Estado de la Amenaza

Octubre 2016

Claudio Tana

Gerente de Consultoría

ctana@neosecure.com

Cel. +54 911 35152388

Algunos hechos recientes

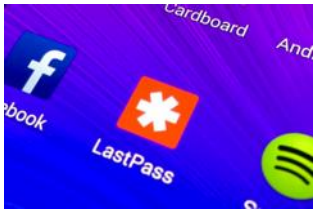
NEOSECURE

OPM

juniper NETWORKS

]HackingTeam[

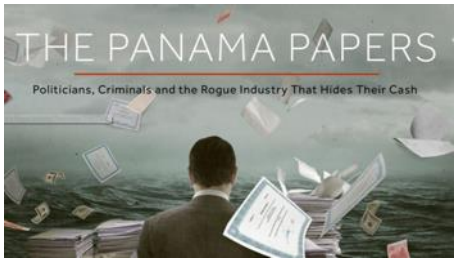
staminus SecureShield



IRS

Kreditech DIGITAL LENDING

Apple Developer Tools
XcodeGhost



Hay que entender bien la amenaza

La amenaza se ha diversificado. Por un lado más compleja, y por otro, se comporta como una industria lucrativa que opera muy bien.

Clasificación

Agenda

NEOSECURE

- Clasificación de las Amenazas
- Amenazas del Tipo I
- Amenazas del Tipo II
- Amenazas del Tipo III

Agenda

NEOSECURE

- Clasificación de las Amenazas
- Amenazas del Tipo I
- Amenazas del Tipo II
- Amenazas del Tipo III

Clasificación de las Amenazas

Permite agrupar diferentes amenazas bajo características similares, facilitando el entendimiento y a su vez agilizando el proceso de evaluación del riesgo y la preparación frente a la respuesta a incidentes.

Amenazas Tipo I

- Nivel avanzado y personalizado de:
  - Técnicas
  - Tácticas
  - Procedimientos

Amenazas Tipo II

- Nivel profesional de:
  - Técnicas
  - Tácticas
  - Procedimientos

Amenazas Tipo III

- Uso de técnicas básicas

Agenda

- Clasificación de las Amenazas
- Amenazas Tipo I
- Amenazas Tipo II
- Amenazas Tipo III

Técnicas utilizadas

- Caracterización
  - Desarrollo de exploits 0-Day
  - Desarrollo de malware 0-Day
  - Estudio de procesos internos
  - Know-how específico de sistemas complejos
  - Espionaje
  - Ingeniería social
- Usos
  - Espionaje industrial y político
  - Guerra electrónica
  - Sabotaje
- Origen
  - Gobiernos
- Destino
  - Empresas de alta tecnología, infraestructura crítica, gobiernos


Las amenazas tipo 1 están hechas a medida, contemplan piezas de alta ingeniería y su detección es muy compleja

Agenda

- Clasificación de las Amenazas
- Amenazas del Tipo I
- Amenazas del Tipo II
- Amenazas del Tipo III

Descripción

- Caracterización
  - Uso de malware comercial o de dominio público, personalizado para el ataque
  - Explotación de vulnerabilidades ya existentes
  - Explotación de vulnerabilidades de aplicación
  - Ingeniería social
  - Preparación de mediano plazo

- Usos
  - Fraude, robo de credenciales, activismo, extorsión
- Objetivos
  - Bancos, Retail, Cadenas de Restaurants y Hoteles, Hospitales, Gobiernos
- Origen
  - Grupos delictuales
  - Grupos activistas

Es una industria establecida

Ecosistema

Análisis de principales amenazas

Ataques al canal electrónico

- DDoS
- Malware
- Hacking Aplicativo

Ataques externos

- Explotación de vulnerabilidades
- Malware
- Spearphishing
- Evasión

Ataques Internos

- Suplantación
- Vulnerabilidad Aplicativa
- Insiders

Agenda

NEOSECURE

- Clasificación de las Amenazas
- Amenazas del Tipo I
- Amenazas del Tipo II
- Amenazas del Tipo III

Descripción

- Lo que caracteriza a estas amenazas es su bajo nivel de preparación
- A sus autores se les denomina Script-Kiddies
- No generan gran impacto, salvo daño colateral a quienes no poseen controles de seguridad

Cómo ha evolucionado el escenario

NEOSECURE

Symantec

No es casualidad que los incidentes a las empresas **high-tech** hayan disminuído. Se ha hecho un **gran esfuerzo** en introducir **nuevos controles** de seguridad.

DOW

JUNIPER NETWORKS

2010-2013

2015

NORTHROP GRUMMAN

KASPERSKY lab

Focos de Acción

- Protección contra Malware y Ransomware
- Automatizar la respuesta a Incidentes de seguridad
- Monitorear la actividad y el comportamiento de los usuarios
- Eliminar las puerta traseras en aplicaciones de negocio
- Proteger los datos en repositorios locales y en la nube
- Revisar y evaluar la arquitectura de red

Conclusiones

Frente a las amenazas Tipo 1 la defensa es posible, pero es cara y compleja.

La industria local debe preocuparse de las amenazas Tipo 2

¡Muchas Gracias!


COLOMBIA
PERU
CHILE
ARGENTINA