiero y de seguros (16%), y desplazando al energético al cuarto lugar con un 14%.
- El continente europeo en su conjunto experimentó el mayor porcentaje de incidentes en el sector energético a nivel global, con un 43%, seguido por el financiero y de seguros, con un 37%.
- Casi el 70% de los ataques a los que respondió X-Force en Europa se produjeron en Estados miembros de la UE.

optimizar sus tácticas y las organizaciones deben estar bien preparadas para dar respuesta. ”

“Si bien la preocupación por los 'ataques diseñados por IA' es comprensible, no debemos pasar por alto las amenazas existentes que continúan año tras año perturbando las empresas, como los ataques que explotan la identidad", afirma Ascensio Chazarra, Cyber Threat Management Offering Leader de IBM Consulting para EMEA. "*Este problema sólo empeorará a medida que los adversarios aprovechen la IA para optimizar sus tácticas y las organizaciones deben estar bien preparadas para dar respuesta"*.

Una crisis de identidad global a punto de empeorar

La explotación y uso ilegítimo de cuentas válidas se ha convertido en un método habitual para los ciberdelincuentes, lo que ha dado como resultado miles de millones de credenciales comprometidas en la Dark Web actualmente. En este sentido, X-Force observó que los atacantes estuvieron invirtiendo cada vez más en operaciones para hacerse con las identidades de los usuarios, con un aumento del 266% en el malware de robo de información diseñado para obtener datos personales identificables como correos electrónicos, credenciales de redes sociales y aplicaciones de mensajería, detalles bancarios o datos de wallets de criptomonedas, entre otros.

Este método de “fácil acceso” para los atacantes es más complejo de detectar, lo que provoca una respuesta

costosa por parte de las empresas. Según X-Force, los principales incidentes causados por ciberdelincuentes que utilizan cuentas válidas se asocian a medidas de respuesta casi un 200% más complejas por parte de los equipos de seguridad que el incidente medio, ya que los defensores tienen que distinguir entre la actividad legítima y maliciosa de los usuarios en la red. De hecho, el informe de 2023 Cost of a Data Breach Report de IBM afirma que se necesitan aproximadamente 11 meses para detectar y recuperar las filtraciones causadas por credenciales robadas o comprometidas, suponiendo el ciclo de vida de respuesta más largo que cualquier otro tipo de ataque.

El acceso a la actividad online de los usuarios quedó patente en el desmantelamiento por parte del FBI y las fuerzas de seguridad europeas, en abril de 2023, de un foro mundial de ciberdelincuencia que recopilaba los datos de acceso de más de 80 millones de cuentas de usuario. Es probable que las amenazas que tienen como objetivo la identidad digital sigan creciendo a medida que los adversarios aprovechen la IA generativa para optimizar sus ataques. Ya en 2023, X-Force observó más de 800.000 publicaciones sobre IA y GPT en foros de la Dark Web, lo que reafirma que estas innovaciones han captado la atención y el interés de los ciberdelincuentes.

Además de la crisis en torno a la identidad digital, a nivel global algunos de los puntos más destacados son:

- **Los ataques a infraestructuras críticas revelan los "pasos en falso" de la industria.** En casi el 85% de los ataques a sectores críticos a nivel global, los datos comprometidos podrían haberse mitigado con parches, autenticación multifactor o principios de mínimo privilegio, lo que indica que lo que la industria de la seguridad ha descrito históricamente como "seguridad básica" puede ser más difícil de conseguir de lo que se cree.
- En todo el mundo, casi el 70% de los ataques a los que X-Force respondió iban dirigidos contra organizaciones de infraestructuras críticas, un 74% en el caso de la Unión Europea, un hallazgo alarmante que pone en relieve que los ciberdelincuentes están aprovechándose de la necesidad que tienen las empresas de que sus sistemas mantengan un funcionamiento continuo.
- Casi el 85% de los ataques a los que X-Force respondió en este ámbito fueron causados por la explotación de aplicaciones de cara al público, correos electrónicos de suplantación de identidad y el uso ilegítimo de cuentas válidas. Esto último supone un mayor riesgo para el sector, ya que DHS CISA afirma que la mayoría de los ataques que tuvieron éxito en organismos públicos, organizaciones de infraestructuras críticas y agencias gubernamentales a nivel estatal en 2022 implicaron el uso ilegítimo de cuentas válidas. Esto pone de relieve la necesidad de que estas organizaciones realicen con frecuencia pruebas de estrés en sus entornos para detectar posibles exposiciones y desarrollar planes de respuesta a incidentes.
- **Los grupos de ransomware se orientan hacia un modelo de negocio más ágil.** Los ataques de ransomware a empresas experimentaron un descenso de casi el 12% el año pasado, a medida que las grandes organizaciones optan por no pagar y descifrar, en favor de reconstruir su infraestructura. Es probable que este creciente rechazo afecte a las expectativas de ingresos de los adversarios procedentes de la extorsión basada en el cifrado de la información, por lo que se ha observado que los grupos que antes se especializaban en ransomware han pasado a dedicarse al robo de información.
- **Los ataques de la IA generativa todavía no son rentables.** El análisis de X-Force prevé que cuando una sola tecnología de IA generativa se acerque al 50% de la cuota de mercado o cuando se consolide en tres o menos tecnologías, podrían desencadenarse ataques a escala contra estas plataformas, lo cual significará una mayor inversión en nuevas herramientas por parte de los ciberdelincuentes.
- Para que los ciberdelincuentes vean la rentabilidad de sus campañas, las tecnologías a las que se dirigen

deben ser omnipresentes en la mayoría de las organizaciones de todo el mundo. De la misma manera que los avances tecnológicos del pasado fomentaron las actividades de los ciberdelincuentes -como se observó con el ransomware y el dominio del mercado de Windows Server, las estafas BEC y el dominio de Microsoft 365 o el cryptojacking y la consolidación del mercado de la infraestructura como servicio-, es muy probable que este patrón se extienda a la IA.

- Aunque la IA generativa se encuentra actualmente en su fase previa a la comercialización masiva, es primordial que las empresas protejan sus modelos de IA antes de que los ciberdelincuentes amplíen su actividad. Las empresas también deben reconocer que su infraestructura subyacente existente es una puerta de entrada a sus modelos de IA que no requiere tácticas novedosas por parte de los delincuentes para atacar - destacando la necesidad de un enfoque holístico de la seguridad en la era de la IA generativa, como se indica en el IBM Framework for Securing Generative AI.

Otras conclusiones relevantes del estudio:

- **¿Dónde ha ido a parar todo el phishing?** : A pesar de seguir siendo uno de los principales vectores de infección, el volumen de los ataques de phishing disminuyó un 44 % con respecto a 2022. Pero con la IA capaz de optimizar este ataque y las conclusiones de X-Force que indican que la IA puede acelerar los ataques en casi dos días, este vector de infección seguirá siendo una opción preferida para los ciberdelincuentes.
- **Todo el mundo es vulnerable**: Red Hat Insights descubrió que el 92% de los clientes tienen al menos un CVE con exploits conocidos sin abordar en su entorno en el momento del análisis, mientras que el 80% de las diez principales vulnerabilidades detectadas en los sistemas en 2023 recibieron una puntuación de gravedad base CVSS "Alta" o "Crítica".
- **"Kerberoasting" da sus frutos**: X-Force observó un aumento del 100% en los ataques "kerberoasting", en los que los atacantes intentan hacerse pasar por usuarios para escalar privilegios abusando de los tickets de Microsoft Active Directory.
- **Configuraciones erróneas de seguridad**: Las pruebas de penetración de X-Force Red indican que las configuraciones erróneas de seguridad representaron el 30% de las exposiciones totales identificadas, observando más de 140 formas en que los atacantes pueden explotar las configuraciones erróneas.

Recursos adicionales

- Descargue una copia del X-Force Threat Intelligence Index 2024.
- Más información sobre las principales conclusiones del informe en este blog de IBM Security Intelligence.
- Inscríbase en el webinar *What is shifting in European Cyber Threats?,* que tendrá lugar el jueves 21 de marzo a las 17:00 CET (11:00 ET)
- Contacte con el equipo de IBM X-Force para una revisión personalizada de los resultados.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación. alfonso.mateos@ibm.com