appgate

FRAUD BEAT 2026

FRAUD BEAT

REPORTE ANUAL

IA Y ESTRATEGIAS AVANZADAS PARA COMBATIR

EL FRAUDE DIGITAL

TABLA DE **CONTENIDOS**

appgate

INTRODUCCIÓN

UNA NUEVA ERA DE ***AMENAZAS DIGITALES***

En 2024, el panorama de las amenazas digitales se transformó drásticamente, con un aumento del 57% de los incidentes mundiales en comparación con 2023. Los atacantes explotaron herramientas avanzadas como el malware, el phishing y las falsas campañas en redes sociales para atacar identidades y credenciales. América Latina y Asia-Pacífico se vieron particularmente afectadas, enfrentando altos volúmenes de phishing y redirecciones maliciosas, mientras que Estados Unidos luchó con cuentas comprometidas y aplicaciones móviles no autorizadas.

Este informe revela las principales tendencias de las amenazas digitales en 2024, profundiza en las regiones e industrias más afectadas y explora estrategias eficaces para protegerse contra estos riesgos en constante evolución.

appgate

PRINCIPALES TIPOS DE ATAQUES **EN 2024**

Desde Appgate, nuestro Centro de Operaciones de Seguridad (SOC), ha observado las siguientes tendencias clave en 2024:

- ***El 86%*** de los incidentes de amenazas registrados se debieron al phishing, lo que lo convierte en el tipo de ataque más común de los ciberdelincuentes. Los ataques incluyeron redireccionamientos maliciosos y falsas campañas en redes sociales, siendo LATAM y APAC las regiones más afectadas.
- ***El 12%*** de los incidentes estaban relacionados con redes sociales falsas utilizadas para suplantar marcas y personas. Este tipo de ataque fue particularmente prevalente en LATAM, con Argentina, Brasil y Ecuador reportando el mayor número de incidentes.
- La explotación de aplicaciones públicas representó el ***15%*** de los incidentes y fue un vector inicial común tanto en LATAM como en APAC. Los ciberdelincuentes explotaron configuraciones inseguras para obtener acceso a sistemas sensibles.

El Centro de Operaciones de Seguridad (SOC) de Appgate dio pasos significativos en 2024, fortaleciendo su capacidad para detectar, mitigar y responder a las amenazas cibernéticas de manera más eficiente. Estos son algunos de los avances más notables:

1. **Alianza más fuerte con Google** – Una nueva colaboración con Google ha mejorado nuestra velocidad de bloqueo en Chrome, lo que lleva a una mitigación de phishing más rápida para los usuarios finales y mejores negociaciones con los proveedores de servicios.
2. **Replit Trusted Reporter** – Appgate fue reconocido oficialmente como Informe Confiable por Replit, reforzando nuestra credibilidad en la identificación y denuncia de actividades fraudulentas.
3. **Monitorización interna mejorada** – Las mejoras continuas en nuestros procesos de monitorización SOC han aumentado la precisión de la detección y los tiempos de respuesta.
4. **Perspectivas en las tendencias de phishing** – Nuestro último análisis destaca cómo ciertos proveedores de alojamiento han reducido significativamente sus tiempos de respuesta a las solicitudes de retirada, contribuyendo a mejorar la mitigación del phishing en todo el sector.

PHISHING 71%

DESVIO DE PHISHING 14%

REDES SOCIALES FALSAS 12%

OTROS 3%

ANÁLISIS DE TENDENCIAS: ***2024 VS 2023***

La comparación de los datos de 2023 y 2024 revela un aumento significativo del volumen de incidentes, según los tipos de ataque gestionados por el **SOC.**

Entre las principales conclusiones se incluyen:

LOS INCIDENTES DE PHISHING CRECIERON UN **86% en 2024**

LOS CASOS DE FALSIFICACIÓN EN REDES SOCIALES CASI SE DUPLICARON, AUMENTANDO **un 99%**

El crecimiento exponencial de los incidentes de phishing y falsificación en redes sociales en 2024 demuestra que los ciberdelincuentes aprovechan cada vez más la ingeniería social y las plataformas digitales para ejecutar sus ataques. Este aumento refleja la creciente sofisticación de los métodos utilizados y la capacidad de los atacantes para explotar la confianza en las aplicaciones y plataformas en línea. Las organizaciones deben responder con una detección robusta, una prevención proactiva y la vigilancia continua de las amenazas emergentes

.

IMPACTO DE LA IA ***EN LOS PRINCIPALES ATAQUES EN 2024***

En 2024, la inteligencia artificial (IA) desempeñó un papel crucial en la evolución de los ciberataques que más afectan a nuestros clientes. Los avances de la IA han permitido a los ciberdelincuentes mejorar la sofisticación, la eficacia y la escala de sus tácticas, especialmente en el phishing, los falsos ataques a redes sociales y el malware como servicio (MaaS).

PHISHING

La IA permitió a los atacantes a crear mensajes personalizados utilizando datos públicos y tecnologías deepfake, aumentando la tasa de éxito de las campañas.

REDES SOCIALES FALSAS

Los bots inteligentes impulsados por IA generativa operaron perfiles falsos e identificaron objetivos vulnerables.

MALWARE COMO SERVICIO (MAAS)

Las herramientas impulsadas por IA automatizaron la distribución y personalización del malware, haciendo que los ataques fueran más devastadores.

"Se prevé que las pérdidas por fraude generativo de IA en EE.UU. alcancen los 40.000 millones de dólares en 2027. Esta escalada apunta a la necesidad urgente de que diversas industrias se mantengan no solo uno, sino varios pasos por delante de los defraudadores.".

-Fraud.net

LA CARRERA ARMAMENTÍSTICA DE LA IA: ***CÓMO EL APRENDIZAJE AUTOMÁTICO IMPULSA TANTO EL FRAUDE COMO LA DEFENSA***

La IA está transformando significativamente el panorama del fraude digital, introduciendo tanto nuevos retos para la prevención como métodos innovadores para los defraudadores.

"El contenido falso nunca ha sido tan fácil de crear -o más difícil de atrapar-. A medida que crecen las amenazas, los bancos pueden invertir en IA y otras tecnologías para ayudar a detectar el fraude y evitar pérdidas."

-Centro Deloitte de Servicios Financieros

IA EN LA DETECCIÓN DEL FRAUDE

En respuesta a estas amenazas cambiantes, las organizaciones están adoptando cada vez más sistemas de detección de fraudes basados en IA. Estos sistemas utilizan algoritmos avanzados para analizar grandes cantidades de datos en busca de patrones irregulares indicativos de actividad fraudulenta. Al aprender continuamente de las interacciones, la IA mejora sus capacidades predictivas, lo que permite una identificación y respuesta más rápidas ante posibles fraudes.

TENDENCIAS DEL FUTURO

A medida que aumenta la sofisticación de las herramientas de IA, también lo hace la complejidad de las tramas de fraude. Los expertos predicen que la integración de la IA tanto en las actividades fraudulentas como en las estrategias de detección requerirá un enfoque multicapa de la seguridad de la red. Se aconseja a las empresas que empleen la IA no sólo como mecanismo de defensa, sino también como contramedida contra las propias tácticas utilizadas por los defraudadores.

Con las soluciones 360 Fraud Protection de Appgate, las empresas obtienen acceso a herramientas que evolucionan con las amenazas, como algoritmos de aprendizaje automático diseñados para anticiparse a los ataques y neutralizarlos.

LA PROACTIVIDAD, ***PIEDRA ANGULAR DE LA CIBERSEGURIDAD***

En un mundo en el que las amenazas digitales evolucionan constantemente, estar protegido requiere un enfoque proactivo y soluciones avanzadas. Las organizaciones se enfrentan a importantes retos debido al crecimiento de ataques sofisticados como el phishing, la divulgación de información y el uso no autorizado de marcas comerciales. Sin una estrategia sólida, el impacto financiero, reputacional y operativo puede ser devastador.

MANTENERSE A LA VANGUARDIA:

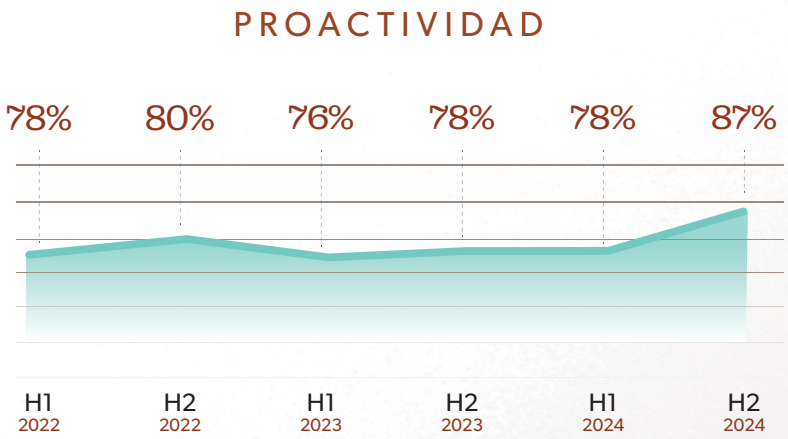
El panorama moderno de las amenazas digitales es dinámico. Los atacantes aprovechan la IA generativa para crear campañas de phishing y malware más convincentes. Mantenerse a la vanguardia requiere no sólo responder a los incidentes, sino anticiparse a futuros vectores de ataque con defensas adaptables. Realiza evaluaciones periódicas de ciberseguridad para detectar y corregir vulnerabilidades antes de que puedan ser explotadas.

NUESTRAS ESTRATEGIAS PARA AYUDARLE A MANTENERSE PROTEGIDO INCLUYEN:

1. **Mitigación de amenazas en tiempo real**
   Aprovechar la tecnología impulsada por IA permite a las organizaciones identificar vulnerabilidades y mitigar amenazas antes de que se intensifiquen. Este enfoque proactivo garantiza que los riesgos emergentes se aborden a medida que se desarrollan, minimizando la exposición a posibles brechas.
2. **Soluciones de detección avanzada:**
   Mediante la supervisión continua de patrones de acceso y comportamientos sospechosos, las empresas pueden anticiparse a los ataques en lugar de limitarse a reaccionar ante ellos. Los sistemas de detección proactiva ofrecen una capa de defensa que evoluciona con las tácticas de los ciberdelincuentes.

PROACTIVIDAD EN ACCIÓN: ***EL COMPROMISO DE APPGATE***

Desde 2022, Appgate ha logrado sistemáticamente una tasa de proactividad global superior al 80%, lo que demuestra su compromiso de adelantarse a las Amenazas Digitales. A pesar de un aumento significativo del volumen de entradas, las medidas proactivas han impulsado un notable crecimiento de la eficacia, que culminará con una impresionante tasa de proactividad del 87% en el segundo semestre de 2024. Esta tendencia al alza subraya la fortaleza y adaptabilidad de las soluciones de Appgate en un panorama de amenazas en constante evolución.



CUMPLIMIENTO DE LAS ***NORMAS ISO***

360 Brand Guardian de Appgate ayuda al sector financiero a cumplir múltiples normas ISO detectando y eliminando las amenazas digitales que comprometen la seguridad de la información, la ciberseguridad y la prevención del fraude. Por ejemplo, ISO 27032, que se centra en la ciberseguridad y la protección contra ataques en línea, se alinea con la capacidad de 360 Brand Guardian para prevenir la explotación de la identidad de marca. He aquí cómo podemos ayudar a tu organización:

ISO 27032 (Ciberseguridad)

1. **Protección contra ciberataques:** Detecta y neutraliza ataques de phishing, sitios falsos y fraudes online.
2. **Mitigación de amenazas en la web y la dark-web:** Identificar dominios maliciosos antes de que se utilicen en campañas de fraude.
3. **Colaboración con otras medidas de seguridad:** Se integra con herramientas de detección de fraudes y protección de la identidad para una estrategia de seguridad integral.

360 Brand Guardian actúa como una capa esencial de protección para las empresas que buscan reforzar su seguridad digital y cumplir con la normativa internacional. Su capacidad para identificar y eliminar amenazas en la Web, junto con su integración con estrategias de ciberseguridad más amplias, lo convierten en una herramienta clave dentro de cualquier programa de gestión de riesgos y cumplimiento normativo. Al reducir los riesgos de fraude, phishing y spoofing, ayuda a las organizaciones a mantener la confianza de sus clientes y a operar de forma segura en el marco de las mejores prácticas internacionales.

DE CARA AL ***FUTURO***

El futuro de la ciberseguridad exige un enfoque multicapa que equilibre la tecnología punta con una estrategia vigilante y previsora. Al invertir en defensas sólidas y fomentar una cultura de concienciación, las organizaciones pueden proteger sus datos, sus operaciones y -lo que es más importante- la confianza de sus clientes.

"La mejor defensa es la proactiva. En un mundo de amenazas cambiantes, ir por delante no es sólo una ventaja, es una necesidad. Appgate está aquí para garantizar que siempre estés un paso por delante".

ACERCA DE **APPGATE**

Appgate asegura y protege los activos y aplicaciones más valiosos de una organización. Appgate es el líder del mercado en Zero Trust Network Access (ZTNA) y protección contra el fraude en línea. Los productos de Appgate incluyen Appgate SDP para ZTNA Universal y 360 Fraud Protection. Los servicios de Appgate incluyen análisis de asesoramiento sobre amenazas e implantación de ZTNA. Appgate protege a miles de empresas y organismos públicos de todo el mundo. Más información en appgate.com.

appgate