infoblox

Threat Intel

NOTAS DE LA SOLUCIÓN

DETECCIÓN DE AMENAZAS BASADA EN DNS PARA DESCUBRIRLAS ANTES DE QUE ATAQUEN

DATOS Y CIFRAS

- El alcance del DNS es enorme. Ahora hay 1589 extensiones de primer nivel y cada día se crean 200.000 nuevos dominios.
- El 81% de las organizaciones han sufrido uno o más ataques de phishing en los últimos 12 meses, según el Estudio sobre el Estado Global de la Ciberseguridad de 2023 de la CRA
- El 75% de las organizaciones se enfrentaron a ataques de smishing (phishing por SMS), según el Informe 2024 de Proofpoint sobre el estado del phishing
- En los ataques de phishing y spear phishing se utilizan con frecuencia dominios similares. En 2022, los hackers chinos utilizaron 42.000 dominios impostores en una campaña masiva de ataques de phishing, según Hacker News.
- No se trata solo de dominios similares. Los atacantes a menudo registran dominios con varios meses de antelación para usarlos en una amplia gama de ataques. Un ejemplo es el conjunto de herramientas Decoy Dog, identificado por primera vez por Threat Intel de Infoblox. Muchos de los dominios C2 rusos utilizados por Decoy Dog se configuran con anticipación e Infoblox los descubrió en otoño de 2022.
- Infoblox detecta y bloquea alrededor de 25.000 nuevos dominios similares a la semana.
- **En resumen:** Existe una necesidad crucial de threat intelligence que identifique de manera proactiva estos dominios emergentes, que podrían usarse en ataques futuros

DESAFÍOS

A los atacantes les encanta el phishing porque es barato y todo lo que requiere es que una persona cometa un error y haga clic en el enlace. Los ataques de phishing por SMS, comúnmente conocidos como smishing, se han incrementado recientemente, y los actores llevan a cabo operaciones de smishing masivas y resilientes. Los dominios de apariencia similar se utilizan a menudo en ataques de phishing y spear phishing. En 2022, los hackers chinos usaron 42.000 dominios impostores en una campaña de ataques de phishing masiva.

Mientras que el phishing y los dominios similares son un problema creciente, hay otros casos en los que se han registrado dominios con meses de antelación antes de utilizarlos en una amplia gama de ataques. Un ejemplo es el recientemente descubierto conjunto de herramientas Decoy Dog, compuesto por un grupo de balizas que explotaban el DNS para comunicarse con la infraestructura de comando y control. El conjunto de herramientas utiliza el RAT Pupy, a menudo asociado con actores estatales en el pasado. Muchos de los dominios asociados con Decoy Dog llevaban activos desde abril de 2022 y eran persistentes y de bajo perfil, lo que dificultaba su detección con las herramientas de seguridad tradicionales.

Se requiere un enfoque diferente para detectar estos ataques, cuyos dominios se configuran mucho antes de la ofensiva.

CAZA DE AMENAZAS BASADA EN DNS

La caza de amenazas basada en DNS utiliza el DNS y análisis a gran escala para rastrear la infraestructura del adversario antes de que inicie un ataque real. Más específicamente, puede:

- Buscar dominios nuevos para los clientes y clasificarlos como nuevos/emergentes o sospechosos utilizando metadatos, tales como el registrador, la extensión TLD, los certificados SSL, el servidor de nombres, el comportamiento de registro, etc.
- Tomar avisos de terceros publicados, por ejemplo, de la CISA, y mejorarlos para encontrar más indicadores utilizando metadatos del DNS. Por ejemplo, en un anuncio reciente de la CISA, Infoblox identificó 13 dominios adicionales que no estaban en el aviso, basándose simplemente en la capacidad de correlacionar metadatos del DNS, lo que ayudó enormemente a reducir un vector de amenaza potencial.

La caza de amenazas basada en DNS protege contra dominios sospechosos semanas o meses antes de que se confirmen como maliciosos y se utilicen en ataques.

UTILIZAR BLOXONE THREAT DEFENSE PARA LA PROTECCIÓN PROACTIVA

Debido a la posición singular de Infoblox en la ruta de consultas, la solución logra observar, analizar y bloquear la intención de comunicarse para ofrecer protección con carácter proactivo. Infoblox, líder del mercado y experto en DNS, rastrea la infraestructura del adversario y revisa los registros del DNS para identificar actividades sospechosas en una fase temprana del ciclo de vida de la amenaza, cuando existe la "intención de comprometer", antes de que comience el ataque real. De este modo, Threat Intel de Infoblox puede identificar dominios nuevos o similares destinados al uso malicioso durante la fase de instrumentalización y clasificarlos como sospechosos semanas o meses antes de que otras organizaciones/proveedores de seguridad los señalen como maliciosos. La principal razón de este desfase entre la clasificación proactiva de las sospechas de amenaza de Infoblox y la detección que ofrecen otras soluciones de seguridad es que estas últimas evalúan la conducta del tráfico o el contenido asociado a esos dominios, algo que muchas veces solo es notorio una vez ya activada la amenaza.

Dominios de alto riesgo

Cuando el equipo considera que ciertos dominios son sospechosos, Infoblox los incluye en un feed llamado «Infoblox Riesgo alto», disponible en BloxOne Threat Defense, para permitir a nuestros clientes protegerse de manera preventiva contra amenazas nuevas y emergentes. Son fuentes con indicadores de dominios muy sospechosos, cuya actividad maliciosa aún no se ha confirmado, pero que muestran indicios de haber sido adquiridos por actores de amenazas como parte de su fase de instrumentalización y pueden activarse para el uso malicioso en el futuro. Los feeds se clasifican en tres categorías:

- **Similares sospechosos:** Tipos de dominios sospechosos que se asemejan a dominios legítimos, posiblemente para el uso en futuras actividades de phishing.
- **NOED sospechosos** (dominios emergentes observados recientemente): Tipos de dominios sospechoso de alto riesgo, que solo se han observado recientemente en el tráfico de clientes (y, por tanto, «emergentes»)
- **Dominios sospechosos:** Otros dominios que parecen sospechosos, pero que no se ajustan al perfil de un similar o NOED sospechoso.

Infoblox lanzó el servicio de datos de dominios emergentes sospechosos a principios de noviembre de 2022 y detectó y clasificó 19,4 millones de indicadores sospechosos activos en 2023. El número de dominios sospechosos activos no hace más que aumentar. Además del elevado volumen, otro criterio importante es la calidad de la clasificación de sospechosos: de los millones de dominios clasificados como sospechosos, solo el 0,0002% se han identificados como falsos positivos.

Este concepto de bloquear dominios sospechosos ha ayudado a los clientes de Infoblox a bloquear con antelación algunos avisos de seguridad, incluidos Decoy Dog, y ataques de MFA, como Oktapus. Muchos de los dominios asociados con el conjunto de herramientas Decoy Dog ya habían sido descubiertos e incluidos en los feeds de dominios sospechosos de BloxOne Threat Defense en otoño de 2022. Así pues, los clientes de BloxOne Threat Defense Advanced que habían configurado su política para bloquear los feeds de dominios sospechosos estaban protegidos contra muchos de los dominios C2 desde entonces.

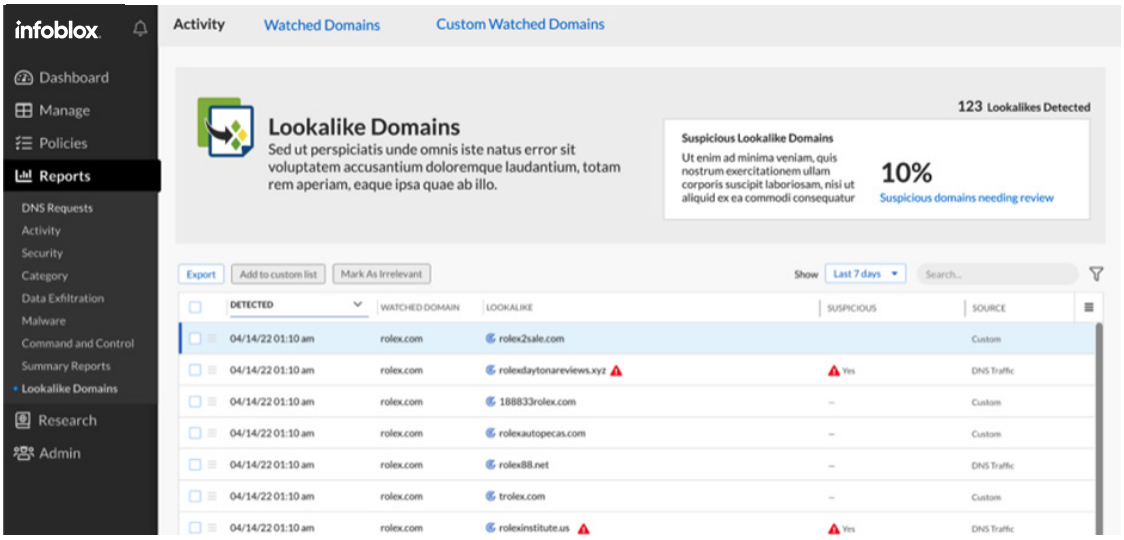
Infoblox añadió 19,4 millones de dominios a los feeds de dominios sospechosos en 2023, que redujeron considerablemente el riesgo de ataques futuros.

Dominios similares

Además de las fuentes de sospechosos, los clientes de Infoblox pueden utilizar la función de seguridad de dominios similares integrada en BloxOne Threat Defense para identificar y detener de forma proactiva amenazas de ingeniería social que utilizan dominios similares en ataques dirigidos avanzados con la intención de penetrar en una empresa, comprometer a sus clientes o dañar su valiosa marca.

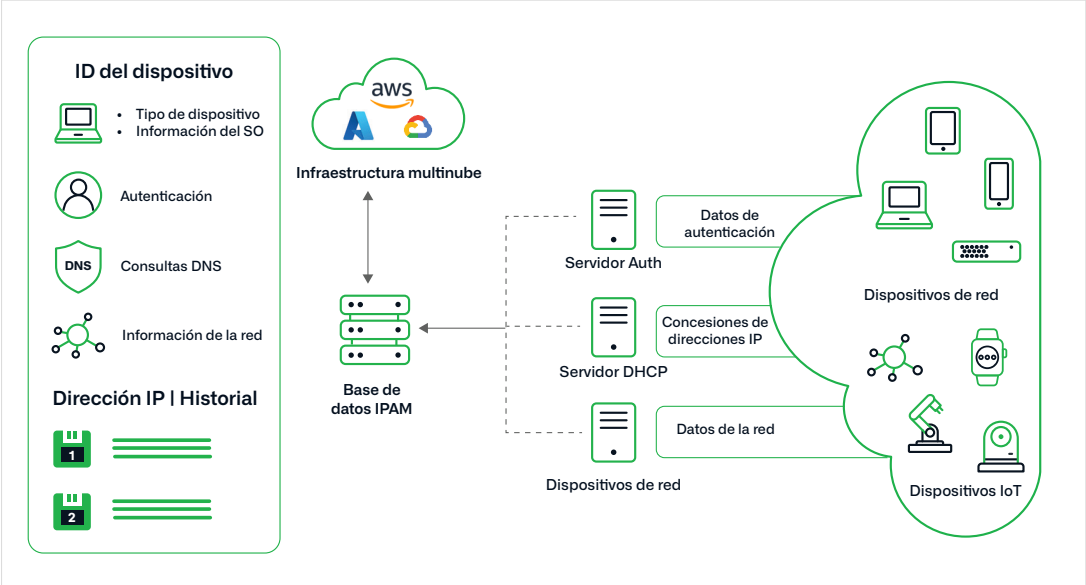
Los clientes pueden señalar dominios utilizados por su propia organización, socios de la cadena de suministro u otros dominios susceptibles de ser imitados en un intento de engañar a los usuarios, socios o clientes como parte de un ciberataque. Infoblox inicia entonces un proceso de monitorización continua de posibles dominios similares y analiza el registro, la actividad, el historial, etc. de cada uno de ellos para evaluar su nivel de riesgo. Estas conclusiones se presentan en un panel interactivo para que los clientes puedan tomar rápidamente decisiones sobre los siguientes pasos con conocimiento de causa. Además, la información se actualiza constantemente para reflejar nuevos dominios similares o actividades relacionadas con los ya identificados.

Existe un servicio de «desactivación», disponible por separado, que aprovecha las profundas relaciones de confianza de Infoblox y nuestra posición única en el entorno global de TI para ayudar a las empresas amenazadas a responder y limitar su exposición económica y de marca. Los servicios de mitigación de dominios de Infoblox incluyen servicios de validación para confirmar que, de hecho, se ha producido un incidente; mitigación mediante la coordinación con los principales ISP y reguladores, y monitorización seguida de informes para comprender mejor el panorama de la amenaza y fortalecer la seguridad. Gracias a nuestra buena reputación por la diligencia y calidad de investigación, el tiempo medio de eliminación en algunas regiones puede ser de apenas 24 horas, lo que permite a nuestros clientes erradicar muchas amenazas antes de que actúen y recuperar rápidamente la normalidad.



Fácil atribución de usuarios y dispositivos

Aunque bloquear las comunicaciones de estos dominios es el primer paso, es igualmente importante contar con visibilidad rápida de los dispositivos o activos involucrados en esas comunicaciones. La sincronización de los metadatos de IPAM con el DNS proporciona la visibilidad necesaria para identificar el origen de las consultas maliciosas en la red. Utilizando datos de IPAM, es sencillo determinar si la actividad anómala del DNS proviene de dispositivos de red, como cortafuegos, dispositivos de usuario o de otro tipo de activo conectado a la red. Con Infoblox, es incluso posible definir fácilmente una política de seguridad basada en metadatos de IPAM.



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

+1.408.986.4000
www.infoblox.com

Versión: 20240411v1