HOJA DE DATOS

Infoblox Advanced DNS Protection

Minimice las interrupciones del negocio causadas por ataques basados en DNS

DESAFÍO: INTERRUPCIONES DEL SERVICIO

El DNS es fundamental para todas las organizaciones porque proporciona la conectividad de red de misión crítica necesaria para administrar una empresa. Si su servidor DNS externo deja de funcionar, toda su red se desconecta de Internet. La interrupción del DNS interfiere o cierra sus aplicaciones de TI críticas, como correo electrónico, sitios web, VoIP y software como servicio (SaaS). Dado que un gran número de empleados empezó a trabajar a distancia en 2020, hubo un gran aumento en los ataques DDoS. El DNS sigue siendo un servicio objetivo líder para DDoS, ya que es fundamental mantener un negocio en línea. Además de la pérdida de confianza de los clientes, los ataques DDoS exitosos pueden costar a una organización cientos de miles de dólares en ingresos perdidos al mes.

Infoblox ofrece la gama de protección más amplia del mercado para proteger sus servicios DNS vitales de los ataques, garantizando la disponibilidad de cinco nueves de la que depende su organización. Proporciona visibilidad centralizada sobre quién está utilizando la red, en qué dispositivos se encuentra y detalles sobre el ataque para garantizar una respuesta rápida.

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

Con Infoblox Advanced DNS Protection (ADP), su negocio siempre está en funcionamiento, incluso bajo un ataque basado en DNS. Infoblox bloquea la gama más amplia de ataques, como ataques volumétricos, NXDOMAIN, exploits y secuestros de DNS. A diferencia de los enfoques que se basan en el sobreaprovisionamiento de la infraestructura o en la simple limitación de la velocidad de respuesta, la protección avanzada de DNS detecta de forma inteligente y mitiga los ataques DNS mientras responde solo a consultas legítimas mediante el uso de inteligencia sobre amenazas constantemente actualizada, sin necesidad de implementar parches de seguridad. Con Infoblox, puede llevar la fiabilidad de la red al siguiente nivel garantizando que su infraestructura crítica, y su negocio, sigan funcionando en todo momento.

CARACTERÍSTICAS PRINCIPALES

Reduzca las interrupciones del negocio: La protección avanzada de DNS (ADP) de Infoblox supervisa, detecta y detiene continuamente todo tipo de ataques de DNS, incluidos los ataques no volumétricos, como los exploits de DNS y el secuestro de DNS, mientras responde a las consultas legítimas. También mantiene la integridad del DNS, que los ataques de secuestro del DNS pueden poner en peligro. Infoblox proporciona una base sólida para la seguridad, lo que permite una disponibilidad de cinco nueve para su red.

Adáptese a las amenazas evolutivas: Infoblox ADP utiliza la tecnología Infoblox Threat Adapt fondo para actualizar automáticamente la protección contra amenazas nuevas y en evolución. Threat Adapt aplica análisis e investigación independientes a las técnicas de ataque en evolución, incluyendo lo que los especialistas en amenazas Infoblox han visto en las redes para actualizar la protección. Adapta automáticamente la protección para reflejar los cambios en la configuración de DNS.

HABILITE DOT Y DOH

La comunicación entre el solucionador del cliente DNS (stub) y el servidor 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 "última milla" del DNS. Como respuesta, el sector inició DNS a través de TLS (DoT) y DNS a través de HTTPS (DoH) para proporcionar privacidad y cifrado entre clientes DNS y servidores DNS de Internet externos. 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. ADP optimiza el cifrado DNS para nuestro motor de paquetes de alto rendimiento llamado Fast Path para que pueda terminar las conexiones DoT y DoH cifradas en su red.

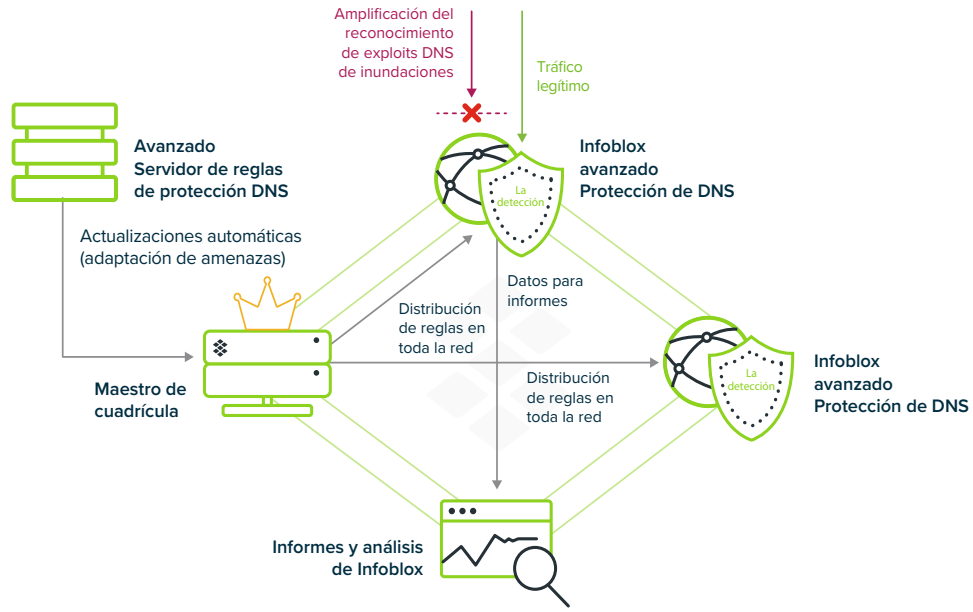

Figura 1: La protección avanzada de DNS de Infoblox proporciona una defensa única contra los ataques basados en DNS.

CARACTERÍSTICAS PRINCIPALES (CONT'D.)

Obtenga visibilidad en un solo panel de vidrio:
Con Infoblox, su organización puede ver fácilmente los ataques DNS anteriores o actuales y mejorar la eficiencia operativa gracias a nuestra rápida corrección de amenazas. Infoblox Advanced DNS Protection también proporciona una visión única de los puntos de ataque en toda la red y las fuentes de ataque, proporcionando la inteligencia necesaria para la gestión de amenazas. Está integrado con nuestra solución DNS.

Implemente de forma flexible:
Con Infoblox, tiene la opción de implementar como complemento de suscripción en dispositivos Trinzic virtuales y físicos.

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"

—VP de atención al cliente, gran proveedor de servicios

"Llevo cuatro años utilizando Infoblox para el servicio de DNS, DHCP y gestión de direcciones IP. Es un producto estupendo. Hemos desplazado otros recursos porque funciona muy bien. Nuestra huella global está gestionada por 1.5 FTE, lo que equivale a 65 dispositivos".

—Gestor de Infraestructura Global, Adobe

TABLA 1:
RESUMEN DE LOS TIPOS DE ATAQUE CONTRA LOS QUE SE DEFIENDE LA PROTECCIÓN DNS AVANZADA (ADP)

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
TCP/UDP/ICMP inundaciones	Volumétrico	Denegación de servicio en la capa 3 al dejar caer una red o un servicio al inundarla 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

Software ADP: disponible en plataformas físicas y virtuales

Software ADP es un complemento de software para dispositivos Trinzic TE-815/825/1415/1425/2215/2225/4015/4025.

TE - 4015/4025

TE - 1415/1425

TE - 2215/2225

TE - 815/TE 825

Empezar con una evaluación

60 días de evaluación gratuita del software ADP con licencia temporal para clientes estará disponible a través de sus administradores de cuentas/SE.

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com