HOJA DE DATOS

Infoblox DNS Infrastructure Protection

Minimice las interrupciones del negocio causadas por ataques basados en el DNS

DESAFÍO: INTERRUPCIONES DEL SERVICIO

El DNS es la red troncal oculta de las operaciones digitales. Cada sitio web, aplicación y usuario depende de él para mantener la conexión. Si los servicios del DNS se interrumpen, pueden provocar la pérdida de millones de ingresos y de confianza de los clientes. Es especialmente cierto para los servicios del DNS externos, que mantienen en línea los sitios web, correos electrónicos y otras aplicaciones públicas. Al mismo tiempo, los servidores del DNS externos deben estar expuestos al internet público, lo que los convierte en blanco constante de ciberataques, como:

- **Ataques DDoS**, que saturan los servidores con tráfico masivo de múltiples fuentes y provocan que se bloqueen los sitios web.
- **Secuestro de DNS**, donde los atacantes manipulan los registros del DNS para redirigir el tráfico a un sitio malicioso
- **Envenenamiento de la caché**, donde los atacantes inyectan datos maliciosos o no válidos en la caché de una red, bien para servir contenido malicioso, bien para redirigir a los usuarios a sitios maliciosos
- **Exploits de NXDOMAIN**, que inundan los servidores del DNS con consultas de dominios inexistentes y provocan interrupciones del servicio

Además, los registros del DNS autoritativos externos se distribuyen a través de servidores de internet en todo el mundo. Por tanto, si un atacante logra modificarlos, pueden tardarse horas —o incluso días— en corregir todos los datos incorrectos, durante los cuales sus sitios web y otras aplicaciones en línea pueden quedar totalmente inaccesibles.

Infoblox DNS Infrastructure Protection (antes Advanced DNS Protection) detiene los ataques DDoS y otros dirigidos a los servidores del DNS. Este complemento de software NIOS mantiene en funcionamiento sus aplicaciones críticas conectadas a internet, incluso cuando la infraestructura del DNS está bajo un fuerte ataque.

SOLUCIÓN: PROTEJA SU EMPRESA DE LAS INTERRUPCIONES CAUSADAS POR ATAQUES BASADOS EN DNS

DNS Infrastructure Protection detecta y bloquea continuamente una amplia gama de amenazas dirigidas contra servicios del DNS críticos y evita que los atacantes manipulen la integridad del DNS. Bloquea tanto los ataques volumétricos, p. ej., DDoS y NXDOMAIN, como exploits no volumétricos, como el secuestro del DNS, el envenenamiento de la caché y otras amenazas dirigidas contra servidores del DNS externos e internos.

A diferencia de los enfoques únicos que pueden bloquear el tráfico legítimo, DNS Infrastructure Protection utiliza inteligencia continuamente actualizada para identificar amenazas genuinas. Mientras tanto, mantiene el flujo del tráfico real para que su empresa siga en funcionamiento, incluso cuando la infraestructura de DNS está bajo ataque.

CARACTERÍSTICAS PRINCIPALES

Reduzca las interrupciones empresariales: Infoblox DNS Infrastructure Protection supervisa, detecta y detiene continuamente todo tipo de ataques al DNS —volumétricos o no, como las vulnerabilidades y el secuestro del DNS—, mientras responde a consultas legítimas. También mantiene la integridad del DNS, que los ataques de secuestro del DNS pueden poner en riesgo. Infoblox contribuye a garantizar que los sitios web y las aplicaciones de misión crítica permanezcan en línea y disponibles.

Adáptese a las amenazas en continua evolución: Infoblox DNS Infrastructure Protection utiliza la tecnología Infoblox Threat Adapt™ para actualizar automáticamente la protección contra amenazas nuevas y en evolución a medida que surgen. Threat Adapt aplica análisis e investigaciones independientes a las técnicas de ataque en constante evolución para incluir lo que los especialistas en amenazas de Infoblox observan en las redes de los clientes y actualizar la protección. Adapta automáticamente la protección para reflejar los cambios en la configuración del DNS.

Obtenga visibilidad con un panel único de control: DNS

HABILITAR EL DNS CIFRADO (DoH Y DoT)

La comunicación entre el solucionador del cliente DNS (stub) y el servidor del DNS local (solucionador recursivo) no está cifrada. Las comunicaciones no cifradas están sujetas a espionaje, interceptación y exfiltración de datos, también conocido como el problema de seguridad de «último kilómetro» del DNS. Como respuesta, el sector puso en marcha DNS a través de TLS (DoT) y DNS a través de HTTPS (DoH) para proporcionar privacidad y cifrado entre clientes del DNS y servidores del DNS de internet externo. Implementar el cifrado a través del solucionador de DNS en su red le permite mantener el control de la experiencia de red de su usuario, a la vez que proporciona seguridad y filtrado de contenido según sus requisitos de política de seguridad. DNS Infrastructure Protection optimiza el cifrado del DNS para que pueda eliminar las conexiones cifradas de DNS sobre TLS y DoH en su red.

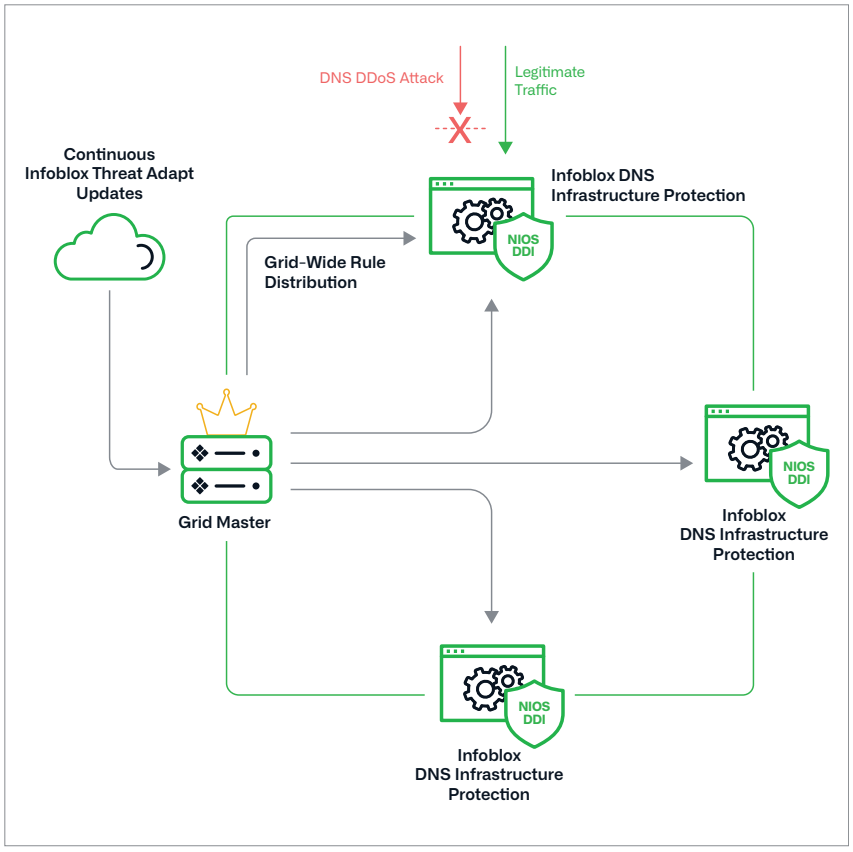

Figura 1. Infoblox DNS Infrastructure Protection proporciona una defensa única contra los ataques basados en el DNS

Infrastructure Protection proporciona visibilidad generalizada y centralizada de los patrones de ataque al DNS, tanto en tiempo real como histórico. Los equipos de NetOps y SecOps pueden rastrear las fuentes de amenazas y ver los puntos de ataque en todo el entorno para acelerar la mitigación y mejorar continuamente las defensas.

Disponible en plataformas físicas, virtuales y en la nube: Con Infoblox, puede implementar la solución como complemento de software por suscripción en dispositivos Trinzic virtuales y físicos, lo que permite ejecutar los servicios en un modelo común y admite entornos in situ y en la nube privada y pública.

LO QUE DICEN NUESTROS CLIENTES

"Los incidentes de servicio de los ataques DDoS se han reducido a la mitad y las quejas de los clientes sobre los largos tiempos de carga de página se han reducido significativamente".

Vicepresidente de Atención al Cliente,
Proveedor de servicios de gran tamaño

"Llevo cuatro años utilizando Infoblox para el servicio de DNS, DHCP y la gestión de direcciones IP. Es un producto estupendo. Hemos desplazado otros recursos porque funciona muy bien. Nuestra huella global está gestionada por 1,5 ETC, y son 65 dispositivos".

Gestor de Infraestructura Global,
Adobe

TABLA 1:
RESUMEN DE LOS TIPOS DE ATAQUE DE LOS QUE DEFIENDE DNS INFRASTRUCTURE PROTECTION

Nombre del ataque	Tipo	Cómo funciona
Reflexión de DNS/ ataques DDoS	Volumétrico	Uso de servidores DNS de terceros (resolutores abiertos) para propagar un ataque DoS o DDoS
Amplificación de DNS	Volumétrico	Utilice una consulta especialmente diseñada para crear una respuesta amplificada para inundar a la víctima con tráfico
Inundaciones TCP/ UDP/ICMP	Volumétrico	Denegación de servicio en la capa 3 mediante la interrupción de una red o un servicio inundándolo con grandes cantidades de tráfico
NXDOMAIN	Volumétrico	Inundación del servidor DNS con solicitudes de dominios inexistentes, lo que provoca saturación de caché y menor tiempo de respuesta
Subdominio aleatorio (ataques de goteo lento), ataques de bloqueo de dominio, ataques de dominio fantasma	Sigilo de bajo volumen	Inundación del servidor DNS con solicitudes de dominios fantasma o mal comportamiento que se configuran como parte del ataque, lo que provoca agotamiento de recursos, saturación de caché, límite de consultas salientes y rendimiento degradado
Exploits basados en DNS	Exploits	Ataques que aprovechan las vulnerabilidades del software DNS
Envenenamiento de caché de DNS	Exploits	Corrupción de los datos de la caché de DNS con una dirección no autorizada
Anomalías de protocolo	Exploits	Causa que el servidor se bloquee enviando paquetes y consultas mal formados
Reconocimiento	Exploits	Intentos de los hackers para obtener información sobre el entorno de red antes de lanzar un ataque DDoS grande u otro tipo de ataque
Secuestro de DNS	Exploits	Ataques que anulan la información de registro de dominio para apuntar a un servidor DNS no fiable
Exfiltración de datos (mediante túneles conocidos)	Exploits	El ataque consiste en tunelizar otro protocolo a través del puerto DNS 53, lo que está permitido si el cortafuegos está configurado para transportar tráfico no DNS, con fines de exfiltración de datos.

OPCIONES DEL DISPOSITIVO

DNS Infrastructure Protection: Disponible en plataformas físicas y virtuales

Infoblox DNS Infrastructure Protection defiende contra un amplio espectro de ataques DDoS contra el DNS, garantizando un servicio ininterrumpido a su organización. Es un complemento de software por suscripción compatible con una amplia variedad de dispositivos de hardware y software Trinzic, que le permite salvaguardar la integridad del DNS y evitar ataques DDoS tanto externos como internos contra el DNS que podrían interrumpir sus operaciones empresariales, en entornos locales y de nube privada y pública.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20251007v3