3 motivos

por los que necesita protección proactiva contra el malware

Veamos cómo proteger las brechas existentes en su pila de seguridad.

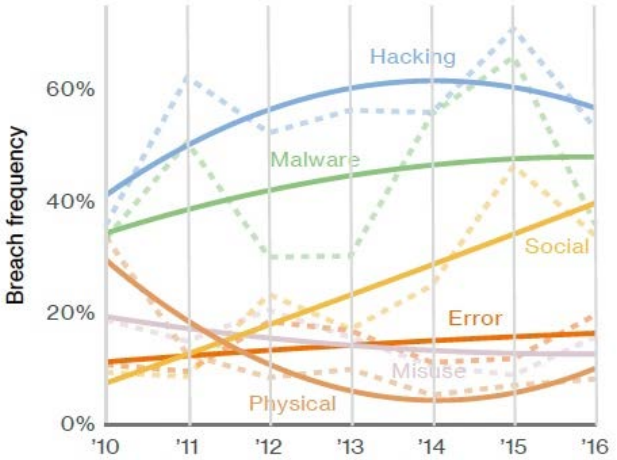
1 Los delitos informáticos siguen en auge

Las amenazas específicas continúan aumentando y evolucionando

La prevalencia, el volumen y la sofisticación de las amenazas específicas como el malware, el ransomware, la exfiltración de datos y el phishing están aumentando.

Los agentes maliciosos evolucionan y se adaptan con el fin de eludir los mecanismos de seguridad convencionales.

Como consecuencia, las organizaciones tienen dificultades para gestionar de manera efectiva esta avalancha.



Porcentaje de filtraciones por categoría de acción de amenazas en el tiempo[1]

La realidad de los delitos informáticos

En 2016, el número de registros de datos robados o perdidos resultó apabullante.

"Una empresa de la lista Fortune 1000 se hundirá a causa de una brecha informática".

Extracto del informe *Dynamics That Will Shape The Future In The Age Of The Customer*de Forrester

2

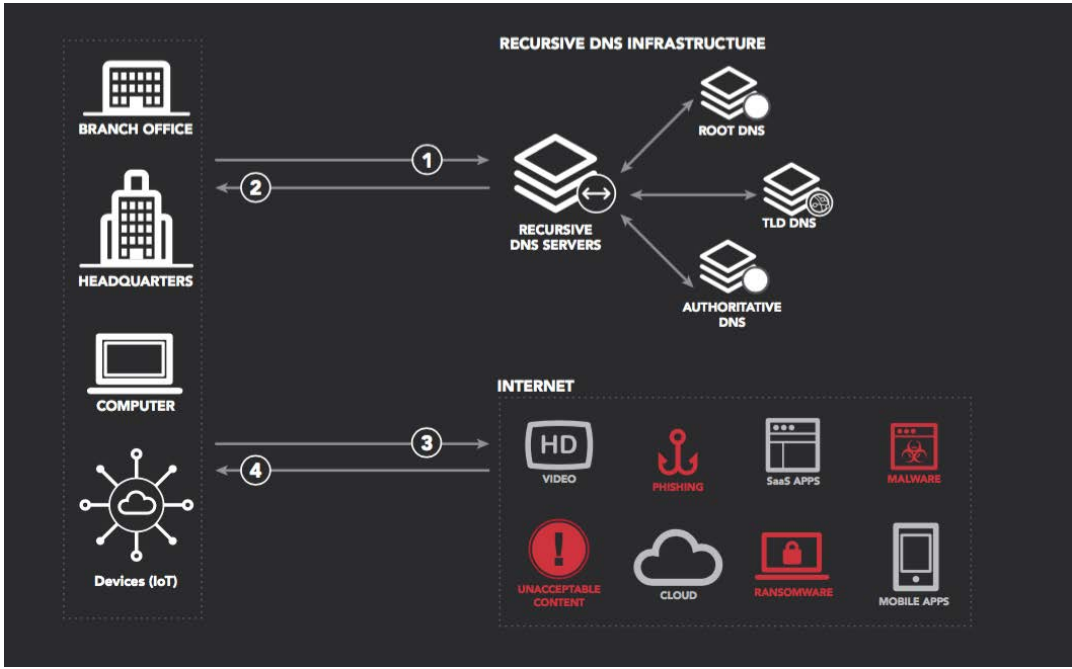
Los agentes maliciosos utilizan cada vez más el sistema de nombres de dominio (DNS) para eludir las defensas

¿Por qué se explota el DNS recursivo?

Casi todas las acciones que se realizan en Internet empiezan por una solicitud al sistema de nombres de dominio (DNS), que traduce los nombres de dominio a direcciones IP.

El protocolo DNS, por naturaleza, tiene carácter abierto y no filtrado.

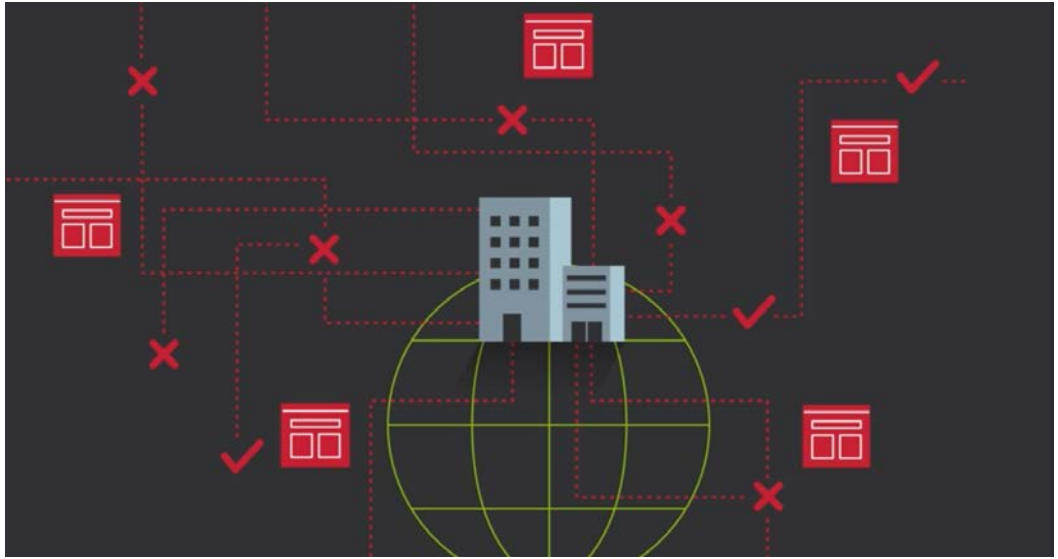
No incluye inteligencia y resolverá las solicitudes de un dominio correcto o malicioso.



¿Por qué se trata de un problema acuciante?

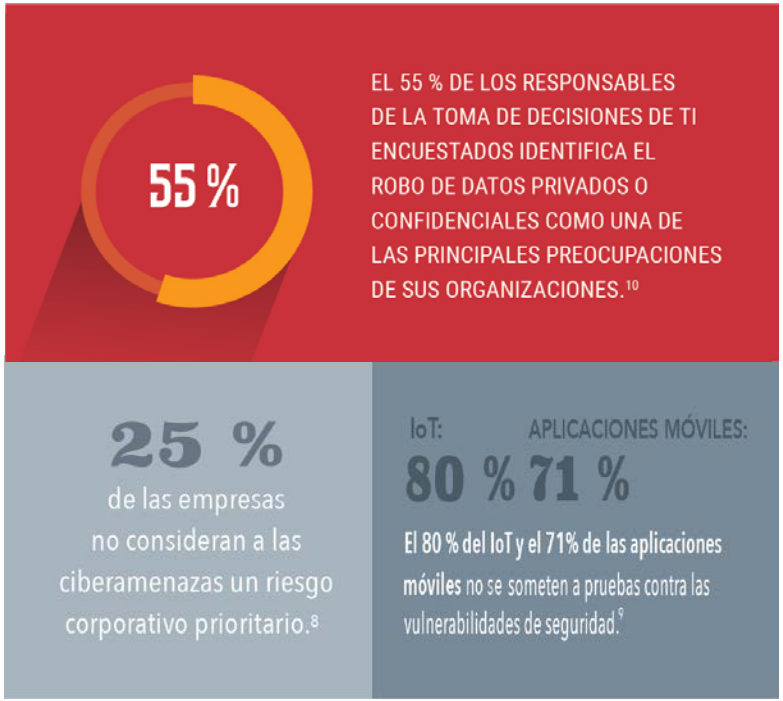
Los ciberdelincuentes se han dado cuenta de lo sencillo que resulta explotar esta brecha de seguridad, sin protección, para introducir malware en la red y extraer datos confidenciales.

El número de ataques que utilizan este vector está creciendo muy rápidamente.



¿Por qué están proliferando estos ataques?

A pesar de la reconocida vulnerabilidad de la infraestructura de DNS, la presión por proteger los datos de los clientes y la información confidencial, y el aumento del número de dispositivos conectados, son pocos los directores de informática y los equipos de TI que hacen de la protección de la infraestructura de DNS una prioridad.



3

Proteger este vector
de ataque
no es tarea fácil

Imagine de cuántas maneras puede acceder el malware a su red...

Basta con que un empleado o visitante de su red:

- Acceda a un enlace mediante un correo electrónico de phishing.
- Haga clic en un anuncio infectado por malware.
- Abra una URL afectada en una red social.
- Navegue a un sitio que utilice la táctica de typosquatting.
- Acceda a un dominio homográfico.
- Comparta contenido multimedia infectado almacenado en el equipo.
- Sucumba ante una táctica de ingeniería social.

Más de un 90 % del malware utiliza el sistema DNS para propagar la infección, tomar el control de su red y sustraer datos.[11]

El volumen de tráfico plantea un problema

Hay miles de dispositivos en una red: portátiles, teléfonos móviles, equipos de escritorio, tablets, impresoras, proyectores, Wi-Fi de invitados y dispositivos de IoT "inteligentes", entre otros.

Realizan cientos de miles de solicitudes de DNS a diario.

Este volumen puede ocultar actividades anómalas. Normalmente, hay demasiado tráfico bueno y muy poco tráfico perjudicial para justificar los recursos necesarios para supervisar los registros de DNS.

La visibilidad de las tendencias globales es vital

Por mucho que asigne recursos para supervisar y examinar al milímetro los registros de DNS, es muy poco probable que pueda detectar y mitigar una intrusión antes de que cause estragos.

Esto se debe a que las muestras de su empresa son demasiado pequeñas como para identificar las amenazas y tendencias que se dan en Internet.

Las herramientas y soluciones de seguridad puntuales no son suficientes.

Tienden a ser reactivas, inconsistentes y poco efectivas.

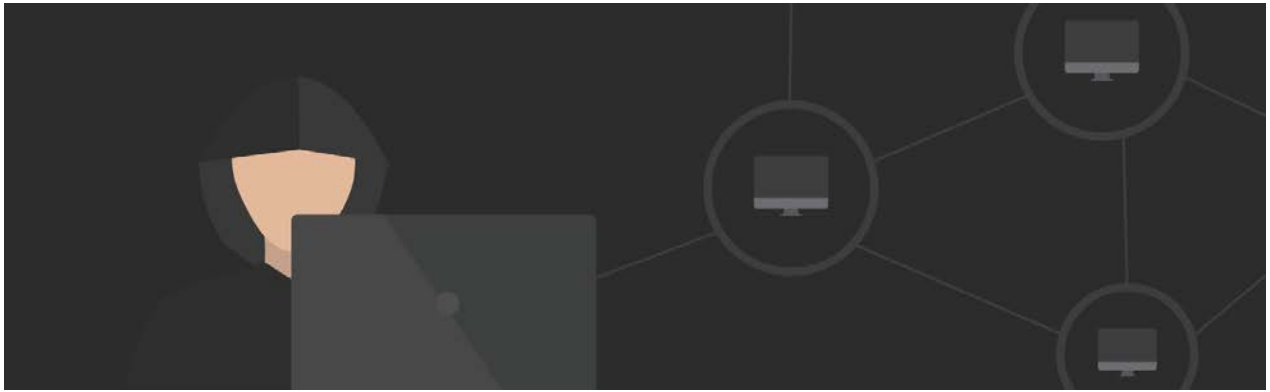
Las capas de defensa son críticas

Los productos como los firewalls, las puertas de enlace web seguras, los antivirus de punto final y los servicios de inteligencia ante amenazas dependen en gran medida de las listas negras, las actualizaciones manuales, los ajustes reactivos y la conformidad total por parte del usuario.

Su eficacia va normalmente en consonancia con la calidad de la base de datos del proveedor.

Es el juego de nunca acabar del gato y el ratón

Dada la tasa de evolución del malware y las medidas evasivas que utilizan los agentes maliciosos para evitar ser detectados (el uso de puertos y protocolos que no son estándar, los algoritmos de generación de dominios, el flat flux o la exfiltración de DNS, por citar algunos), la mayoría de los mecanismos de defensa carecen de agilidad para adaptarse a esta gran variedad de amenazas, por lo que quedan rápidamente obsoletos.



Hay una forma mejor

Akamai
Enterprise Threat Protector

Sources

1. Verizon 2017 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

2. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016

3. https://www.av-test.org/en/statistics/malware/

4. ISACA 2015 Global Cybersecurity Status Report, http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

5. Cybersecurity Ventures, 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

6. Ponemon Institute, The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN

7. www.cyberark.com/noteworthy-cyber-security-statistics/

8. MMC Cyber Handbook 2016, http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf

9. Arxan, 2017 Study on Mobile and Internet of Things Application Security, https://www.arxan.com/2017-Ponemon-Mobile-Iot-Study

10. www.securityweek.com/nearly-50-percent-organizations-hit-dns-attack-last-12-months-survey

11. Cisco 2016 Annual Security Report