THREATQUOTIENT™

ThreatQ™ para servicios financieros

En lo que se refiere a ciberataques, el sector de los servicios financieros es un objetivo de gran atractivo y muy lucrativo. Durante tres años consecutivos, fue claramente el sector más atacado[1]: los clientes sufrieron un 65 % más ciberataques que en ningún otro sector[2].

A pesar de que emplean periódicamente funciones de análisis y simulación de respuesta a incidentes, y presentan tasas de detección y respuesta que se sitúan entre las más rápidas de la industria, las instituciones financieras siguen sufriendo compromisos y fugas de datos. El costo medio de la ciberdelincuencia para las compañías de servicios financieros ha aumentado hasta los 18.37 millones de dólares, el más elevado de todos los sectores[3]. Además de los fondos sustraídos, este costo incluye la detección, respuesta y notificación de la fuga de datos, las sanciones y procedimientos judiciales, así como la pérdida de negocio. De hecho, el sector experimenta la mayor tasa de rotación de clientes tras el incidente, solo superado por la asistencia sanitaria[4].

DESAFÍOS PRINCIPALES

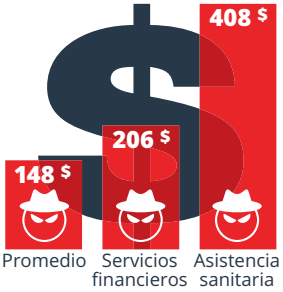
AUMENTO DE LAS SUPERFICIES DE ATAQUE

Los clientes esperan disfrutar de una disponibilidad continua de los servicios, desde cualquier dispositivo y en cualquier lugar. Los ciberdelincuentes interrumpen la marcha del negocio con ataques de denegación de servicio distribuido (DDoS). Estas campañas son relativamente sencillas de ejecutar mediante herramientas y servicios de terceros y se encuentran entre los tipos de ataques más costosos a los que se enfrentan las organizaciones. Las empresas sufren cada vez con más frecuencia ataques contra las redes sociales y móviles que utilizan para la atención y la interacción con sus clientes, así como para el desarrollo de sus operaciones comerciales. Aprovechando el hecho de que muy pocas instituciones financieras incorporan estos vectores en su modelo de amenazas, los ciberdelincuentes emplean timos de phishing, ingeniería social y malware para cometer fraudes financieros, provocar daños a la marca e incluso lanzar amenazas físicas. Para proteger sus superficies de ataque, cada vez mayores, las instituciones financieras necesitan visibilidad de toda la infraestructura, así como un enfoque proactivo y anticipado para cubrir las deficiencias en las defensas.

OBJETIVOS ATRACTIVOS

Los ciberdelincuentes atacan a las instituciones financieras porque ahí es donde está el dinero y son muchas las formas de sacar partido. Aprovechan de forma activa las vulnerabilidades de los cajeros automáticos (ATM), mientras que las redes como SWIFT (Society for Worldwide Interbank Financial Telecommunication) proporcionan a los grupos criminales vías para robar directamente de los bancos o transferir de forma clandestina el dinero robado de otras fuentes. Además, los datos de las cuentas bancarias de los clientes, las tarjetas de pagos y otra información de identificación personal se pueden convertir fácilmente en dinero. La mayoría de los analistas de seguridad están desbordados por la gran cantidad de alertas y necesitan poder centrarse en las amenazas relevantes y de alta prioridad, así como mejorar su capacidad de caza de amenazas.

COSTO POR REGISTRO ROBADO



El sector de los servicios financieros presenta el segundo mayor costo por registro robado (206 dólares); el promedio es de 148 dólares[4].

Aproximadamente el 36 % de las instituciones financieras sufrieron un incidente de seguridad o detectaron el acceso no autorizado a su infraestructura en 2018, lo que supone un incremento del 24 % desde 2017[5].

Los bancos y las instituciones de servicios financieros fueron el objetivo del 25.7 % de todos los ataques de malware el año pasado, más que ningún otro sector[6].

ATAQUES CONTRA APLICACIONES WEB

Las empresas de servicios financieros utilizan aplicaciones web para proporcionar una amplia gama de servicios online y digitales a empleados y clientes. Estas aplicaciones permiten a los usuarios enviar y obtener datos de bases de datos mediante sus navegadores. Los autores de amenazas aprovechan las vulnerabilidades de estas aplicaciones y los dispositivos utilizados para acceder a ellas, para infiltrarse en las redes y sistemas, y robar datos confidenciales y dinero. Hay una gran variedad de ataques contra aplicaciones web, por lo que las instituciones financieras deben saber en tiempo real cómo operan los adversarios y conocer las campañas y la infraestructura utilizada, para poder acelerar la respuesta y la prevención.

> *"Ahora se envían datos de indicadores de riesgo procedentes de fuentes de confianza a listas de vigilancia solo para detección en varios controles de seguridad internos, sin necesidad de que los miembros del equipo realicen una supervisión diaria. Lo que es más importante, exportamos datos seleccionados a la herramienta adecuada para su consumo, por lo que no procesamos ingentes cantidades de datos a través la red, con la consiguiente ralentización del funcionamiento general que esto implicaría".*
>
> — Director de respuesta a amenazas, empresa de servicios financieros del índice Fortune 500

PONIENDO ORDEN EN LAS OPERACIONES DE SEGURIDAD DE LOS SERVICIOS FINANCIEROS

Una plataforma robusta de inteligencia sobre amenazas debe ser capaz de ofrecer a los proveedores de servicios financieros el contexto y la capacidad de priorizar que necesitan para poder adoptar mejores decisiones, acelerar la detección y la respuesta, e impulsar la colaboración entre los equipos y el aprendizaje que facilita una mejora continua. No es preciso alterar la infraestructura o los flujos de trabajo de seguridad existentes; todas las herramientas y tecnologías funcionan perfectamente con la arquitectura abierta de ThreatQ.

CONSIGA MÁS CON THREATQ:

- **CONSOLIDACIÓN** en un repositorio central de todas las fuentes de inteligencia sobre amenazas y datos de vulnerabilidades externas (p. ej., FS-ISAC) e internas (p. ej., SIEM).
- **ELIMINACIÓN** del ruido y fácil navegación por enormes cantidades de datos para centrase en los recursos y las vulnerabilidades fundamentales.
- **PRIORIZACIÓN** de lo que es más importante para su entorno.
- **CAZA PROACTIVA** de actividad maliciosa que pueda ser indicativa de compromiso de datos de cuentas bancarias, fraude con tarjetas de pago, ataques DDoS y otros perjuicios para los consumidores y comercios.
- **FOCO** en las vulnerabilidades de seguridad conocidas en exploits activos actualmente, que pueden afectar a su nivel de cumplimiento de normativas y de seguridad.
- **ACELERACIÓN DEL ANÁLISIS** y la respuesta a ataques contra varios objetivos, incluidos sistemas ATM, la red SWIFT, las aplicaciones web, los nuevos canales digitales y la infraestructura de apoyo.
- **ENVÍO AUTOMÁTICO** de la inteligencia sobre amenazas a las herramientas de detección y respuesta.

Solicite una demostración en directo de la plataforma ThreatQ y ThreatQ Investigations en threatq.com/demo.

1 IBM, "2019 IBM X-Force Threat Intelligence Index" (Índice de inteligencia sobre amenazas IBM X-Force 2019), https://www.ibm.com/account/reg/us-en/signup?formid=urx-36763

2 The World Bank, "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision" (Ciberseguridad, ciberriesgo y regulación y supervisión del sector financiero), 2018, http://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and- financial-sector-regulation-and-supervision

3 Accenture, "The Cost of Cybercrime" (El costo de la ciberdelincuencia), 2019 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

4 IBM, "2018 Ponemon Cost of a Data Breach Study" (Estudio del costo de una fuga de datos, Ponemon 2018), https://www.ibm.com/security/data-breach

5 Security Boulevard, "Cybersecurity Investment to Shoot Up in Financial Industry in 2019; Top Firms Already Spend $1 Billion" (La inversión en ciberseguridad se dispara en el sector financiero en 2019; las principales instituciones ya han gastado 1000 millones de dólares), https://securityboulevard.com/2018/12/cybersecurity- investment-to-shoot-up-in-financial-industry-in-2019-top-firms-already-spend-1-billion/

6 Helpnetsecurity, "Which cyber threats should financial institutions be on the lookout for?" (¿Cuáles son las ciberamenazas a las que deberían prestar atención las instituciones financieras?), https://www.helpnetsecurity.com/2019/04/30/2019-cyber-threats-finance/

ACERCA DE THREATQUOTIENT™

El objetivo de ThreatQuotient es mejorar la eficacia y la eficiencia en las operaciones de seguridad mediante el empleo de una plataforma centrada en las amenazas. Gracias a la integración de los procesos y tecnologías de una organización en una sola arquitectura de seguridad, ThreatQuotient acelera y simplifica las investigaciones y facilita la colaboración tanto dentro de cada equipo, como entre distintos equipos y herramientas. Mediante la automatización, la priorización y la visualización, las soluciones de ThreatQuotient reducen la cantidad de información irrelevante y destacan las amenazas que tienen mayor prioridad con el fin de facilitar su detección y ayudar con la toma de decisiones cuando los recursos son limitados. ThreatQuotient tiene su sede central en Virginia del Norte y centros de operaciones internacionales en Europa y Asia-Pacífico. Para obtener más información, visite https://threatquotient.com.

ThreatQ-for-Financial-Services_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885