Informe semestral de ciberseguridad 2016 de Cisco

Hermes Romero
Security Account Manager
Agosto de 2016

Las batallas asimétricas superan nuestra capacidad de respuesta

- Métodos innovadores
- Ataques persistentes
- Tácticas cambiantes
- Operaciones globales

Cantidad de vulnerabilidades en aumento

Infraestructura frágil

Dilema del cifrado

Proveedores de soluciones de defensa saturados

Una mirada a través de la telemetría global de Cisco

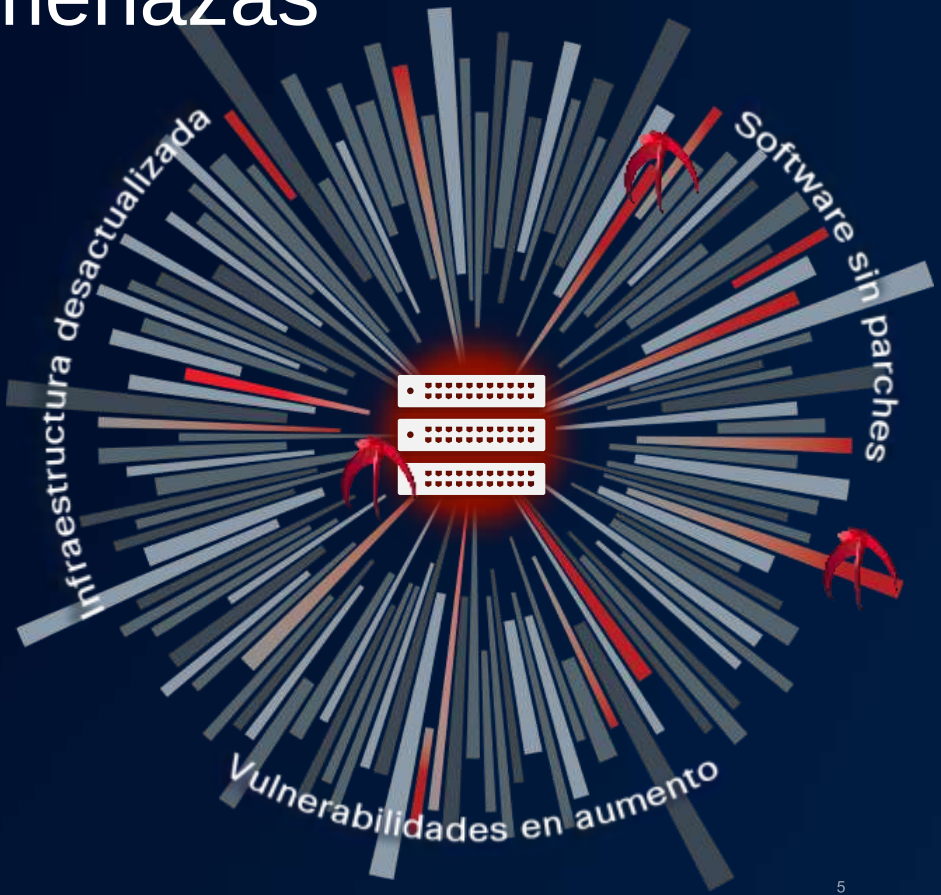
- 16 000 millones de solicitudes web por día
- 600 000 millones de correos electrónicos por día
- En total, se bloquean casi 20 000 millones de amenazas por día
  - Más de 1,5 millones de muestras únicas de malware diarias (17 por segundo)
- 18 500 millones de consultas de AMP
  - 214 000 consultas de AMP por segundo

Agenda

- Panorama actual de amenazas
- Aumento del tiempo para operar
- Reducción del tiempo para asegurar
- Perspectiva global

Panorama actual de amenazas

- Evolución del ransomware
- Avances en la inteligencia de técnicas maliciosas
- Prácticas cuestionables de la red
- Perspectiva geopolítica en conflicto



Ransomware

La técnica de cifrado permite la personalización por objetivo

Uso de bitcoins para realizar pagos anónimos

Los sistemas de marcado de archivos que ya se han cifrado

Plazos dobles para:
1.Aumento de costos
2.Eliminación de datos

Ransomware 2.0

Capacidad de autopropagación

- Aprovechamiento de una vulnerabilidad en un producto con alto grado de implementación
- Replicación a todas las unidades disponibles
- Infecciones en los archivos
- Actividad de fuerza bruta limitada
- Comando y control con capacidad de recuperación
- Uso de otras puertas traseras

Modular

- Propagación en almacenamiento masivo por medio de Autorun.Inf/USB
- Ataques a la infraestructura de autenticación
- Infecciones al comando y control/informes
- Limitador de velocidad
- Limitador de direcciones objetivo RFC 1918

Vulnerabilidades

Los atacantes ven las mejores oportunidades donde los proveedores de soluciones de defensa están saturados.

Oportunidades aprovechadas por los atacantes

Presión sobre los proveedores de soluciones de defensa

Al ritmo actual, en diciembre de 2016 las alertas acumulativas superarán las 10 000

Los atacantes apuntan al tráfico cifrado

CWE-287: Problemas de autenticación

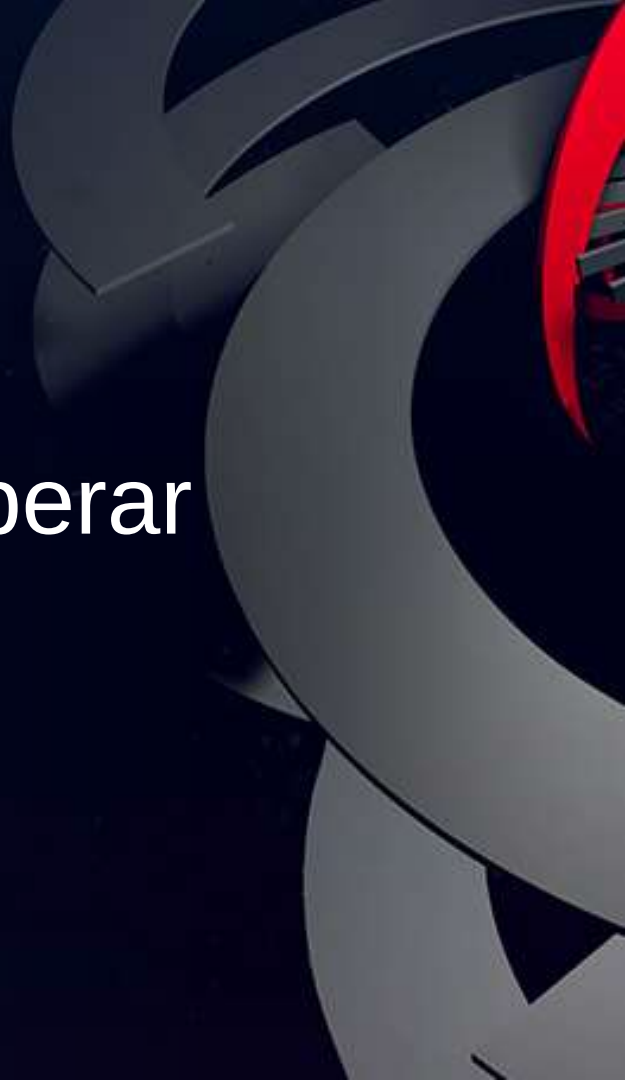
8 → 19

CWE-310: Problemas de criptografía

4 → 13

Aumento del tiempo para operar

Los atacantes aprovechan el tiempo sin límites para operar.



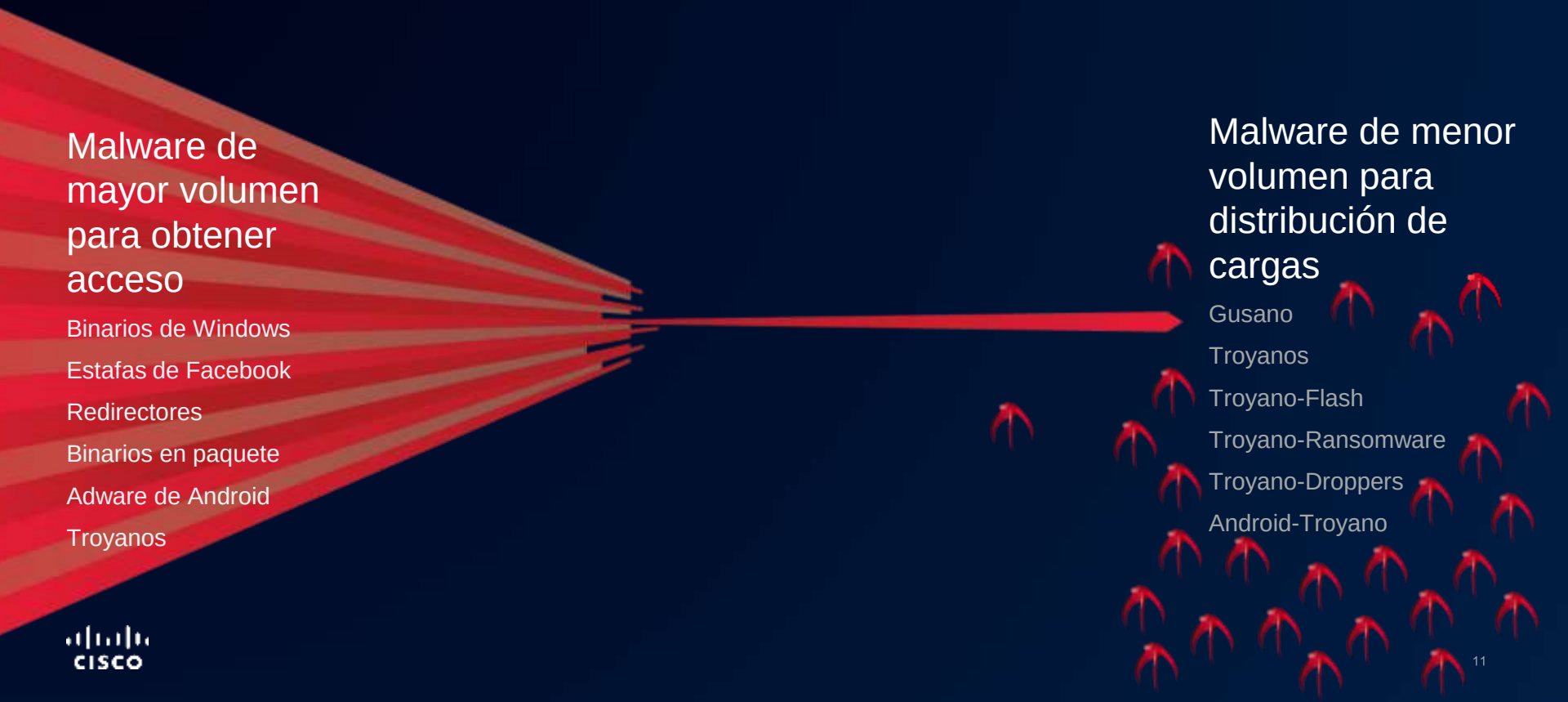
Vectores de ataque: servidores en el horizonte

Los atacantes expanden su enfoque de ataques sobre los clientes a ataques sobre los servidores

Las vulnerabilidades de Adobe Flash siguen siendo aprovechadas por los kits de ataque.

En abril, Cisco calculó que el 10% de todos los servidores Jboss en todo el mundo se vio amenazado.

Métodos de ataque: un espectro de oportunidades



Malware de mayor volumen para obtener acceso

- Binarios de Windows
- Estafas de Facebook
- Redirectores
- Binarios en paquete
- Adware de Android
- Troyanos

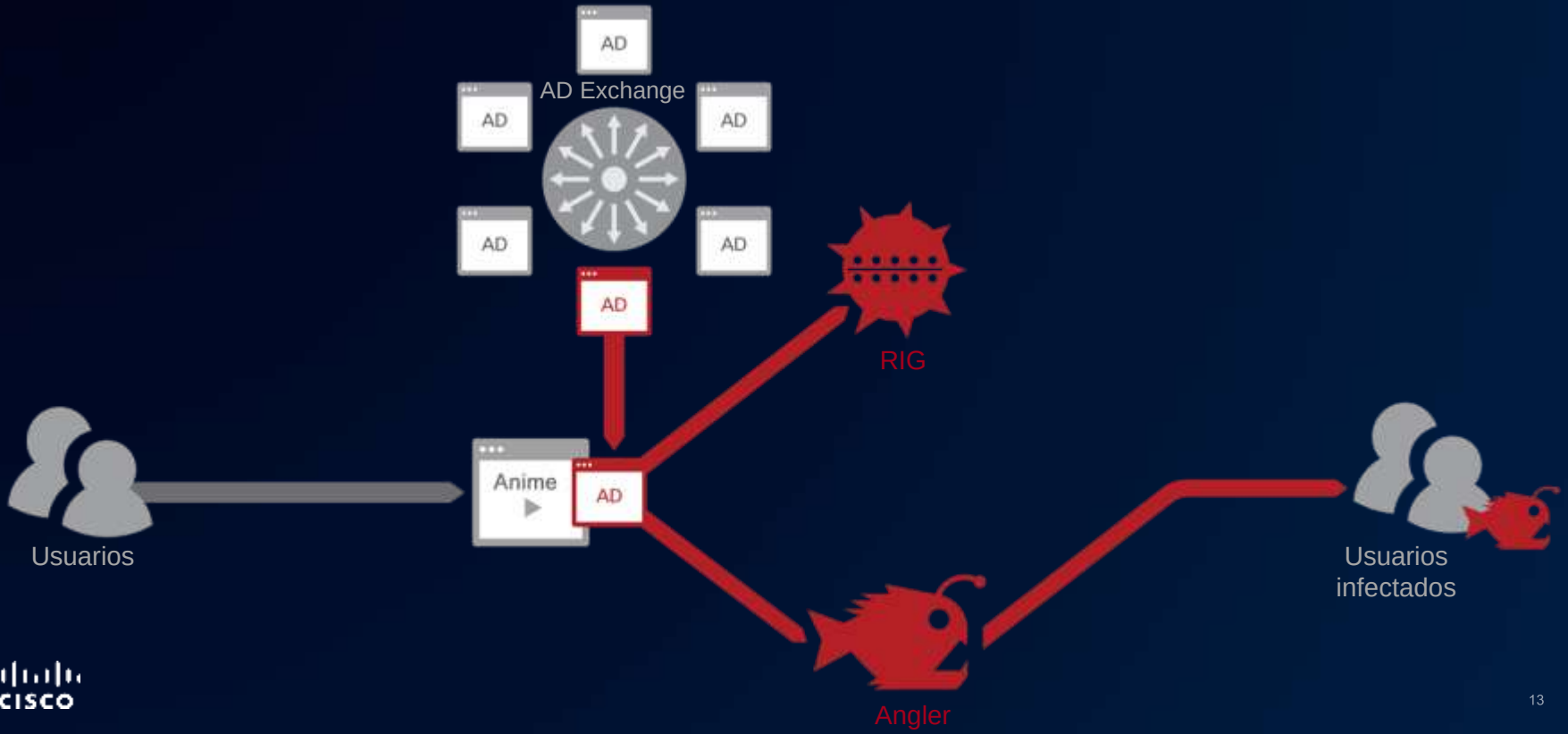
Malware de menor volumen para distribución de cargas

- Gusano
- Troyanos
- Troyano-Flash
- Troyano-Ransomware
- Troyano-Droppers
- Android-Troyano

Actividad de los kits de ataque: Adobe Flash y publicidad maliciosa

Las vulnerabilidades de Adobe Flash y Microsoft Silverlight son aprovechadas por la mayoría de los kits de ataque

Publicidad maliciosa como servicio: Distribuidores que expanden oportunidades



Uso malicioso de HTTPS:

HTTPS registró un aumento del 300% en la cantidad de inyectores por anuncios en los últimos 4 meses.

Mayor

300%

en 4 meses

La inyección de anuncios es el método que más contribuyó al aumento. Los atacantes están usando tráfico HTTPS para expandir su tiempo de operación.

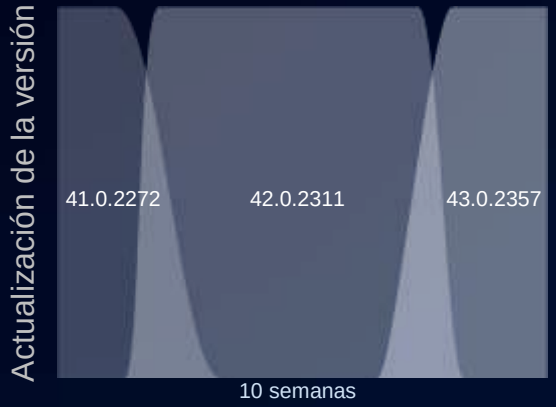
Reducción del tiempo para asegurar

Es la clave para debilitar el éxito de los atacantes.

Tiempo para corregir: las terminales vulnerables son objetivos tentadores

Navegadores

Chrome

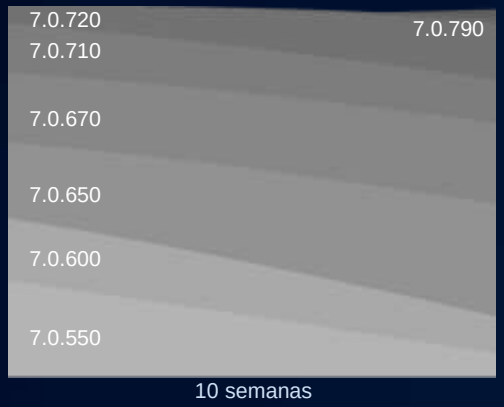


Patrón de picos

Actualizadas por los usuarios. La velocidad de la adopción es alta. Pequeñas superposiciones entre las versiones.

Aplicaciones

Java



Patrón de pendientes

Actualizadas por los usuarios y las organizaciones. Migraciones lentas con gran cantidad de versiones distintas en ejecución al mismo tiempo.

Software para empresas

Office

Patrón de cajas

Actualizado por las organizaciones. Cambios nulos o muy escasos para actualizar de una versión a otra. Quedan expuestas.

Infraestructura: la edificación de la economía digital sobre una infraestructura frágil

Una infraestructura frágil e insegura no podrá sustentar de manera segura la economía del futuro.

Dispositivos que están ejecutando vulnerabilidades conocidas durante un promedio de

5 años

Y el problema es sistémico

Cisco

5,64

años

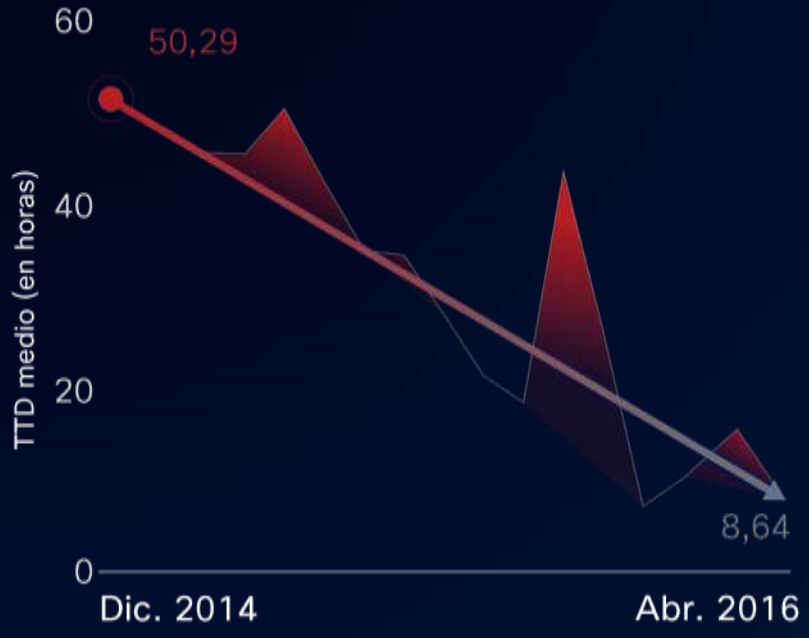
Apache/OpenSSH

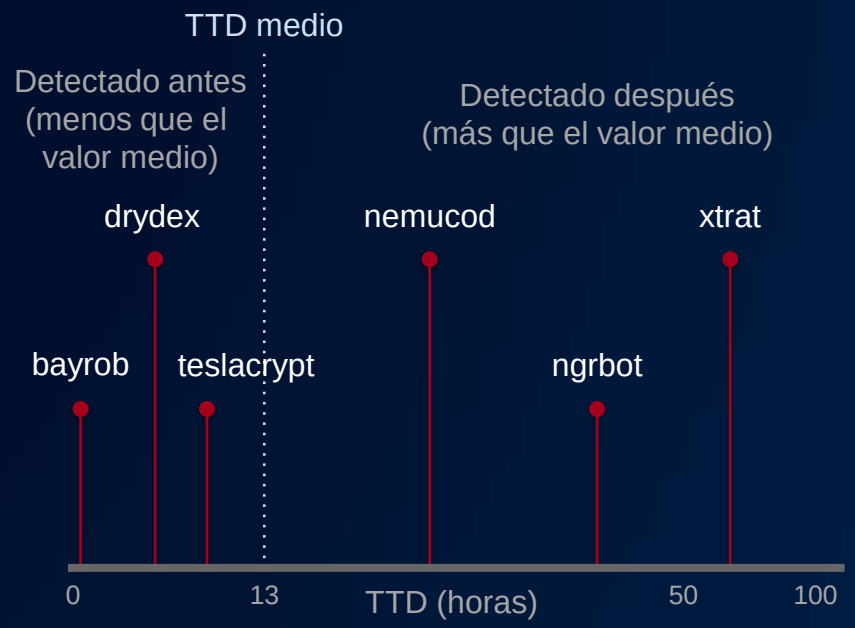
5,05

años

Tiempo de detección: mejorar la detección de los atacantes

Lograr una ventaja en la “carrera armamentista” continua.





Cifrado: borrar las huellas

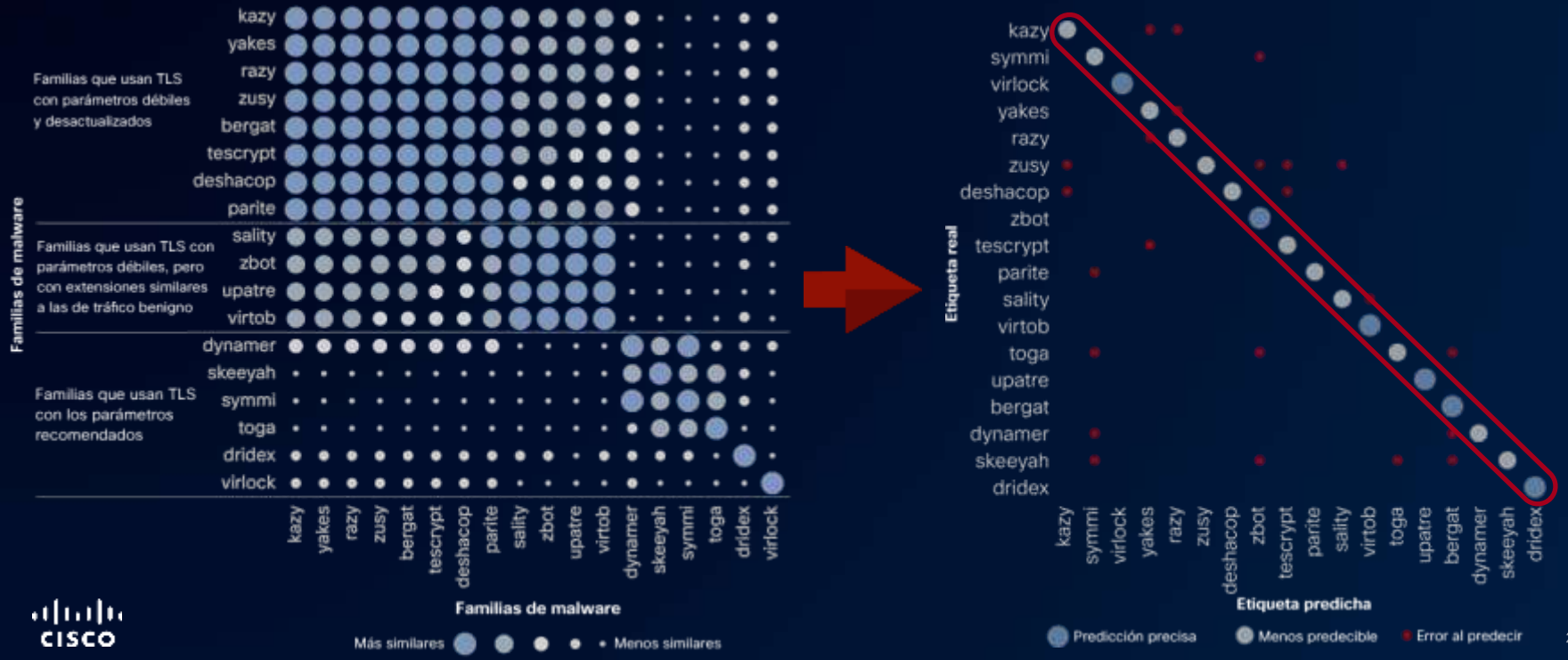
Los atacantes ocultan sus huellas en el tráfico cifrado para no ser detectados.

Aumento en el tráfico de malware por HTTP	Porcentaje de aumento	Porcentaje promedio HTTPS
Publicidad	+9,27%	34,06%
Motores de búsqueda y portales	+8,58%	64,27%
Chat y mensajería instantánea	+8,23%	96,83%

Categoría enero-abril	Porcentaje promedio HTTPS
Correo electrónico de la organización	97,88%
Chat y mensajería instantánea	96,83%
Correo electrónico web	96,31%
Almacenamiento y copia de respaldo en línea	95,70%
Telefonía por Internet	95,07%

Uso malicioso de TLS: detectar lo indetectable

Gracias al aprendizaje automático podemos detectar e identificar con exactitud malware con características similares.



Respuesta ante los incidentes: una vista desde el interior

Una infraestructura obsoleta crea vulnerabilidades que saturan a los proveedores de soluciones de defensa

Infraestructura obsoleta

Falta de procesos

Restricciones de presupuesto

Falta de parches

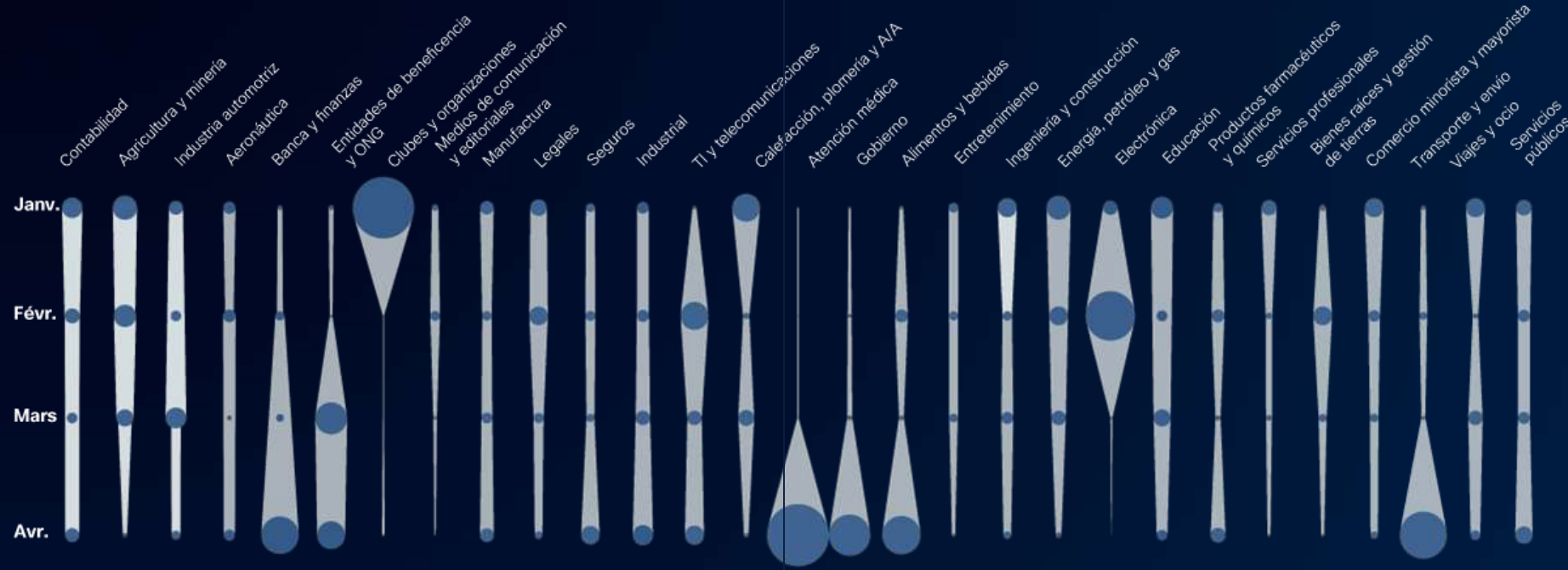
No utilizar las herramientas disponibles

Perspectiva global

Los atacantes operan en una escala global para maximizar las ganancias y para evitar ser detectados.

Riesgo vertical de hallazgo de malware

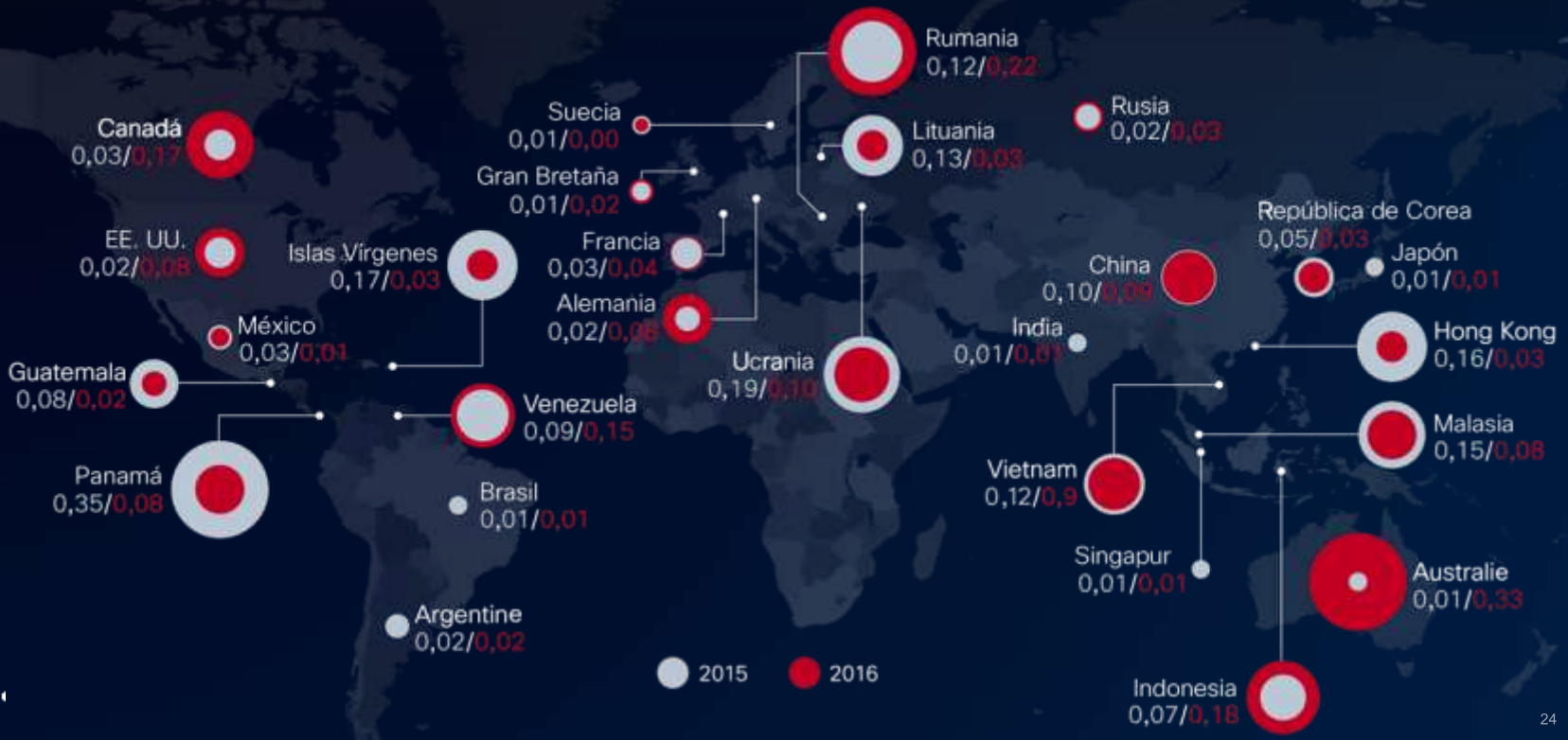
Ningún sector está seguro. Los atacantes se diversifican en varios sectores.



Índice de hallazgos en comparación con la línea de base

Bloqueos web por país

Los atacantes no respetan las fronteras y mudan su base de operaciones.



Las infraestructuras desactualizadas son un problema mundial

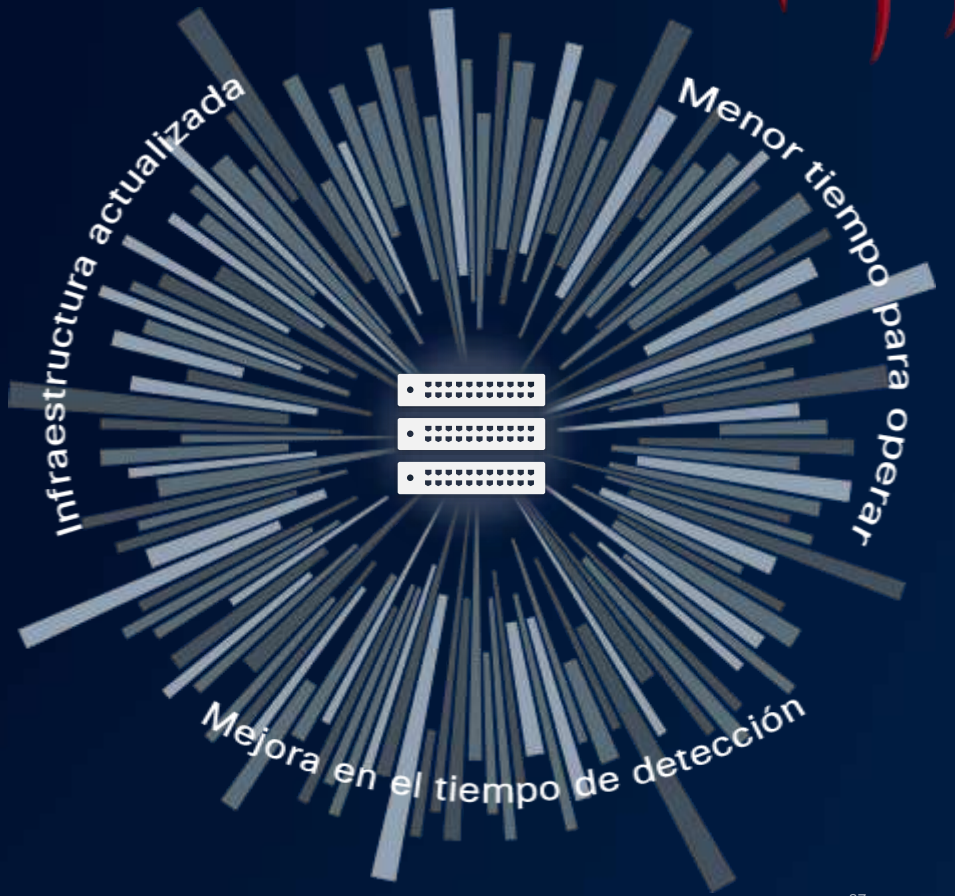
Geopolítica: las señales contradictorias limitan la seguridad

Los gobiernos pretenden imponer sus propias reglas, pero estas son contradictorias

El público también está preocupado por su privacidad

Conclusión

- Ransomware extendido y potente
- Copias de respaldo de datos periódicas
- Mejora en las prácticas de red
- Integrar las defensas
- Medir el tiempo de detección



Resumen

Aumento del tiempo para operar

Acelerar el tiempo para asegurar

Influencia global, impacto local