Lo que está en juego con la innovación

Tendencias de ataque a los servicios financieros

En el panorama actual, tan caracterizado por una transformación digital sin precedentes, el sector de los servicios financieros se encuentra en una encrucijada de innovación y riesgo. A medida que la tecnología redefine el panorama de las transacciones financieras, al mismo tiempo inicia una nueva era de amenazas que apuntan al núcleo de la estabilidad económica.

Ataques contra los servicios financieros y sus clientes

9 000 millones
Número de ataques a aplicaciones web y API de servicios financieros

Número 1
Los servicios financieros son el sector con más ataques DDoS, incluso superando al sector de los videojuegos

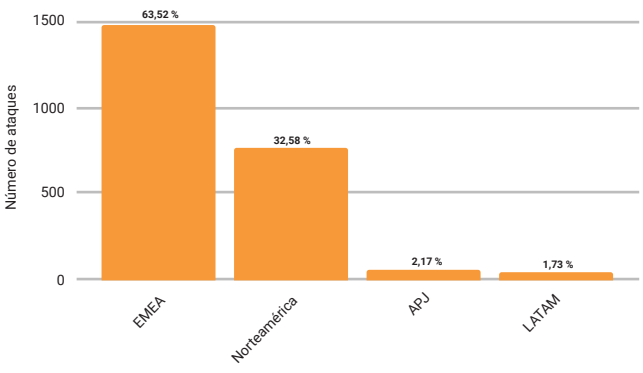
50,6 %
Los servicios financieros tienen el mayor número de víctimas de ataques de phishing en T2 2023

> 1 billón
Número de solicitudes de bots maliciosos

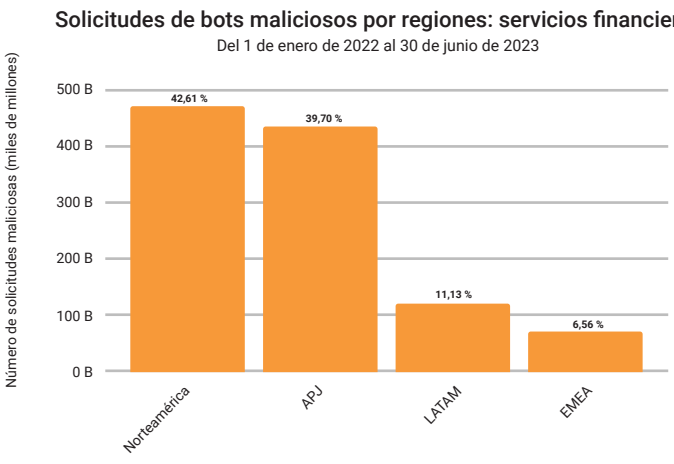
Instantáneas regionales

El número de ataques DDoS de capa 3 y capa 4 en Europa, Oriente Medio y África (EMEA) es casi el doble que en Norteamérica

Ataques DDoS por regiones: servicios financieros
Del 1 de enero de 2022 al 30 de junio de 2023



Solicitudes de bots maliciosos por regiones: servicios financieros
Del 1 de enero de 2022 al 30 de junio de 2023



Asia-Pacífico y Japón (APJ) es la segunda región objetivo de las solicitudes de bots maliciosos

Posibles riesgos de seguridad a los que prestar atención

API en la sombra
Las API no documentadas y sin seguimiento pueden plantear problemas de supervisión para las empresas que no son conscientes de quién las utiliza y de qué manera.

Scripts de terceros
Los atacantes pueden aprovechar las vulnerabilidades del cliente o inyectar código malicioso en scripts de terceros que se cargan como parte del sitio web. Esto expone a los servicios financieros al riesgo de robo de información web, lo que puede provocar que los datos de los clientes sean sustraídos o utilizados en transacciones no autorizadas.

Agregadores financieros
Las brechas de seguridad entre los agregadores financieros y la forma en que se recopilan los datos pueden crear una nueva vía de explotación para los atacantes, lo que lleva al robo de identidad.

Recomendaciones de seguridad y prácticas recomendadas

- Conozca su superficie de ataque para diseñar estrategias de mitigación y establecer controles de seguridad
- Implemente herramientas de seguridad de API para detectar y supervisar las API no autorizadas
- Consulte los 10 principales riesgos de seguridad de API según OWASP y el marco de MITRE ATT&CK para desarrollar medidas de formación y planes de prueba para grupos de penetración/simulación de ciberataques
- Utilice una estrategia de defensa multicapa que incluya la ejecución periódica de auditorías de seguridad y la implementación de detección y mitigación avanzadas
- Utilice soluciones como Client-Side Protection & Compliance (anteriormente conocida como Page Integrity Manager) que puedan mitigar los riesgos que plantean los ataques del lado del cliente
- Cree un modelo de control basado en el Edge para proporcionar visibilidad del tráfico de bots/API
- Realice un ejercicio en directo si no ha sufrido un ataque DDoS en los últimos tres trimestres; valide sus guías y lleve a cabo un seguimiento de las tendencias en cuanto a tamaño y velocidad para evaluar su riesgo en función de las capacidades actuales

Para obtener más información sobre la tendencia de los ataques en el sector de los servicios financieros, lea nuestro informe completo.

Descargar informe

 | Asistencia | Publicado en octubre de 2023