RANSOMWARE

QUE NO DETENGA TU NEGOCIO

NEOSECURE

SABEMOS DE SEGURIDAD

RANSOMWARE

QUE NO DETENGA TU NEGOCIO

Claudio Tana
Gerente de Consultoria
NeoSecure Argentina

AGENDA

- Estado de las amenazas
- Ransomware
- Cómo opera
- ¿Cómo controlar Ransomware?

NEOSECURE
SABEMOS DE SEGURIDAD

“Credenciales legitimas de usuarios fueron usadas en la mayoría de las intrusiones de datos, con casi el 63% de estas siendo muy débiles, default, o robadas”

2016 Verizon Data Breach Investigations Report (DBIR)

CASOS REGIONALES DE RANSOMWARE

NEOSECURE
SABEMOS DE SEGURIDAD

- **2 Clínicas**
  - Ingresan de forma remota
  - Cifran base SQL Server, y sus respaldos
  - ERP deja de operar, **dificultades en pagar sueldos**
- **Clínica oftalmológica**
  - Secuestran datos de estación de trabajo
  - **Secuestro cuenta Google**
- **Empresa Distribuidora**
  - Cifran repositorio compartido de archivos (FTP)
- **Cadena de supermercados**
  - Se infecta usuario, avisa a TI
  - **TI pierde datos de servidor central**
  - Recuperan una parte desde respaldos

- **Empresa Minera**
  - Usuario busca en google temas académicos
  - Es redireccionado a sitio con malware, se infecta.
  - **Cifran todos sus datos**

- **Farmacia**
  - Usuario de TI se infecta al navegar
  - Cifr**an datos del servidor central**
  - **150 sucursales inoperativas por aprox 24 horas.**

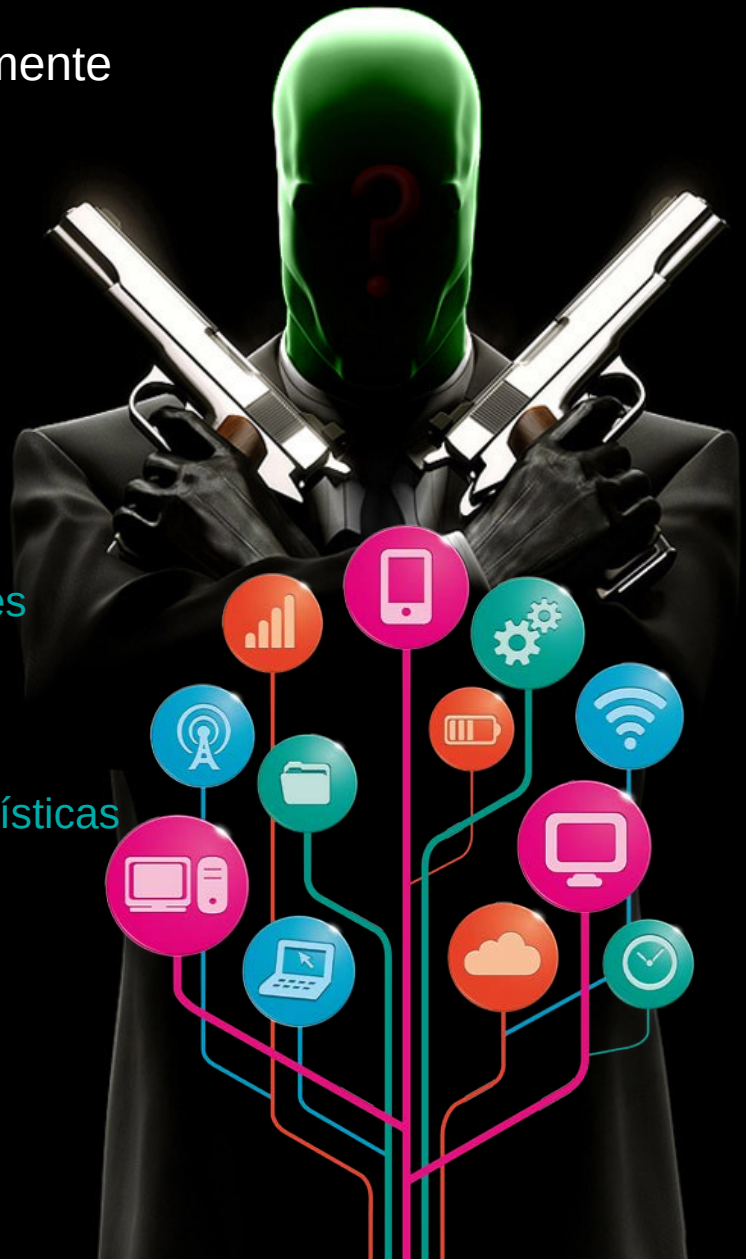
AGENDA

- Estado de las amenazas
- Ransomware
- Cómo opera
- ¿Cómo controlar Ransomware?

Ransomware

RANSOMWARE

- Un cibercriminal selecciona cuidadosamente a sus próximas víctima
- Les envía un malware que bloquea el acceso a sus datos
- Solicita un rescate en Bitcoins

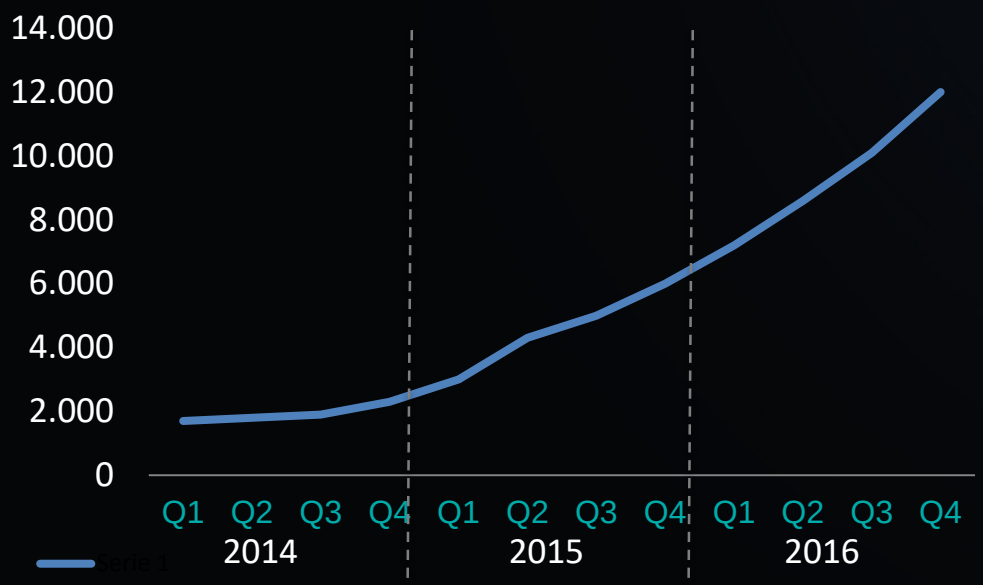


Negocio genera sobre US$300M anuales

El Ransomware como servicio disparó las estadísticas

Un solo proveedor de servicio infecta más de 3.000 víctimas

Evolución Ransomware

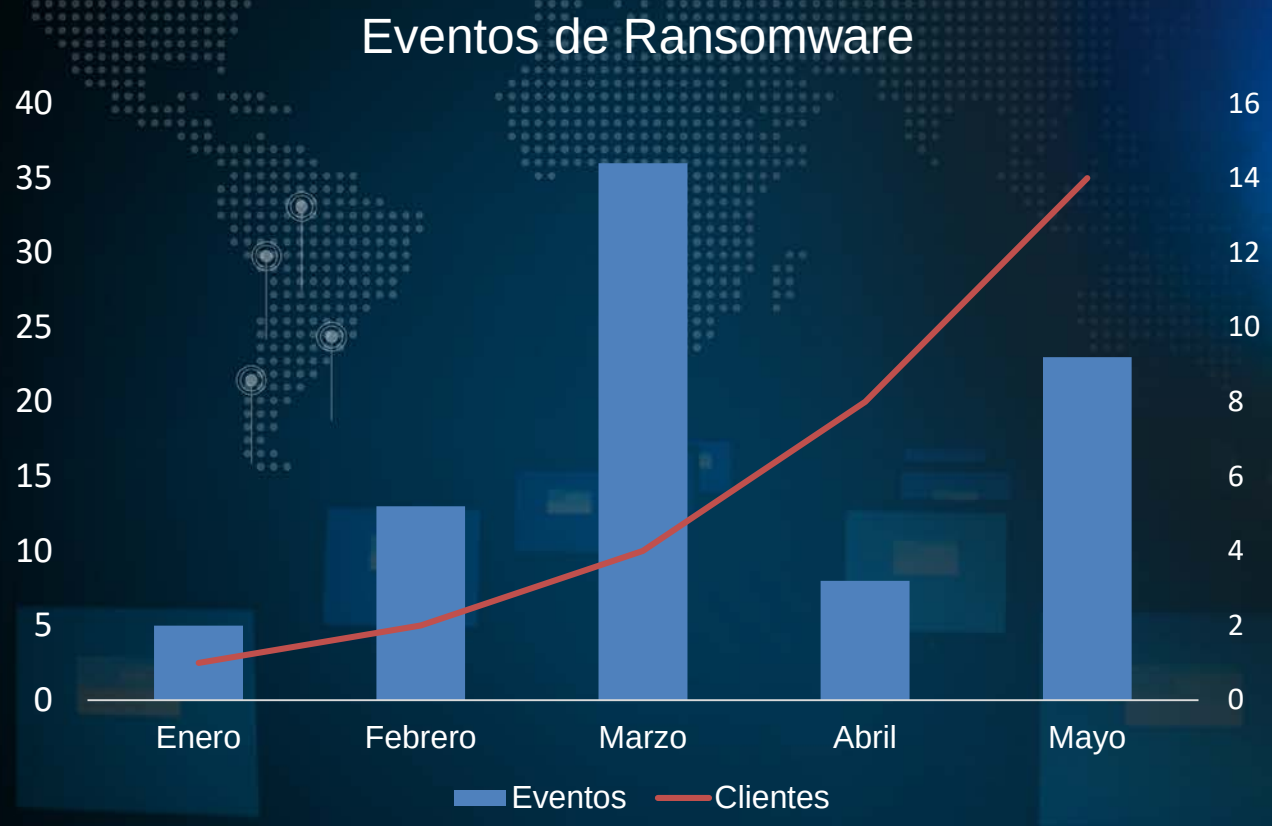


Fuente: Intel Security

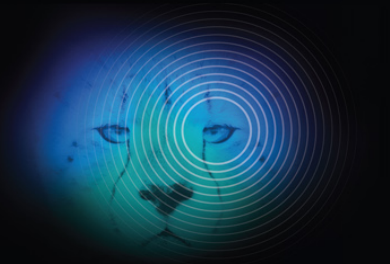
- Primeras versiones presentaban fallas
- Sólo algunos conocían el negocio
- Hoy es una industria establecida

NEOSECURE
SABEMOS DE SEGURIDAD

DATOS LOCALES



Fuente: Data Science NeoSecure



AGENDA

Estado de las amenazas

Ransomware

Cómo opera

¿Cómo controlar Ransomware?

¿QUÉ HACE EL RANSOMWARE?

NEOSECURE
SABEMOS DE SEGURIDAD

- El Ransomware está diseñado para:
- Prevenir el acceso y uso regular del sistema operativo
- Cifrar los archivos para que no puedan ser utilizados
- Evitar que se ejecuten algunas aplicaciones

- Para devolver el equipo a un estado operativo “normal”, el ransomware demanda que el usuario:
- Pague una suma (mediana a considerable) de dinero
- Algunos más excéntricos piden al usuario que completen encuestas

Cómo Opera Ransomware

NEOSECURE
SABEMOS DE SEGURIDAD

El proceso de recuperación ante un ataque de Ransomware es largo

1. Abrir una billetera en Bitcoins
2. Comprar Bitcoins
3. Depositar al hacker y obtener llave
4. Descifrar los archivos
5. Restaurar los respaldos

No Hay Garantía de Recuperación

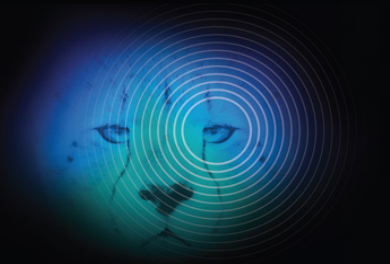
LOS VECTORES DE INFECCIÓN MÁS COMUNES

- Correo electrónico (SPAM y spoofing de cuentas legítimas)
- Redes P2P (torrents)
- Sitios Web infectados
- Enlaces compartidos hacia servicios de almacenamiento en la nube
- Aplicaciones “truchas” para dispositivos móviles distribuidas fuera de las appstores oficiales

LO MÁS RECIENTE…

NEOSECURE
SABEMOS DE SEGURIDAD

- Nadie se salva:
  - Más y más variedades de ransomware para Windows
  - Variantes específicas para Linux
  - Variantes específicas para Mac OS X
  - Variantes específicas para Android e iOS
- En marzo/2016 se detectó que algunos anuncios publicitarios (desarrollados en Adobe Flash) en varios sitios importantes de noticias estaban infectados con ransomware: New York Times, Newsweek, MSN, BBC…
- Ya es hoy el cyber-ataque más común en Latinoamérica
- Recién algunos fabricantes están liberando herramientas o módulos anti-ransomware



AGENDA

Estado de las amenazas

Ransomware

Cómo opera

› ¿Cómo controlar Ransomware?

Control de Ransomware

- Denegar la descarga y ejecución del código conocido malicioso
- Permitir la ejecución del código confiable conocido
- Evaluar mediante varias técnicas lo desconocido. Posteriormente decidir su ejecución

Control del Ransomware

NEOSECURE
SABEMOS DE SEGURIDAD

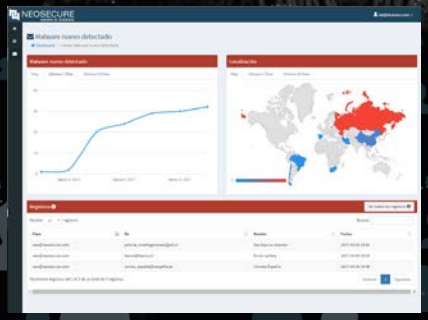
- Detección avanzada de:
  - Correo Phishing y adjuntos maliciosos
  - Archivos maliciosos en la web
  - Comunicación de comando y control de malware
- Análisis en Sandboxing
- Generación de indicadores de compromiso
- Bloqueo de amenazas antes que ingresen a la red

NEOSANDBOX:

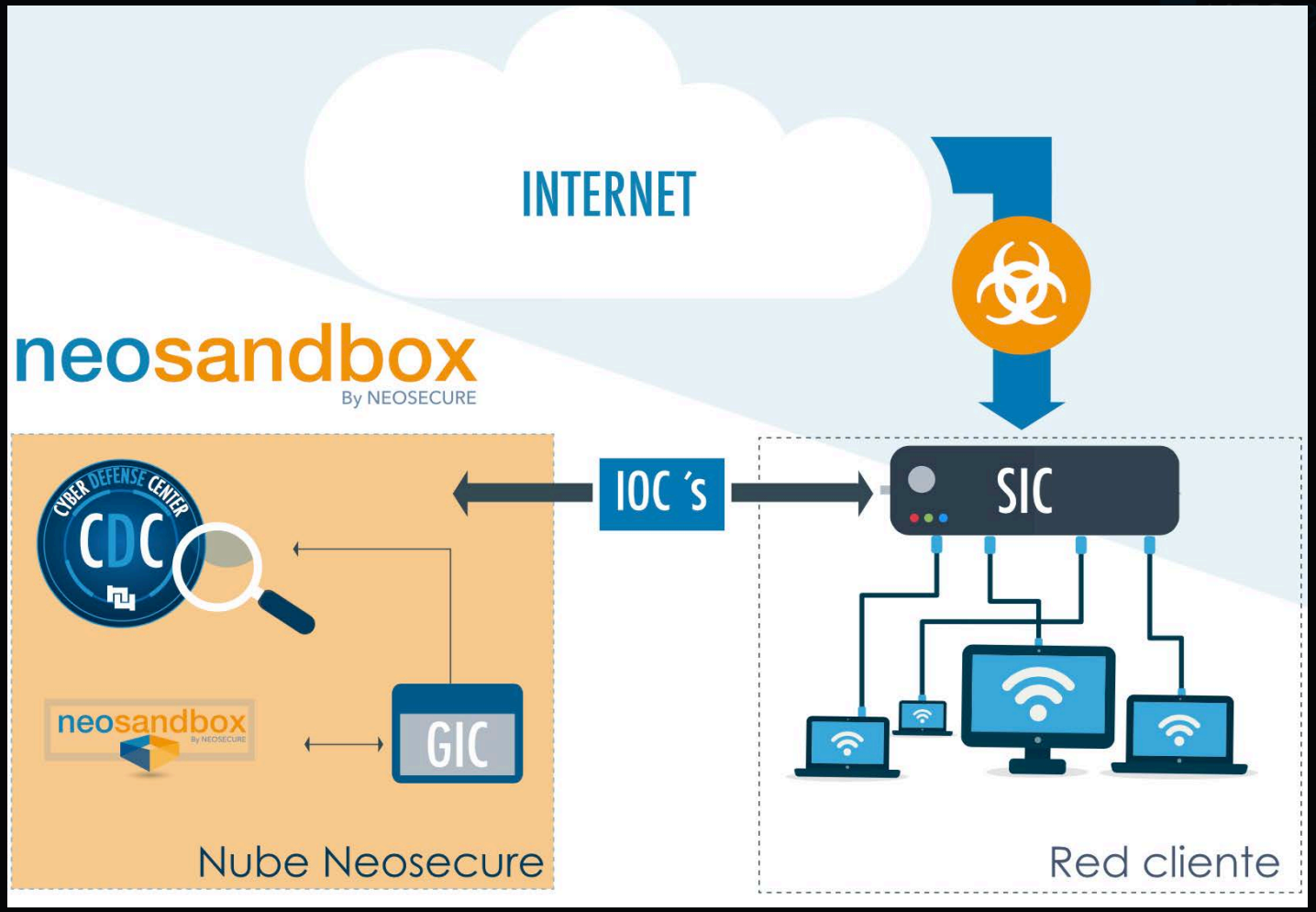
LA SOLUCIÓN DE NEOSECURE CONTRA RANSOMWARE Y AMENAZAS AVANZADAS

El servicio examina todo el correo electrónico y la navegación capaz de detectar y bloquear tanto el Ransomware como otras amenazas desconocidas antes que ingresen a la red de la organización.

- Servidor se instala en el cliente y actúa como proxy.
- Monitoreo 7x24 en tiempo real a través del CDC de NeoSecure.
- Se conecta al sistema de Inteligencia de la Amenaza de NeoSecure.
- Inspección de tráfico HTTP, HTTPS y SMTP.
- Detecta y bloquea amenazas conocidas y desconocidas.
- Capacidades multi-sitio y multi-vínculo.
- Interfaz para reportería.



PROTECCIÓN NAVEGACIÓN Y CORREO



BENEFICIOS DE LA SOLUCIÓN

NEOSECURE
SABEMOS DE SEGURIDAD

- Rápida implementación.
- Full servicio: monitoreo + administración + soporte.
- 3 funcionalidades en un servicio: AV perimetral, Antimalware y Antispam.
- Alto nivel de protección, mucho mayor al antivirus.
- No solo protege contra Ransomware, detecta y bloquea la mayoría de las amenazas avanzadas.
- Sistema comunitario: Indicadores de compromiso se distribuyen cada minuto, protección inmediata ante detecciones dentro de la comunidad

¿Qué puedo hacer además de Tecnologia?

NEOSECURE
SABEMOS DE SEGURIDAD

- ✓ Mantener al día el sistema operativo y programas de tu computadora con las actualizaciones y parches de seguridad más recientes
- ✓ Instalar y mantener actualizado un software antimalware
- ✓ Sólo instalar software nuevo desde fuentes confiables
- ✓ Evitar utilizar una cuenta con privilegios de administrador del sistema para las tareas del día a día
- ✓ Habilitar en tu equipo un firewall (cortafuegos) personal
- ✓ Tener mucho cuidado con los dispositivos de almacenamiento externos (USB) que conectas a tu computadora
- ✓ Evitar la descarga de archivos desde redes peer-to-peer (P2P)
- ✓ No descargar archivos adjuntos de mensajes de correo-e sospechosos o redes sociales
- ✓ Y finalmente… un poco de **sentido común**

Como para reflexionar…

- "Pienso que los virus de computadora deberían contar como un tipo de vida. Creo que eso dice algo acerca de la naturaleza humana, en el sentido de que la única forma de vida que hemos logrado crear hasta ahora sea puramente destructiva. Hemos creado vida a nuestra propia imagen"

- —Stephen Hawking

NEOSECURE
SABEMOS DE SEGURIDAD

MUCHAS GRACIAS!!!

Presencia Local en:

Argentina
Chile
Colombia
Perú

Argentina
Av. Cerrito 1186, piso 7 - CABA
Fonos: (54 9 11) 4819-0100