NOTAS DE LA SOLUCIÓN

Infoblox Threat Intel

Caza, rastrea y detiene las amenazas en su origen: DNS

RETOS DEL USO DE THREAT INTELLIGENCE CENTRADA EN MALWARE

La mayoría de las soluciones de seguridad adoptan un enfoque de threat intelligence centrado en el malware, que requiere que los riesgos se materialicen antes de marcar un dominio como malicioso. Este enfoque posterior a los incidentes significa que juegan a cazar topos, tratando de detectar sitios web maliciosos a medida que aparecen y añadiéndolos a las fuentes de threat intel para bloquearlos.

Por tanto, pese a los esfuerzos del sector de la seguridad, los ataques MFA, los ataques con dominios falsos similares y los ataques de suplantación de identidad dirigidos siguen afectando a las organizaciones, lo que provoca filtraciones de datos y daños a la reputación de la marca. Es necesario adoptar una metodología de seguridad diferente, capaz de proteger con carácter proactivo a las empresas frente a los actores delictivos, cuando estos construyen su infraestructura de ataque.

DESMANTELAR LA CIBERDELINCUENCIA EN SU NÚCLEO CON THREAT INTEL DE INFOBLOX

Threat Intel de Infoblox combina sus conocimientos expertos en DNS líderes del mercado con ciencia de datos de vanguardia para identificar la infraestructura de los actores de amenazas antes de que estos la usen y suspender las comunicaciones con esos dominios de alto riesgo. Threat Intel de Infoblox es la primera y única solución que se centra en efectuar un seguimiento de los actores de amenazas en el DNS y de sus actividades en internet, de modo que protege proactivamente a los clientes frente a ataques emergentes, en especial smishing, dominios falsos similares, dominios de alto riesgo, ransomware, malware de mando y control (C&C) y más. Infoblox Threat Defense utiliza Threat Intel de Infoblox para detectar y detener amenazas críticas meses antes que otros sistemas de seguridad. Threat Intel de Infoblox se centra en el DNS por usted, lo que le permite proteger su red sin sacrificar su rendimiento.

ESTADÍSTICAS CLAVE:

En el primer trimestre de 2024,

- El 60% de las amenazas se detectaron antes de la primera consulta DNS
- El 82% de las amenazas se detectaron tras una sola consulta al DNS
- El 89% de las amenazas se detectaron en las primeras 48 horas

DATOS Y CIFRAS

- Los ataques de autenticación multifactor (MFA) son los más visible y amenazantes de 2023, que combinan la vulnerabilidad de los empleados (incluidos los que trabajan desde casa o en remoto) con el uso de dominios falsos similares al original
- El 75% de las organizaciones se enfrentaron a ataques de smishing (Informe 2024 de Proofpoint sobre el estado del phishing)
- Para muchos ataques, los actores de amenazas envejecen sus dominios durante bastante tiempo, incluso meses, después de registrarlos

DISPONIBILIDAD INMEDIATA DE THREAT INTEL DE INFOBLOX

Threat Defense, el producto de detección del DNS y respuesta de Infoblox, está disponible en cuatro paquetes:

1. Threat Defense Essentials
2. Threat Defense Business On-Premises
3. Threat Defense Business Cloud
4. Threat Defense Advanced

Cada paquete ofrece acceso a una variedad de datos de Threat Intel de Infoblox a través de "fuentes RPZ". El paquete Advanced también incluye una herramienta para la inclusión y distribución personalizada de fuentes de amenazas llamada TIDE (Threat Intelligence Data Exchange), además de un portal de investigación de amenazas llamado Dossier basado en estos datos, y más ventajas.

Estas son las fuentes de amenazas disponibles para cada paquete de Threat Defense:

Fuentes	Esencial	Business OnPrem	Business Cloud	Advanced
Infoblox Base	X	X	X	X
Infoblox Base IP		X	X	X
Infoblox Riesgo alto				X
Infoblox Riesgo medio				X
Infoblox Riesgo bajo				X
Infoblox Informativo		X	X	X
Nombres de host públicos de DoH	X	X	X	X
IP públicas de DoH	X	X	X	X
Bogon	X	X	X	X
Dominios AIS DHS	X	X	X	X
IP AIS DHS	X	X	X	X
IP de EECN		X	X	X
IP sanciones OFAC EE.UU.				X
IP sanciones OFAC EE.UU. Riesgo alto		X	X	X
IP sanciones OFAC EE.UU. Riesgo medio		X	X	X
Nombres de host y dominios de criptomonedas		X	X	X
IP de nodos de salida Tor		X	X	X

DESCRIPCIÓN RESUMIDA DE LOS FEEDS

Infoblox Base: La fuente de Infoblox Base habilita la protección contra dominios conocidos malintencionados o comprometidos. Se incluye el malware conocido, el ransomware, APT, los kits de exploits, los servidores de nombres maliciosos, los sumideros, etc. Recomendamos bloquearlos para todos los usuarios.

Infoblox Base IP: La fuente Infoblox Base IP habilita la protección contra direcciones IP maliciosas o comprometidas conocidas. Estas IP son infraestructuras conocidas que hospedan amenazas capaces de actuar o controlar un sistema a través de C&C, descargas de malware y sitios de phishing activos. Recomendamos bloquearlos para todos los usuarios.

Infoblox Riesgo alto: La fuente Infoblox Riesgo alto incluye dominios aún no confirmados, pero muy sospechosos, que es muy probable que se utilicen en un acto malicioso en algún momento. Estos dominios, aún no confirmados, se asocian a un alto nivel de amenaza con gran confianza, por lo que recomendamos bloquearlos para la mayoría de los usuarios. Se incluyen dominios sospechosos, dominios similares sospechosos y NOED (dominios emergentes recién observados) sospechosos con una puntuación combinada elevada en niveles de amenaza y de confianza.

Infoblox Riesgo medio: La fuente Infoblox Riesgo medio incluye dominios aún no confirmados, pero que presentan un riesgo medio. Son dominios sospechosos con una puntuación combinada de los niveles de amenaza y confianza inferior a la de la fuente de riesgo alto, pero superior a la de la fuente de riesgo bajo. Aun así, es probable que puedan utilizarse en actos maliciosos, por lo que recomendamos bloquearlos para la mayoría de los usuarios. Se incluyen dominios sospechosos, dominios similares sospechosos y NOED (dominios emergentes recién observados) sospechosos con una puntuación combinada media en niveles de amenaza y de confianza.

Infoblox Riesgo bajo: La fuente Infoblox Riesgo bajo incluye dominios aún no confirmados, pero que aun así son sospechosos y es posible que puedan utilizarse en actos maliciosos. Estos dominios presentan una puntuación combinada de los niveles de amenaza y confianza más baja. Se recomienda que la mayoría de los usuarios los monitoricen con la opción Allow-WithLog (permitir con registro) y que los bloqueen en entornos sensibles. Se incluyen dominios sospechosos, dominios similares sospechosos y NOED (dominios emergentes recién observados) sospechosos con una puntuación combinada baja en niveles de amenaza y de confianza.

Infoblox Informativo: La fuente Infoblox Informativo incluye dominios con niveles de amenaza y confianza bajos. Se usan para fines informativos en función de la política y la sensibilidad del entorno. Esta fuente incluye dominios emergentes recién observados (NOED). Se recomienda monitorizarlos con la opción Allow-WithLog (permitir con registro) para la mayoría de los usuarios e incluirlos en el modo de bloqueo para entornos confidenciales (ya que los nuevos dominios no son críticos en su mayor parte, y es mejor habilitarlos cuando se hayan establecido durante un periodo más largo).

Bogon: Las IP de Bogon suelen ser direcciones de origen de ataques DDoS. “Bogon” es un nombre informal para un paquete IP disponible públicamente en internet, que afirma provenir de una zona del espacio de direcciones IP reservada, pero aún no asignada ni delegada por la Autoridad de Números Asignados en Internet (IANA) o un Registro de Internet Regional (RIR) delegado. Las zonas del espacio de direcciones no asignadas se denominan “espacio bogon”. Muchos ISP y cortafuegos de usuario final filtran y bloquean bogons porque carecen de uso legítimo y, por lo general, se deben a una mala configuración, ya sea accidental o malintencionada.

DHS AIS IP y DHS AIS Domain (2 fuentes): El programa Automated Indicator Sharing (AIS) del Departamento de Seguridad Nacional (DHS) de Estados Unidos permite que se intercambien indicadores de ciberamenazas entre el gobierno federal y el sector privado. El programa AIS forma parte del esfuerzo del DHS por crear un ecosistema en el que, tan pronto como una empresa o agencia federal observe un intento de ataque, se comparta el indicador con los socios del programa AIS, incluido Infoblox. Los indicadores de IP contenidos en esta fuente no están validados por el DHS, puesto que se prioriza la velocidad y el volumen. Infoblox no modifica ni verifica los indicadores. Sin embargo, Infoblox clasifica y normaliza los indicadores del programa AIS para facilitar su uso.

Los datos incluidos en las fuentes AIS IP y AIS Hostname incluyen datos del AIS sujetos a las Condiciones de Uso del Intercambio Automatizado de Indicadores del DHS estadounidense, disponibles en www.us-cert.gov/ais, y deben utilizarse de acuerdo con dichas Condiciones de Uso. Antes de proceder a distribuir los datos del AIS, es posible que se le solicite que firme y envíe las Condiciones de Uso disponibles en www.us-cert.gov/ais. Para obtener más información, envíe un correo electrónico a ncciccustomerservice@hq.dhs.gov.

Nombres de host públicos DoH e IP públicas DoH (2 fuentes): esta fuente basada en políticas contiene nombres de dominio e IP de servicios DoH (DNS a través de HTTPS) de terceros. Las organizaciones que deseen implantar políticas de seguridad a través del DNS pueden estar interesadas en evitar la omisión de las políticas de seguridad del DNS mediante el uso de servidores DoH de terceros.

IP de nodos de salida Tor: Los nodos de salida de Tor son las puertas de enlace por las que accede a internet el tráfico cifrado de Tor. Esto significa que un nodo de salida puede monitorizar el tráfico de Tor (después de que abandone la red de capas). La red Tor está diseñada para dificultar la determinación del origen del tráfico.

Nombres de host de criptomonedas: Esta fuente contiene amenazas que permiten a los actores maliciosos llevar a cabo actividades ilegales o fraudulentas, colmenas de monedas que permiten a los propietarios de sitios web incrustar software de minería de criptomonedas en sus webs para reemplazar la publicidad normal, cryptojacking que permite a los propietarios de sitios web minar criptomonedas sin el consentimiento de su propietario y grupos de minería de criptomonedas.

IP de EECN: esta fuente basada en políticas contiene IP de países de Europa del Este ajenos a la UE y de China, que a menudo son fuentes de ciberataques contra la propiedad intelectual u otros datos confidenciales o restringidos, así como de robos de tarjetas de crédito o información financiera.

IP sanciones OFAC EE.UU.: esta fuente basada en políticas contiene IP de los países sancionados por Estados Unidos que figuran en la lista de la Oficina de Control de Activos Extranjeros del Tesoro de Estados Unidos (OFAC), la cual administra y aplica las sanciones económicas impuestas por Estados Unidos a países extranjeros. Encontrará más información en la página “Sanctions Programs and Country Information” disponible en: www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

IP sanciones OFAC EE.UU.: Riesgo alto: esta fuente incluye todos los indicadores de alto riesgo de los países sancionados. En la fuente se incluyen indicadores de los siguientes países: Bielorrusia, Camboya, China, Corea del Norte, Cuba, República Democrática del Congo, Irán, Irak, Libia, Macao, Myanmar, República Centroafricana, Rusia, Siria, Venezuela y Yemen.

IP sanciones OFAC EE.UU.: Riesgo medio: esta fuente incluye todos los indicadores de riesgo medio de los países sancionados. En la fuente se incluyen indicadores de los siguientes países: Bielorrusia, Camboya, China, Corea del Norte, Cuba, República Democrática del Congo, Irán, Irak, Libia, Macao, Myanmar, República Centroafricana, Rusia, Somalia, Sudán del Sur, Sudán, Siria, Venezuela, Yemen y Zimbabue.

OPORTUNIDADES ADICIONALES PARA OPTIMIZAR EL USO DE THREAT INTEL DE INFOBLOX

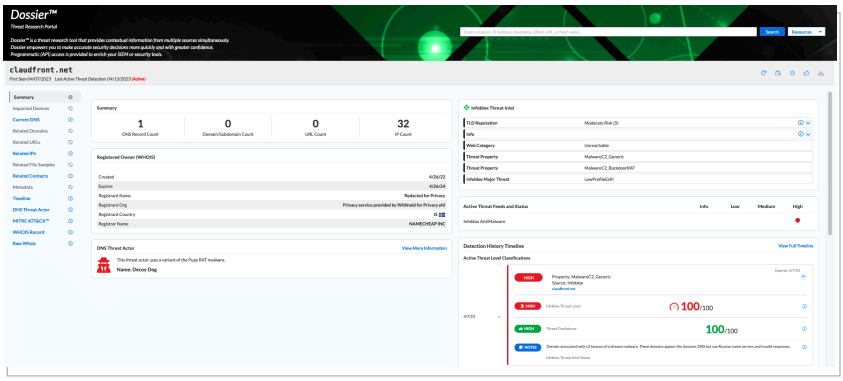
Threat Defense Advanced ofrece dos características únicas que agilizan las investigaciones de amenazas, aceleran la respuesta a incidentes, facilitan la caza de amenazas y mejoran muchas otras actividades de SecOps.

TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE es una plataforma capaz de automatizar la entrada, la gestión y la distribución de Threat Intel de Infoblox. Permite usar fuentes adicionales del gobierno o del sector, de código abierto, de proveedores de threat intelligence (TI) terceros, proveedores de seguridad general o incluso threat intelligence interna.

DOSSIER

Dossier ofrece a los analistas una visión de threat intelligence centrada en el DNS, que incluye el impacto en su propia red y un historial completo de veredictos de un indicador. Se destacan los indicadores relacionados y la información de los actores de amenazas para facilitar la evaluación de las amenazas persistentes. Las ampliaciones incluyen puntuaciones de reputación de Infoblox, información de registro, categorización de contenido, enlaces a publicaciones y otra información actual del DNS. Una API proporciona acceso programático para su integración en productos SIEM.



FUENTES DE AMENAZAS DE TERCEROS DISPONIBLES PARA INFOBLOX THREAT DEFENSE ADVANCED

Threat Defense Advanced ofrece a los clientes la opción de complementar las numerosas opciones de threat intelligence de Infoblox con datos de amenazas adicionales obtenidos de fuentes de terceros. Si bien las funciones TIDE de Threat Defense pueden automatizar la entrada y el intercambio de información sobre amenazas, algunos socios posibilitan una integración rápida y sencilla mediante BYOL (Bring Your Own License). Una vez adquiridas las licencias adecuadas de los socios indicados a continuación, los clientes solo tienen que introducirla en la página BYOL de Threat Defense Advance para activar la integración, que estará lista para usar de inmediato. Algunos socios colaboran con Infoblox para agilizar el proceso de incorporación de los clientes. Los siguientes socios ofrecen compatibilidad inmediata:

FireEye iSIGHT Threat Intelligence: su inteligencia de ciberamenazas sobre IP y nombres de host proporciona a las empresas análisis estratégicos, operativos y tácticos derivados de su equipo de expertos global. Una suscripción a ThreatScape proporciona la inteligencia necesaria para ajustar un programa de seguridad a los objetivos de gestión de riesgos empresariales y defenderse de forma proactiva contra ciberamenazas nuevas y emergentes. Aunque los clientes deben adquiriri la fuente iSight directamente de FireEye, Infoblox puede facilitar la activación de la fuente en la plataforma TIDE.

Fuente de dominios recién observados (NOD) de Farsight Security: Esta fuente de DomainTools ofrece una capa añadida de defensa para combatir la exfiltración de malware, el abuso de marcas y los ataques basados en spam que se originan o terminan en dominios recién activados.

VirusTotal es la plataforma de threat intelligence colaborativa más completa y procesable del planeta. Al proporcionar un contexto integral, ayuda a los equipos de seguridad que se enfrentan con frecuencia a archivos/URL/dominios/direcciones IP desconocidos cuando tratan de comprender un ataque. La integración de la threat intelligence de VirusTotal en Threat Defense permite a los analistas de seguridad aplicar este contexto exclusivo fácilmente, ya que utilizan los datos de inteligencia de dispositivos, eventos y amenazas para hacerse una imagen del incidente con rapidez.

Aviso: Este es un resumen publicitario de las capacidades de threat intelligence contenidas en las ofertas de Threat Defense. Se actualiza periódicamente, pero, al tratarse de un producto SaaS, las capacidades reales de los productos pueden diferir de lo indicado en el presente documento.

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

+1.408.986.4000
www.infoblox.com

Versión: 20251902v2