HOJA DE DATOS

Advanced DNS Protection de Infoblox para proveedores de servicios

DESAFÍO: INTERRUPCIONES DEL SERVICIO

Los CSP, los operadores móviles y los proveedores de nube dependen en gran medida del DNS, en parte como componente esencial de la conectividad y en parte como servicio que ofrecen a sus clientes, ya sea de forma implícita o explícita. Los CSP deben proteger este activo vital, tanto por su reputación como por sus clientes, que dependen de una conectividad a internet estable y siempre activa. Si los servidores del DNS se caen, sus suscriptores se quedan sin conexión a internet. La interrupción del DNS interfiere o cierra sus aplicaciones de TI críticas, como correo electrónico, sitios web, VoIP y software como servicio (SaaS).

Según los principales informes de seguridad, el DNS es el segundo servicio más atacado en la capa de aplicaciones, con un 72% de empresas afectadas en 2018. Neustar estima que el coste derivado de un ataque distribuido de denegación de servicio (DDoS) llevado a cabo a través del DNS es superior a 220.000 dólares por hora, sin incluir la pérdida de suscriptores y los daños a las marcas. Los atacantes buscan los eslabones más débiles —vectores de ataque— de su red, y el protocolo del DNS es fácil de explotar con ataques DDoS o secuestro del DNS; estos ataques comprometen la integridad del DNS.

INFINIDAD DE DEFENSAS, PERO PILOTAJE A CIEGAS

Muchas redes de CSP adoptan una serie de herramientas, entre las que se incluyen sistemas de prevención de intrusiones (IPS), cortafuegos y sistemas de equilibrio de carga, muy eficaces para proteger distintos aspectos de la infraestructura del proveedor. Sin embargo, estas herramientas son ineficaces cuando se aplican al DNS, ya que no están integradas con los servidores del DNS y no tienen conocimiento ni visibilidad del DNS.

Pese a implementar estas herramientas de forma extensiva, muchos CSP siguen quejándose de que el primer conocimiento que tienen de los ataques al DNS es cuando los clientes les informan de un rendimiento lento de la red u otras degradaciones. La mayoría de las organizaciones tienen poca o ninguna alerta temprana de los ataques a los sistemas del DNS. Muchos equipos de operaciones incluso recurren al análisis manual de los datos de los registros del servidor del DNS para determinar si los niveles de tráfico han aumentado y si los servidores se han visto sometidos a estrés o comprometidos.

ÁREAS CRÍTICAS QUE REQUIEREN PROTECCIÓN

Dos áreas críticas que requieren protección dentro de la red del proveedor son los servidores del DNS autoritativos y los servidores de caché del DNS. Los servidores del DNS autoritativos en diversas ubicaciones dentro de la red del proveedor responden a las consultas al DNS y a las solicitudes de conectividad de su base de suscriptores. Los servidores del DNS autoritativos permiten la presencia en la web, las funciones de comercio electrónico y la ubicación de múltiples componentes de red para la conectividad IP móvil, especialmente la itinerancia y la ubicación de la pasarela en redes LTE y 5G. Para garantizar una experiencia de Internet fluida a los suscriptores, la capa de caché del DNS es clave para establecer una respuesta rápida a las consultas al DNS. Por lo tanto, es fundamental almacenar en caché las respuestas a las

VENTAJAS Y CARACTERÍSTICAS

Reduzca las interrupciones del negocio:
Advanced DNS Protection (ADP) de Infoblox supervisa, detecta y detiene continuamente todo tipo de ataques al DNS, incluidos los ataques no volumétricos, como los exploits y el secuestro del 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 del 99,999% para su red.

Adáptese a las amenazas en continua evolución:
ADP de Infoblox 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.

consultas de los sitios web y otras URL de acceso frecuente a fin de lograr tiempos de respuesta aceptables.

UNA NUEVA VARIABLE: DNS CIFRADO

Han surgido nuevos estándares de DNS cifrado que, aunque protegen la privacidad de las consultas al DNS y la integridad de las respuestas, pueden hacer que los CSP pierdan parte del control necesario para gestionar el uso del DNS en sus redes, salvo que proporcionen sus propios servicios de DNS cifrado. El DNS sobre TLS (seguridad de la capa de transporte) —DoT— y el DNS sobre HTTPS —DoH— funcionan cifrando la comunicación del DNS entre el resolutor stub del sistema operativo o una aplicación local y su resolutor del DNS recursivo. Ambas tecnologías garantizan la privacidad y la autenticación de los datos mediante el cifrado de las comunicaciones entre los clientes y los servidores del DNS. Sin embargo, al hacerlo, muchas soluciones se modifican para apuntar a resolutores del DNS externos, lo que permite a los dispositivos cliente acceder a servicios del DNS que quedan fuera del control del proveedor y exponen al suscriptor a posibles riesgos de seguridad y experiencias negativas para el cliente. Los proveedores deben tomar medidas ahora para reducir los riesgos que plantean estas tecnologías. La implementación del cifrado a través del resolutor del DNS en su red le permite mantener el control de la experiencia de red de sus suscriptores. Así permitirá a los proveedores seguir proporcionando seguridad, filtrado de contenidos y otros servicios críticos en la red.

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

Con Advanced DNS Protection (ADP) de Infoblox, su negocio siempre está en funcionamiento, incluso bajo un ataque basado en el DNS. Infoblox bloquea la gama más amplia de ataques, como los ataques volumétricos, los ataques NXDOMAIN, los exploits y el secuestro del DNS. A diferencia de los enfoques que se basan en el sobreaprovisionamiento de la infraestructura o en la simple limitación de la tasa de respuesta, ADP detecta y mitiga de forma inteligente los ataques al DNS, al tiempo que responde únicamente a las 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 asegurando que su infraestructura de red crítica, y su empresa, sigan operativos en todo momento.

ADMITE LOS ESTÁNDARES DE DNS CIFRADOS

Network Identity Operating System (NIOS) de Infoblox es el sistema operativo de identidad de red que sustenta los servicios de red básicos de Infoblox y garantiza el funcionamiento continuo de la infraestructura de red. Encrypted DNS de Infoblox para proveedores de servicios es una función de NIOS que proporciona un cifrado eficiente, al tiempo que ofrece el mejor DNS de su clase y servicios de valor añadido para los suscriptores de Infoblox. Encrypted DNS, compatible con DoT y DoH, ofrece un enfoque único para cifrar su tráfico del DNS. A diferencia de los métodos que dependen de balanceadores de carga o del sobreaprovisionamiento, Encrypted DNS de Infoblox se ejecuta como un único servicio para todas sus demandas de DNS. Encrypted DNS de Infoblox, disponible a través de instancias virtualizadas de ADP, permite a Infoblox cifrar las comunicaciones del DNS de último kilómetro entre sus endpoints y los servidores del DNS, independientemente del protocolo que admita el endpoint. Admite esta capacidad a la vez que resuelve los problemas de rendimiento asociados con la sobrecarga adicional derivada de las comunicaciones del DNS cifrado. Desde el mismo servicio, permitimos a los CSP adaptarse al DNS cifrado con una latencia de microsegundos cuando la conexión ya está establecida, mientras se ejecutan todas las demás funciones del DNS.

VENTAJAS Y CARACTERÍSTICAS

Obtenga visibilidad desde un panel único: con Infoblox, los proveedores de servicios de comunicaciones (CSP) pueden ver fácilmente ataques al DNS anteriores o actuales y mejorar la eficiencia operativa gracias a nuestra rápida corrección de amenazas. Advanced DNS Protection de Infoblox también proporciona una vista única de los vectores de ataque en toda la red y de sus fuentes, lo que ofrece la inteligencia necesaria para la gestión de amenazas. Está integrado con nuestra solución del DNS.

Implemente de manera flexible: los operadores pueden llevar a cabo implementaciones en los dispositivos virtuales Trinzic Flex de Infoblox, que permiten a los operadores añadir capacidades específicas en toda su infraestructura de Infoblox mientras aprovechan las capacidades de escalado elástico y precios basados en la capacidad, específicos del proveedor de servicios.

Reduzca sus costes: el software ADP de Infoblox aprovecha el hardware existente, lo que significa que los clientes solo tienen que actualizar el software que se ejecuta, con los consiguientes costes mínimos para la actualización incremental.

OPCIONES DE IMPLEMENTACIÓN FLEXIBLES

Advanced DNS Protection de Infoblox está diseñado para entornos de CSP que requieren implementaciones periféricas escalables. Está disponible en múltiples opciones de grado operador, incluidas soluciones virtualizadas de funciones de red (VNF) orquestadas y nativas de la nube.

- Trinzic Flex de Infoblox: plataforma virtual escalable basada en los recursos asignados a la máquina virtual. El sistema operativo de identidad de red (NIOS) de Infoblox detecta automáticamente la capacidad de la máquina virtual y la escala a la plataforma adecuada. Además, los dispositivos Trinzic Flex están cubiertos por el Programa de Acuerdo de Licencia de Proveedor de Servicios (SPLA).
- Disponible en plataformas físicas y virtuales: El software ADP es un complemento de suscripción de software para los dispositivos Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025.

Nombre del ataque	Tipo	Cómo funciona
Reflexión del DNS/ ataques DDoS	Volumétrico	Uso de servidores DNS de terceros (resolutores abiertos) para propagar un ataque DoS o DDoS
Amplificación del 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 del 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 del 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 el DNS	Exploits	Ataques que aprovechan las vulnerabilidades del software del DNS
Envenenamiento de la caché del DNS	Exploits	Corrupción de los datos de la caché del 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 del 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)	Explota	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 del DNS, con fines de exfiltración de datos.

Tabla 1: Resumen de los tipos de ataque contra los que defiende Advanced DNS Protection (ADP)

PROTEGER A LOS SUSCRIPTORES Y A LA MARCA

Las soluciones de grado operador de Infoblox para proveedores de servicios protegen a los suscriptores mediante el uso de inteligencia global sobre amenazas y paquetes de protección automatizados. Las soluciones mantienen la disponibilidad de los servicios del DNS críticos en redes en rápida evolución, con tráfico creciente e incluso durante un ataque DDoS malicioso.

- Advanced DNS Protection de Infoblox es la solución de protección del DNS más completa e integrada del sector para la infraestructura del DNS de los proveedores de servicios.
- Capacidad avanzada y automatizada de detección y mitigación de ataques basados en el DNS, como amplificación, reflexión, anomalías de protocolo y túneles, todo ello integrado en el servidor del DNS.
- Soluciones de grado operador y disponible en múltiples formatos, como la función de red virtualizada (VNF) orquestada y soluciones nativas en la nube, que cuentan con el servidor de almacenamiento en caché del DNS más rápido del mundo y compatibilidad con el almacenamiento en caché del DNS y despliegues de DNS autoritativo.
- Inteligencia sobre amenazas y reglas de mitigación con actualizaciones automáticas de Infoblox.
- La tecnología patentada Infoblox Grid proporciona un amplio control, automatización y distribución de las actualizaciones, lo que reduce los costes de soporte operativo y elimina el riesgo de interrupciones causadas por errores de configuración manual.
- Admite protocolos de DNS cifrado, incluidos DNS sobre TLS (DoT) y DNS sobre HTTPS (DoH).

Para obtener más información, visite www.infoblox.com/sp o póngase en contacto con su representante local de Infoblox hoy mismo.

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 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es