23 CONGRESO NACIONAL DE SEGURIDAD

BIENVENIDOS!

Su Presentador:
Braudilio Feliz
Administración de Empresas – UASD
Master en Telecomunicaciones – Golden Gate University
Experiencia basada en muchos años de trabajo
Capas 2 y 3 Switches y Routing
Capas 4-7 ADC – Application Delivery Controllers
API expertise
Kubernetes, Cloud, etc. etc.

Vivo en California, pero Dominicano de pura cepa

CNS

23 CONGRESO NACIONAL DE SEGURIDAD

CNS

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

size: records lost **filter**

interesting story

search...

IN OCTOBER, GOOGLE dramatically announced that it would shut down Google+ in August 2019, because the company had discovered through an internal audit (and a simultaneous *Wall Street Journal* exposé) that a bug in Google+ had exposed 500,000 users' data for about three years. Maybe it should have pulled the plug sooner.

On Monday, Google announced that an additional bug in a Google+ API, part of a November 7 software update, exposed user data from 52.5 million accounts. Or as Google puts it, "some users were impacted." Google found the flaw, and corrected it by November 13. This means that app developers would have had improper user data access for six days. Google says it doesn't have any evidence that the data was misused during that time, or that Google+ was compromised by a third party. But the company is now moving up Google+'s termination date to April, and it will cut off access to Google+ APIs in 90 days.

LEARN MORE

"Our testing revealed that a Google+ API was not operating as intended. We fixed the bug promptly and began an investigation into the issue," David Thacker, Google's vice president of product management, wrote in a blog post on Monday. "We have begun the process of notifying consumer users and enterprise customers that were impacted by this bug. ... We want to give users ample opportunity to transition off of consumer Google+."

Ref: https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

The Experian Credit Score Breach: What Happened and How to Prevent Future API Data Breaches

Published on May 3, 2021, by Cloudentity

Share:

Last week, the public was notified about a pretty serious Experian API-related incident leading to the potential public exposure of credit scores for millions of Americans.

Ref: https://cloudentity.com/2021/05/03/the-experian-credit-score-breach-what-happened-and-how-to-prevent-future-api-data-breaches/

CISA Insights on APT Compromise of Microsoft 365 Via Password Exploits

The APT actors behind the SolarWinds attack are leveraging compromised Microsoft 365 and Azure applications, as well as password exploits and API access to compromise cloud resources.

Ref: https://healthitsecurity.com/news/cisa-insights-on-apt-compromise-of-microsoft-365-via-password-exploits

Optus data breach: everything we know so far about what happened

Who is the attacker? How was the data accessed? What was taken? Digital security experts explain

- Follow the day's news, live
- Get our free news app, morning email briefing or daily news podcast

How was the data accessed?

Reports suggest Optus had an application programming interface (API) available online that did not require authorisation or authentication to access customer data.

Up to 10 million Optus customers are believed to have had their details accessed by an unknown hacker. Photograph: AnuchaCheechang/Getty Images/iStockphoto

Ref: https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened

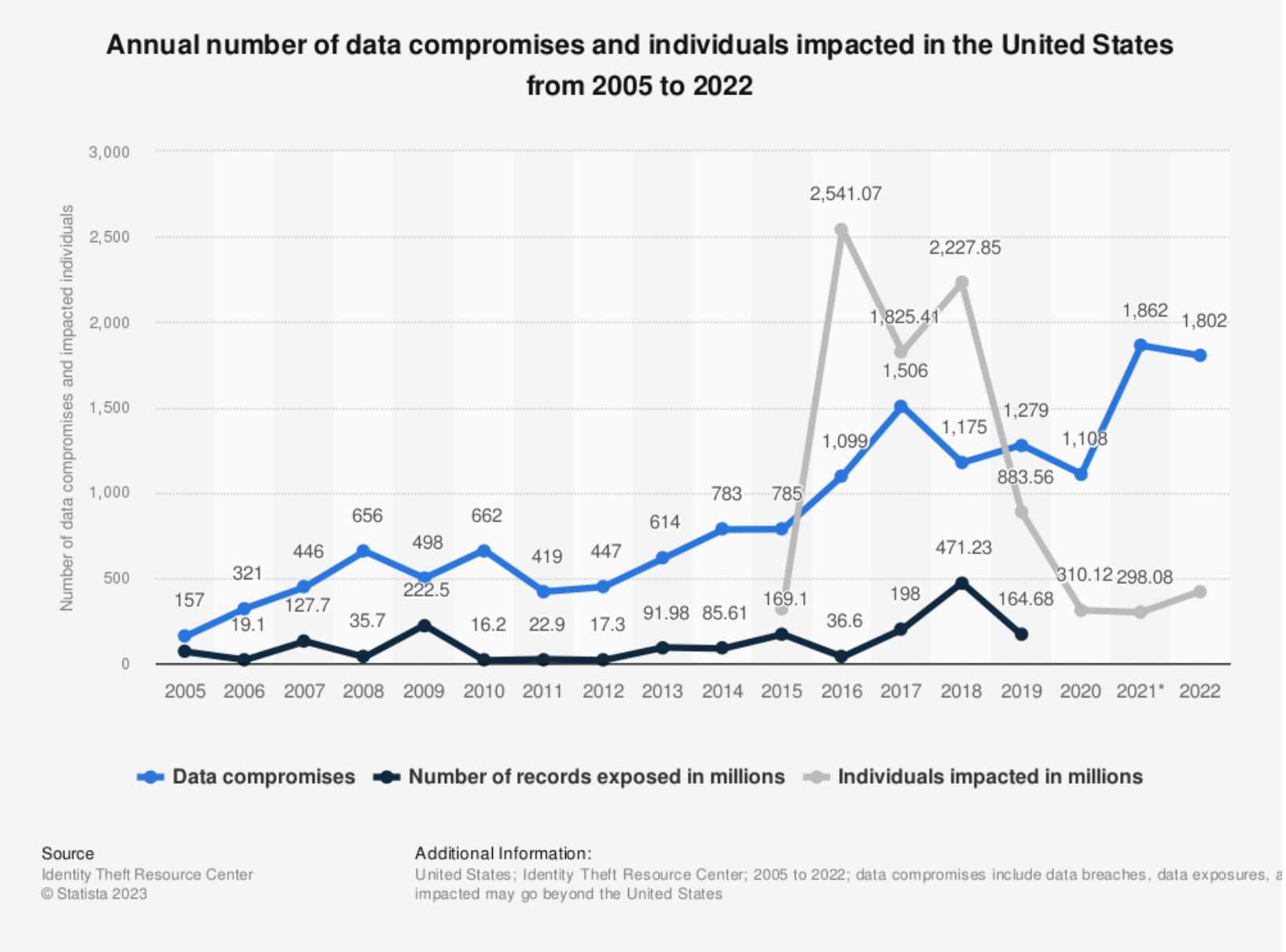
Sector Financiero – Diferentes Casos

Protección contra fraudes y ataques:

- Toma de posesión de acceso virtual del usuario (ATO)
- Identificación de cuentas inactivas
- Fraudes en pagos virtuales
- Pagos a terceros por servicios
- Creación de falsos usuarios
- Utilización de fuerza bruta o credenciales robadas en los puntos de entradas (Login)
- Falsos prestamos virtuales utilizando credenciales robadas o abusando el proceso en combinación con ingeniería social
- Desvio de prestamos a otras cuentas

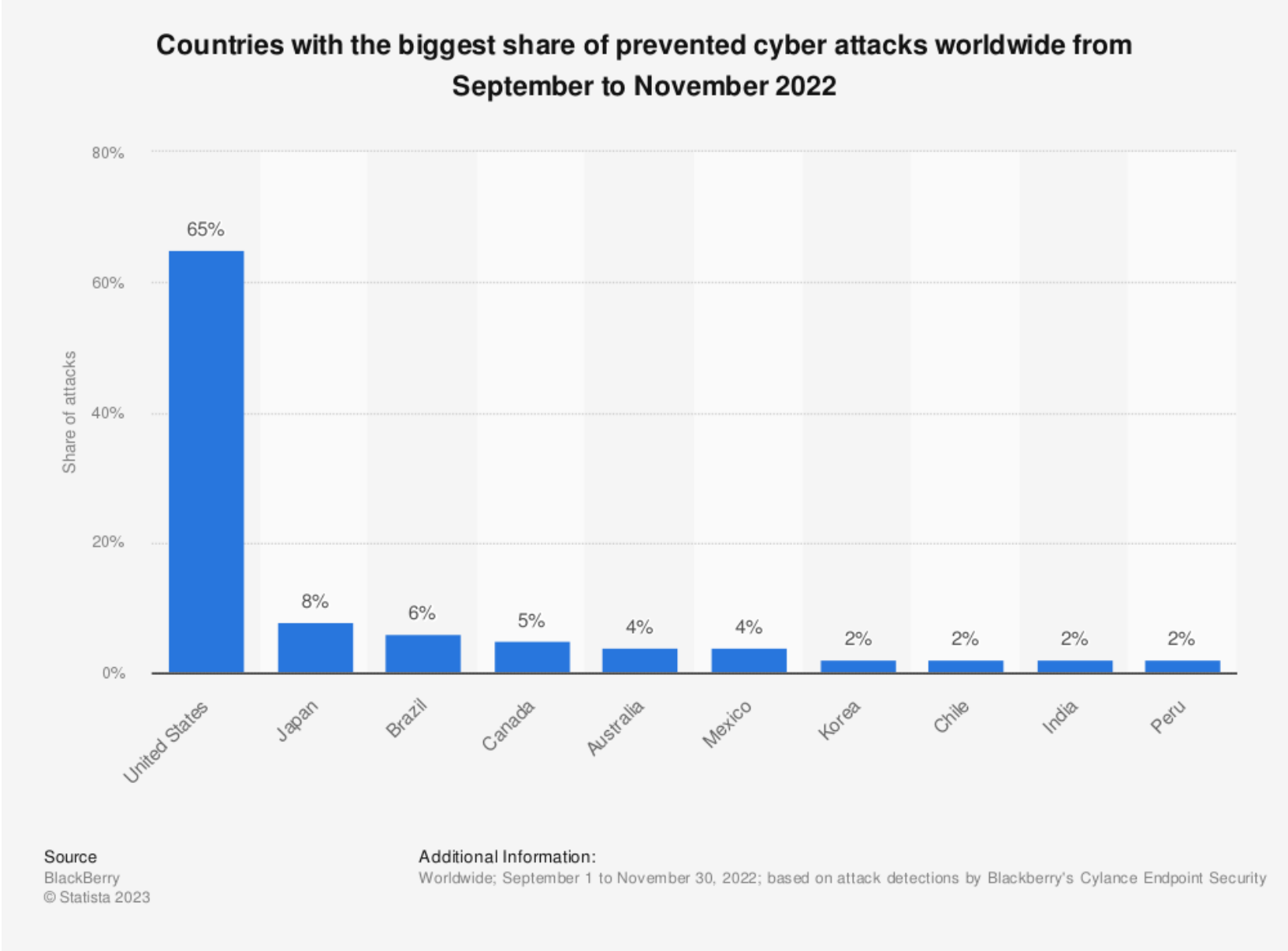
Sources: Gartner, Cequence Threat Report, Cequence estimate from publicly disclosed records breach data

Informaciones de usuarios comprometidas



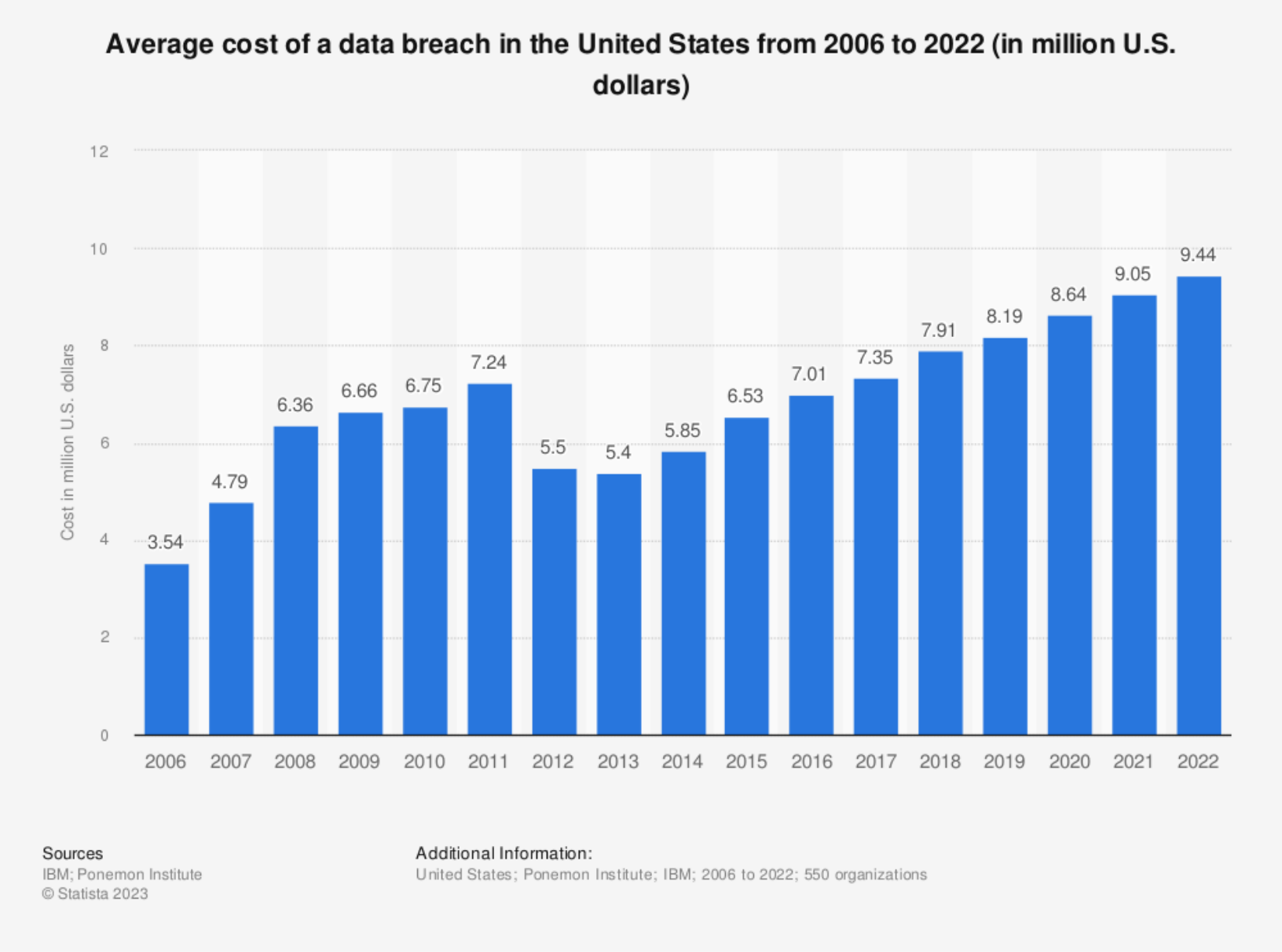
Distribución por país de ataques cibernéticos

Sept-Nov 2022



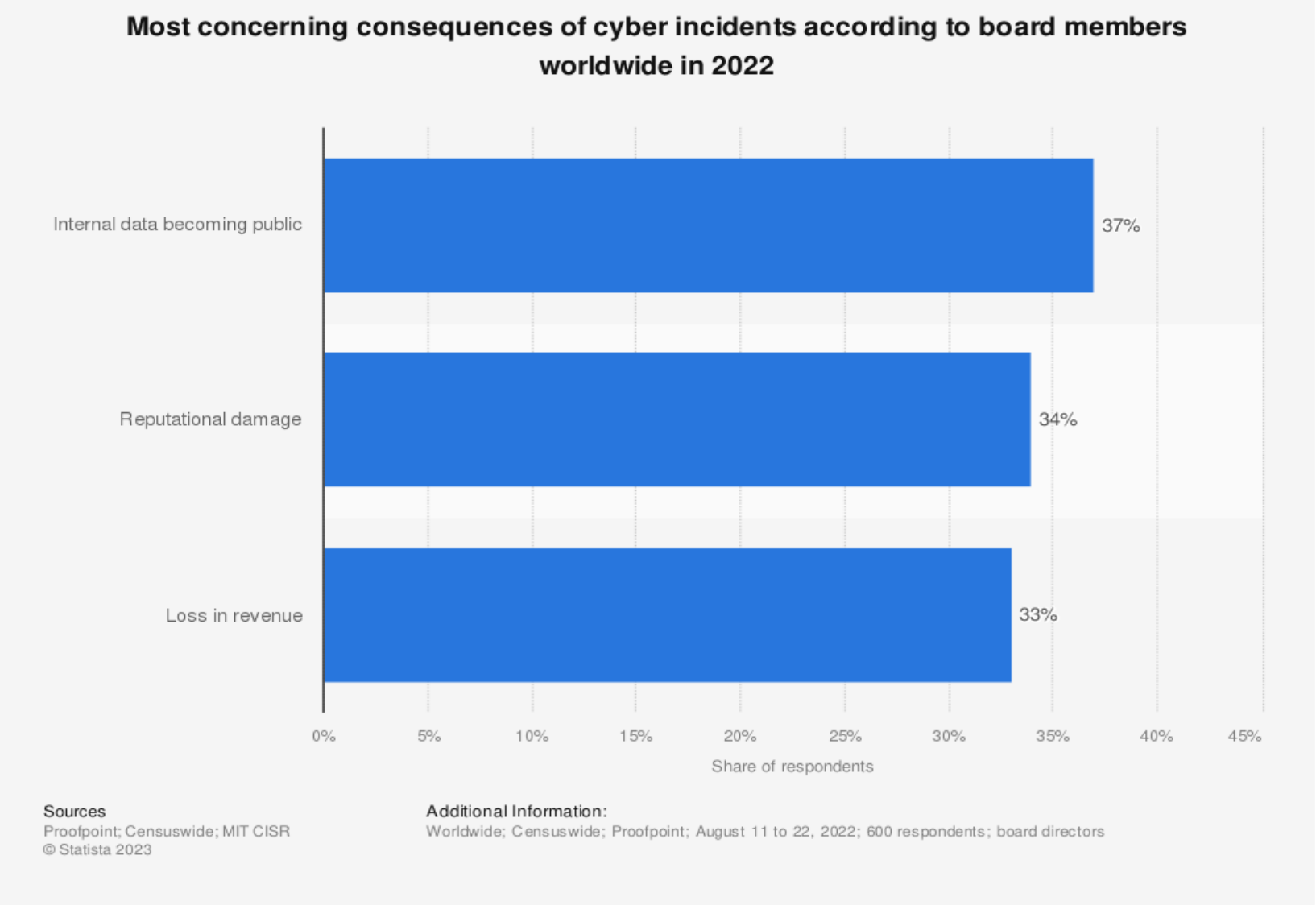
Costo promedio consequencia de ataques cibernéticos

2006 a 2022



Preocupaciones de consequencias de los ataques cibernéticos

2022



APIs en el Mundo Financiero

70%

Requisas de applicaciones

Provienen de transacciones de APIs

90%

De Ing de Desarrollo

Utilizan APIs privadas o de un tercero

50%

Pagos B2B

Y movimiento de fondos via APIs

$49.9B

Costo total de frauds en el sector Financiero. Cada $1 de fraude financiero corresponde a un costo verdadero de $4.16.

42%

El Cybercrimen cuesta a los servicios Financieros 42% más que cualquier otro vertical.

Source: LexisNexis True Cost of Financial Crime Compliance Study

Las APIs han cambiado las reglas del juego para los Hackers

53%

Organizaciones impactadas
Tres o más ataques contra APIs cada mes

80%

Del tráfico bloqueado
A systemas de compañías y basado en API

63M

Registros infiltrados
anualmente, aprovechando las vulnerabilidades de las APIs

2x

Incremento en brechas de seguridad relacionadas con APIs para el 2025

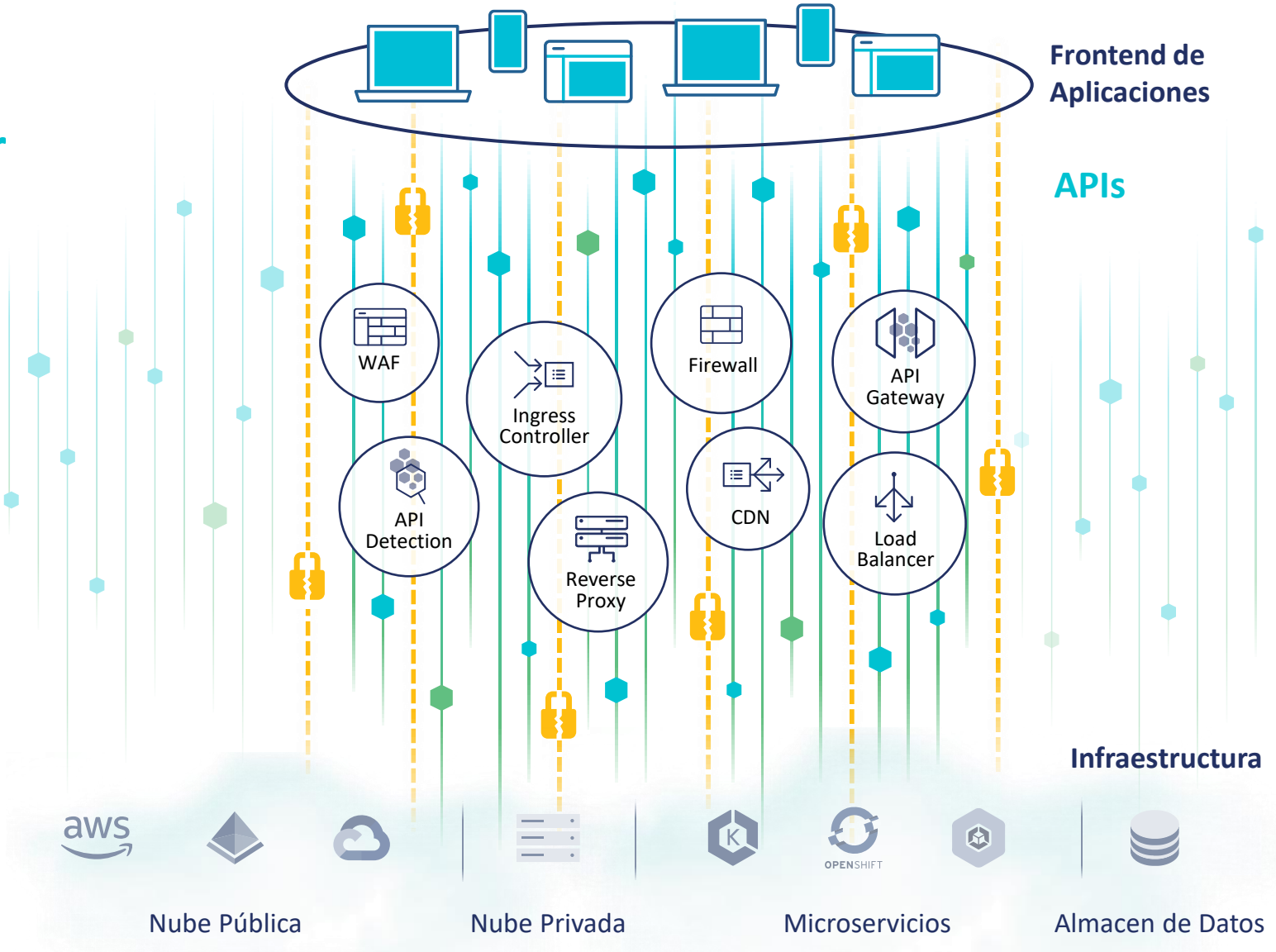
Sources: Gartner, Cequence Threat Report, Cequence estimate from publicly disclosed records breach data

Infraestructura de protección de APIs muy fragmentada

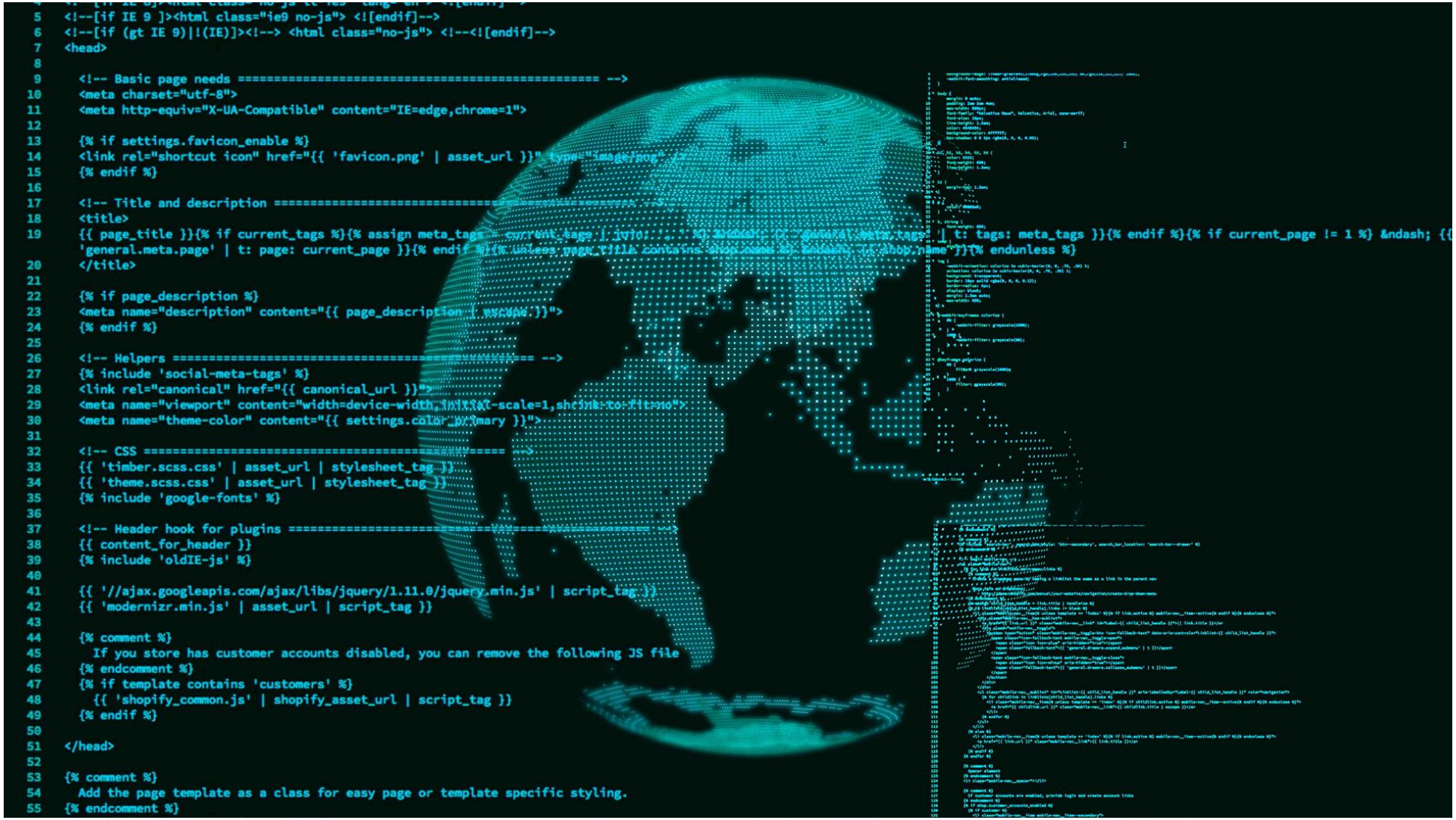
100x de APIs se escoden **sin ser descubiertas** y se convierten en APIs paralelas (shadow APIs)

Incluso aquellas APIs conocidas son **Protegidas pobremente**

Y las soluciones **Fallan en capacidad de crecimiento y efectividad**



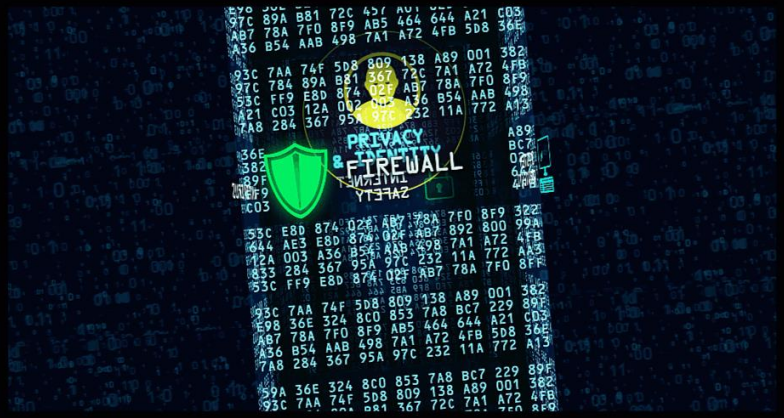
Ataques cibérneticos de todas partes del mundo



Aplicaciones hoy en dia

Todo basado en móvil y APIs

Estan tus sistemas seguros?



Los Servicios Financieros funcionan en APIs

2019

OFX,
el estandard para intercambio de datos financieros,
combinado con FDX
para crear un estandard API

2021

FFIEC
revisó sus guías de seguridad , añadiendo recomendaciones especificas para seguridad de APIs, por ejemplo creando un inventario de las APIs para determinar la superficie de ataque

Según
Financial Data Exchange,
28M+
cuentas de consumidores utilizan**FDX API**

Financial Data Exchange

Preguntas que los Servicios Financieros deben investigar

Cuantas APIs tengo?

Son mis APIs atacadas?

Cual es mi riesgo de superficie de mis APIs?

Modelo de protección de APIs

Alto nivel de madurez

WAF

Solo detecta vulnerabilidades conocidas

Bot Detection

Requiere horas de configuración manual

API Gateway

Concentrada en seguridad para la ingenieria de desarrollo

API Security

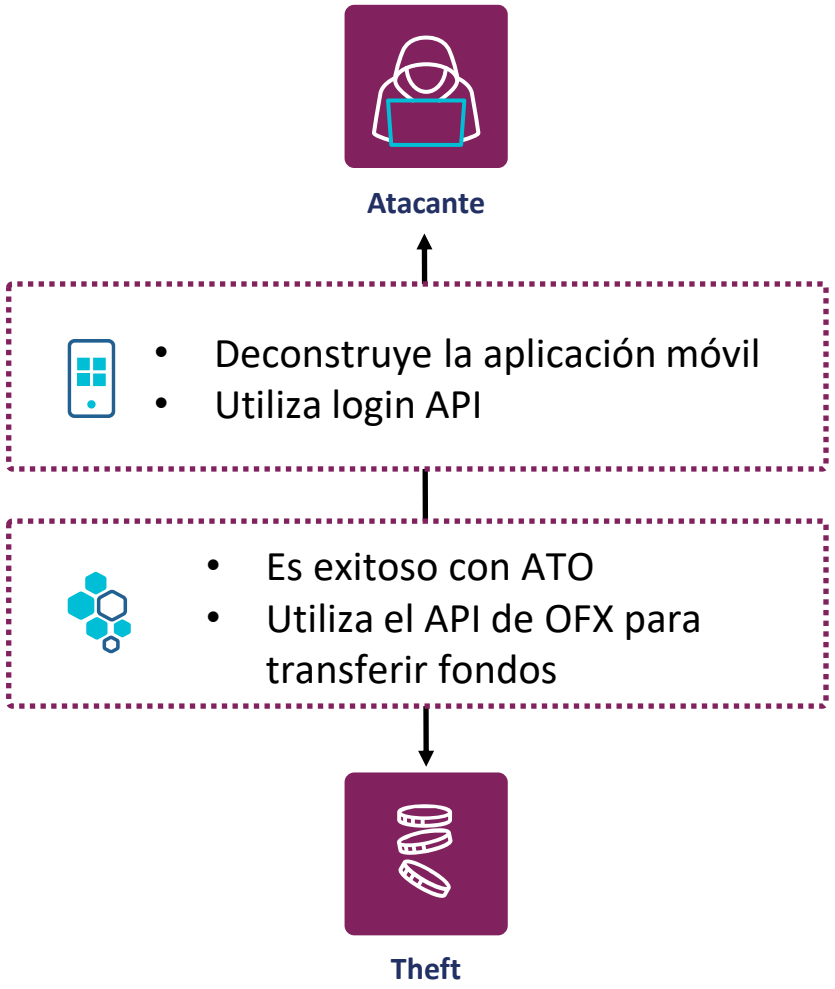
Varias soluciones para resolver cada uno de los problemas con las APIs

Productos Avanzados

Brindando seguridad para las APIs en un ciclo completo, normalmente ofrecidas como una Plataforma y fuertemente basados en ML

Preveniendo ATOs y Fraude Financiero

Ejemplo práctico de una institución financiera



Problema

- 50-90% del tráfico de login es automatizado
- ~40% de las conecciones de login son a tráves de móvil
- Resultado de un ataque: fraude y clients mal-contentos

Objectivo

- Una Plataforma que prevenga el fraude y mantenga en alto los niveles de satifacción de los clients

Solución

- Analysis basado en ML para detector tráfico malicioso
- Utilizar Honey Pots para engañar, por lo menos por un rato, al atacante
- Bloquear el tráfico por completo sin afectar la clientela

ATO & Robo de Fondos a tráves de las APIs

Ciclo de Protección para las APIs

Una Solución efectiva debe de contar con todo lo siguiente

Descubrimiento
Identificar todas los servidores de APIs

Detección
Detectar Ataques según occurren

Inventario
Proveer un Inventario Unificado de todas las APIs

Protección
Bloqueo de ataques en Tiempo Real

Conformidad
Asegurar adherencia a las prácticas de Seguridad y de Gobernanza de Datos

Testing
Seguridad en nuevas APIs antes de producción

Recomendaciones para un programa de protección de las API

Prevenir Acceso no Autorizado

Utilizar medios de autenticación fuertes y controles basados en el uso de tokens para autorizaciones

Inventario De las APIs

Sumamente importante identificar todas las APIs, conocidas y desconocidas incluyendo OFX/FDX

Governanza de las APIs

Asegurarse que las APIs se adhieren a las especificaciones técnicas y regulatorias (FFIEC)

Evitar ser víctima de ataques de DDoS

Identificar puntos de conección de APIs que deban utilizar Rate Limit

Testing Seguridad

Descubrir debilidades y errores de seguridad que puedan contener las APIs durante su desarrollo antes de ser publicadas

Bloquear Pagos o transferencias Fraudulentas

Correlación de anomalias generated by ML y que estan relacionadas con detección de ataques en el area PCI-DSS

Gracias – hora de ir a la playa! O el Bar?