infoblox®

2025 INFORME SOBRE EL PANORAMA DE AMENAZAS AL DNS

La niebla de las ciberamenazas:

cómo utilizan los actores maliciosos el DNS para engañar y evadir

En el último año, los actores maliciosos han hecho rápidos avances en el uso del engaño, ampliando sus operaciones y aprovechando la IA para atacar a personas y organizaciones, y evadir la investigación de amenazas. Infoblox Threat Intel ha observado un nuevo nivel de profesionalidad y rapidez en la forma en que los actores lanzan ciberataques procedentes del Domain Name System (DNS), que afectan tanto a consumidores como a empresas y organismos gubernamentales.

Para defenderse de forma eficaz, los equipos de seguridad deben comprender las amenazas a las que se enfrentan. Obtener información sobre las técnicas adversarias del DNS, los actores que hay detrás de ellas y los riesgos que plantean es esencial para reforzar las estrategias de defensa.

Este informe se basa en grandes volúmenes de telemetría del DNS en tiempo real, análisis de vanguardia y décadas de experiencia en amenazas para ofrecer una perspectiva única sobre cómo explotan el DNS los atacantes. También describe las implicaciones para las empresas y destaca la inteligencia basada en el DNS como capa crítica de la ciberdefensa moderna.

ÍNDICE

EL POTENCIAL SIN EXPLOTAR DE LA INTELIGENCIA DEL DNS 5

SECCIÓN 1: PRINCIPALES OBSERVACIONES DE AMENAZAS AL DNS 6

Naturaleza efímera de los dominios 6

Evasión de controles mediante dominios de un solo uso 6

Dominios maliciosos frente a dominios sospechosos 7

Encubrimiento mediante dominios como parte de los sistemas de distribución del tráfico 7

Dominios vinculados a diversos tipos de amenazas 7

Popularidad de dominios 8

SECCIÓN 2: ACTORES DE AMENAZAS E INVESTIGACIÓN 9

ESTUDIO DE CASO: COORDINACIÓN ENTRE HACKERS DE WORDPRESS Y LA CAMARILLA VEXTRIO VIPER 12

SECCIÓN 3: TÉCNICAS MALICIOSAS DEL DNS 13

LOS SISTEMAS DE DISTRIBUCIÓN DEL TRÁFICO PROPORCIONAN UN NIVEL DE EVASIÓN PELIGROSO 14

El adtech malicioso es un vector de amenazas infracomunicado y de rápido crecimiento 15

Infraestructuras a gran escala, difíciles de interrumpir 15

El adtech malicioso sirve como puerta de entrada al riesgo empresarial 15

Ejemplo de TDS en funcionamiento: 16

Dominios utilizados por los sistemas de distribución de tráfico 17

SECUESTRO DE DOMINIOS PARA ROBAR CONFIANZA 18

Ataques “Sitting Ducks” 18

CNAMES colgantes 18

LOS DOMINIOS SIMILARES Y CON ERRORES TIPOGRÁFICOS ENGAÑAN A LOS USUARIOS 18

LA TUNELIZACIÓN DE DNS UTILIZADA POR ACTORES DE AMENAZAS, PENTESTERS Y HERRAMIENTAS DE SEGURIDAD LEGÍTIMAS 19

Los equipos de seguridad necesitan un bisturí para detener la tunelización del DNS 20

SECCIÓN 4: DESAFÍOS PARA LOS DEFENSORES 21

LA IA ADVERSARIA ELUDE LOS CONTROLES DE SEGURIDAD EXISTENTES 21

Caso práctico: Reckless Rabbit utiliza deepfakes para atacar a víctimas de habla japonesa 21

Chatbots impulsados por inteligencia artificial 22

Ofuscación y evasión de código 23

PROTEGER LA REPUTACIÓN DE LA MARCA Y LA ORGANIZACIÓN 23

PRESIONES DE CUMPLIMIENTO Y DESAFÍOS DE DNS PARA LOS EQUIPOS DE SEGURIDAD 23

PRÓXIMOS PASOS 24

TERMINOLOGÍA UTILIZADA 25

EL POTENCIAL SIN EXPLOTAR DE LA INTELIGENCIA DEL DNS

A menudo se hace referencia al DNS como la guía telefónica de Internet, ya que traduce los nombres de dominio en direcciones IP. Todas las interacciones digitales comienzan con una solicitud al DNS, lo que lo convierte en una fuente de telemetría de alta fidelidad para las operaciones de red, ya que proporciona visibilidad profunda de los activos digitales que inician una conexión en internet.

El DNS también es utilizado por actores maliciosos con fines de phishing, fraude y evasión de la detección, y durante la extracción de datos. Por tanto, analizar el tráfico del DNS y el uso de los dominios es fundamental para los analistas de seguridad. Los datos del DNS pueden transformarse en inteligencia predictiva sobre amenazas gracias a la recopilación integral de la telemetría previa al ataque, el enriquecimiento de los datos, su contraste con referencias y la conducción de búsquedas exhaustivas de amenazas. Esta información ofrece a los defensores una visión completa de las infraestructuras adversarias, las víctimas seleccionadas y las tácticas, antes de que el atacante lance su ataque.

"El DNS ofrece una perspectiva única sobre la actividad de amenazas pasada, que a su vez sirve como bola de cristal para revelar precursores de ciberamenazas futuras".

— **Dra. Renée Burton**
Directora de Inteligencia de Amenazas de Infoblox

Como resultado, el DNS ofrece mucho más que la simple resolución de nombres y se ha convertido tanto en un punto de aplicación de la política de seguridad de las empresas como en un indicador de posibles actividades maliciosas en una red. Organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) y la Agencia de Seguridad Cibernética y de Infraestructuras (CISA) estadounidenses han reconocido el papel fundamental —y temprano— que desempeña el DNS en la ciberseguridad y han destacado su potencial de seguridad preventiva en la reciente publicación especial (SP) del NIST 800-81 Rev. 3.[1]

Este informe aborda cuatro preguntas clave:

¿Cuáles son las principales observaciones sobre el DNS en los últimos 12 meses?

¿Quiénes son los actores de amenazas del DNS y qué actividades recientes se han descubierto?

¿Cuáles son las principales tácticas maliciosas detrás de las técnicas de DNS y por qué son peligrosas?

¿Cuáles son los principales retos para los defensores y qué oportunidades ofrece la inteligencia de amenazas basada en el DNS?

1 Secure Domain Name System (DNS) Deployment Guide, Instituto Nacional de Estándares y Tecnología (NIST), 10 de abril de 2025.

SECCIÓN 1: PRINCIPALES OBSERVACIONES DE AMENAZAS AL DNS

100.8
million newly observed domains in one year

25.1%
of newly observed domains are malicious or suspicious

Naturaleza efímera de los dominios

A finales de mayo de 2025, Infoblox procesaba y analizaba 70.000 millones de consultas al DNS diarias, procedentes de más de 13.000 entornos de Infoblox, que abarcaban millones de direcciones IP en todo tipo de dispositivos.

Los datos totalmente anónimos de más de 1.300 clientes de Infoblox Threat Defense™ proporcionan visibilidad global y detallada de millones de interacciones en internet, que abarcan múltiples tipos de clientes, geografías y sectores. El aumento interanual del volumen de telemetría del DNS era del 21%.

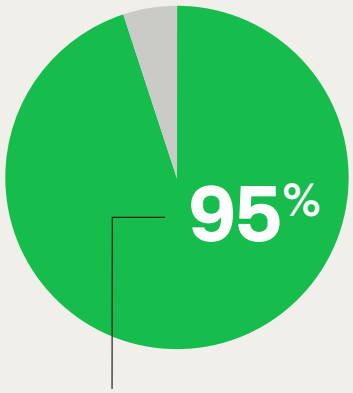
Entre todos los datos recopilados, Infoblox Threat Intel identificó **100,8 millones de dominios nuevos (de segundo nivel) en los últimos 12 meses**. Este elevado volumen de dominios de nueva generación suele ser resultado de infraestructuras que cambian rápidamente, campañas publicitarias a corto plazo e iniciativas de branding.

Evasión de controles mediante dominios de un solo uso

Infoblox clasificó como maliciosos o sospechosos más de una cuarta parte de los dominios nuevos observados (más de 25 millones). Los actores maliciosos registran, activan y despliegan continuamente un gran número de dominios nuevos para evadir los controles de detección. Dado que es difícil identificar y clasificar volúmenes tan grandes de dominios, los atacantes pueden pasar desapercibidos y eludir los mecanismos de bloqueo sin dejar apenas pruebas forenses.

El uso aislado de dominios identificados como relacionados con amenazas, tanto maliciosos como sospechosos, también es significativo. Infoblox Threat Intel descubrió que el 95% de todos los dominios relacionados con amenazas se observaron en un único entorno de red.

El objetivo de esta táctica es sencillo: eludir las defensas forenses que se basan en datos del “paciente cero” aprovechando los dominios desechables, de los que los atacantes disponen de un suministro ilimitado.



of threat-related domains were observed in only one customer environment.

Dominios maliciosos frente a dominios sospechosos

- **Los dominios maliciosos** son amenazas confirmadas respaldadas por pruebas sólidas. No caducan y representan el 1,6% de los más de 100 millones de dominios nuevos observados.
- **Los dominios sospechosos** son amenazas potenciales que carecen de pruebas concluyentes, y representan el 23,5% de todos los dominios nuevos observados. Si no se confirman, estos indicadores caducan al cabo de unos meses. Los analistas de Infoblox Threat Intel supervisan continuamente estos dominios en busca de nuevas pruebas. Cuando se descubren indicadores adicionales, se actualizan las puntuaciones y los dominios sospechosos pueden reclasificarse como maliciosos.

Encubrimiento mediante dominios como parte de los sistemas de distribución del tráfico

Adtech (abreviatura de “tecnología publicitaria”) hace referencia a las herramientas, el software y las plataformas que se utilizan para automatizar, gestionar, segmentar, distribuir y analizar la publicidad digital. Los sistemas de distribución de tráfico (TDS) son plataformas o mecanismos que se utilizan para —de forma legítima o maliciosa— redirigir el tráfico entrante de internet hacia diferentes destinos en función de reglas predefinidas. Los actores de amenazas también han adoptado esta tecnología, a menudo denominada “**adtech malicioso**”.

82%

of customers queried a domain part of a traffic distribution system.

Durante los últimos 12 meses, **el 82% de todos los entornos de clientes** consultaron dominios que formaban parte de TDS, muchos de ellos operados por gestores de adtech malicioso conocidos por ocultar contenido dañino, como sitios de phishing a medida, scareware, estafas e infostealers.

Estos TDS suelen constar de decenas de miles de dominios, que se rotan rápidamente para evadir la detección y distribuir contenido malicioso dirigido a las víctimas ideales, al tiempo que encubren ese contenido ante los investigadores de amenazas.

Con el tiempo, Infoblox Threat Intel descubrió más de **un millón de dominios utilizados por 168 operadores de adtech malicioso** en su infraestructura de TDS. Estos indicadores abarcan múltiples técnicas del DNS, como dominios secuestrados, dominios similares, redireccionamientos y conjuntos de dominios prerregistrados algorítmicamente (algoritmos de nombres de dominio registrados o RDGA). En la sección 3 se ofrece más información sobre los TDS, cómo funcionan y por qué son peligrosos.

Dominios vinculados a diversos tipos de amenazas

A medida que se descubren nuevos dominios relacionados con amenazas, los investigadores de amenazas de Infoblox analizan los actores que hay tras ellos y sus intenciones. La tabla de la página siguiente presenta una lista priorizada de cómo utilizan sus dominios los actores para diversos fines maliciosos.

Lista de los 7 principales: Cómo los actores de amenazas utilizan nuevos dominios	
1	**Participar en actividades fraudulentas y estafas**, como sitios falsos de inversión en criptomonedas.
2	**Alojar contenido ilegal**, incluidos juegos de azar (especialmente en regiones como China) y material para adultos.
3	**Crear páginas de phishing** diseñadas para robar información personal o datos de tarjetas de crédito.
4	**Desplegar software malicioso.** Algunos ejemplos comunes son los infostealers o ladrones de información (p. ej., Lumma Stealer), los cargadores a través de descargas ocultas (ej., SocGholish), las redes de bots y el ransomware (ej., BlackBasta).
5	**Encubrir sus actividades** a través de TDS y distribuir cargas útiles varias o engañar a los usuarios para que permitan notificaciones no deseadas en el navegador.
6	**Distribuir programas potencialmente no deseados** (**PUP**), como scareware o extensiones de navegador innecesarias.
7	**Llevar a cabo campañas de spam y distribuir correos electrónicos maliciosos**.

Tabla 1. Finalidad de los actores en los dominios recién observados.

Popularidad de dominios

La telemetría del DNS de Infoblox también proporciona información sobre el uso de los tipos de dominios, lo que ofrece pistas sobre la popularidad de las aplicaciones y la velocidad a la que los actores maliciosos adquieren destrezas para situar con éxito grandes volúmenes de dominios instrumentalizados ante las víctimas.

19 DAYS

Time needed for a TDS domain to become popular

Observaciones clave:

- Ocho categorías de dominios, como redes de distribución de contenidos (CDN), proveedores de tecnología, proveedores de seguridad, herramientas de productividad empresarial, motores de búsqueda, almacenamiento, servicios en la nube y conferencias en red, representan la mayoría (aproximadamente el 70% en un día determinado) de todos los dominios en las consultas de clientes al DNS.
- En mayo de 2025, las consultas de dominios relacionados con el uso personal de internet, como compras en línea, juegos y redes sociales (p. ej., TikTok y Facebook), alcanzaron la paridad con las asociadas a las plataformas de colaboración profesional (p. ej., Microsoft Teams y Slack). Estos datos ilustran la **creciente superposición entre el uso profesional y personal de internet**, superposición de la que son muy conscientes los actores maliciosos.

- Los adversarios buscan continuamente superficies de ataque débiles, como los dispositivos móviles y los equipos propios (BYOD), y engañan a los usuarios para que ejecuten acciones de alto riesgo destinadas a extraer datos de la empresa, credenciales incluidas. Esta tendencia también se destacó en el Informe de investigaciones sobre violaciones de datos de 2025 de Verizon,[2] que afirma que ningún dispositivo está fuera de alcance y señala que el **46% de las credenciales corporativas robadas** procedían de dispositivos no gestionados o personales.
- Infoblox Threat Intel observó popularizarse dominios que forman parte de TDS[3] en tan solo 19 días, **2,35 veces más rápido que en 2024 y 39 veces más rápido que en 2020.** La velocidad a la que los dominios de los TDS ganan popularidad —comparable a la de sitios legítimos como `panerabread[.]com` o `draftkings[.]com`— ilustra la eficacia con la que los dominios instrumentalizados se propagan y obtienen el acceso de las víctimas. Los actores de amenazas despliegan rápidamente grandes volúmenes de estos dominios frente a sus objetivos, con lo que maximizan el impacto de sus campañas y superan a fuentes de inteligencia más lentas, como la inteligencia de fuentes abiertas (OSINT) y el análisis forense.

SECCIÓN 2: ACTORES DE AMENAZAS E INVESTIGACIÓN

204K
total identified suspicious domain clusters

662
total identified DNS threat actors

10
new actors publicly disclosed in the past 12 months

Los 100 millones de nuevos dominios descubiertos durante el último año no son fuerzas de la naturaleza, sino que siempre son el resultado de acciones humanas y se activan con fines específicos. Infoblox Threat Intel analiza e investiga continuamente a los actores que se esconden detrás de los dominios relacionados con amenazas, para enriquecer la telemetría recopilada y correlacionar patrones comunes

Desde el inicio de su investigación, Infoblox Threat Intel ha descubierto un total de 204.000 clústeres de dominios sospechosos, cada uno de los cuales comparte elementos de amenaza comunes, y ha identificado 662 actores de amenazas distintos. Solo en los últimos 12 meses, los investigadores de Infoblox han revelado públicamente 10 nuevos actores a través de diversos informes de investigación y entradas de blog.

2 2025 Data Breach Investigations Report, Verizon.

3 Un dominio se considera popular cuando pertenece al subconjunto de dominios que representan la mayor parte del tráfico de clientes durante un periodo específico. En un día determinado, puede oscilar entre 6.000 y 10.000 dominios. Para obtener más información, consulte https://blogs.infoblox.com/wp-content/uploads/infoblox-whitelists-that-work.pdf.

La siguiente lista refleja los principales actores de amenazas identificados y revelados públicamente por Infoblox Threat Intel entre el 1 de julio de 2024 y el 1 de julio de 2025.

Actor	Descripción
	Este actor opera un TDS malicioso que secuestra tráfico web legítimo, principalmente de sitios WordPress comprometidos, y lo redirige a estafas, software malicioso y contenido de phishing. VexTrio está considerado uno de los actores más omnipresentes y evasivos del panorama de amenazas. Durante los últimos 12 meses, este actor ha aparecido en varios informes por su relación con hackers afiliados y es conocido por secuestrar dominios para suministrar su infraestructura de ataque. **Informes publicados recientemente:** • Lo molesto y lo malicioso: la inquietante relación entre los hackers de WordPress y una camarilla de adtech • Empujados hacia la madriguera
	Este sofisticado grupo de actores de amenazas al DNS se dedica a secuestrar recursos abandonados en la nube, como buckets de Amazon S3 y puntos de conexión de Azure, aprovechando registros del DNS mal configurados u olvidados, en particular entradas de nombres canónicos (CNAME) descolgadas. Una vez que Hazy Hawk obtiene el control de estos subdominios, aprovecha la confianza inherente de los dominios legítimos para alojar contenido malicioso. Sus operaciones suelen consistir en redirigir a los usuarios a través de TDS para distribuir estafas, software malicioso y notificaciones push engañosas. **Informes publicados recientemente:** • Nublado con posibilidad de secuestro: los registros del DNS olvidados permiten actuar a un estafador
	Este actor de amenazas con motivaciones económicas lleva desde febrero de 2023 utilizando dominios secuestrados para ejecutar estafas de inversión. Incrusta estos dominios en anuncios de Facebook de corta duración en varios continentes, dirigidos a víctimas en más de 30 idiomas, entre ellos inglés, italiano, polaco, turco y español. El actor emplea el vector de ataque Sitting Ducks para secuestrar dominios con buena reputación, que luego utiliza para ocultar sus sitios fraudulentos ante los investigadores de seguridad. En octubre de 2024, Infoblox había identificado casi 5.000 dominios secuestrados vinculados a este actor. **Informes publicados recientemente:** • Descubriendo los patrones de TTP de los actores y el papel del DNS en las estafas de inversión • Los depredadores del DNS secuestran dominios para abastecer su infraestructura de ataque

	Reckless Rabbit es un actor dedicado a las estafas de inversión que atrae a sus víctimas a través de anuncios maliciosos en Facebook. Emplea RDGA basados en diccionarios y se dirige a personas de varios países, entre ellos Austria, Bélgica, Dinamarca, Francia, Polonia, Suecia y el Reino Unido. El actor utiliza RDGA y recomendaciones falsas. **Informes publicados recientemente:** • Descubriendo los patrones de TTP de los actores y el papel del DNS en las estafas de inversión
	Este actor de phishing lleva a cabo campañas de estafa de inversiones con RDGA basados en diccionarios y suplanta servicios populares. El actor opera su propio servicio de encubrimiento de dominios para la validación de usuarios y se dirige a países de Europa del Este, como Rumanía, Rusia, Polonia y otros. **Informes publicados recientemente:** • Descubriendo los patrones TTP de los actores y el papel del DNS en las estafas de inversión
	Este actor identifica recursos en la nube abandonados y los reutiliza para actividades maliciosas varias. Hasty Hawk es conocido por secuestrar dominios que se utilizan en campañas temáticas de beneficencia y DHL, distribuidas a través de anuncios de Google. Hasty Hawk utiliza principalmente redes de alojamiento “a prueba de balas”, como Proton66, junto con un TDS para dirigir a los usuarios hacia el contenido. **Informes publicados recientemente:** • Los depredadores del DNS secuestran dominios para abastecer su infraestructura de ataque
	Vacant Viper opera el 404TDS, que utiliza para distribuir malware y otro contenido malicioso. Vacant Viper secuestra dominios convertidos en vulnerables debido a servidores del DNS mal configurados —fallo que los investigadores de Infoblox denominan “Sitting Ducks”— y los incorpora a su infraestructura de TDS maliciosa. **Informes publicados recientemente:** • ¿Quién lo hubiese dicho? Secuestrar dominios es muy fácil
	Este actor de adtech malicioso aprovecha las vulnerabilidades de WordPress y distribuye malware, páginas de phishing, aplicaciones falsas y contenido no deseado. Ejecuta un TDS extenso que incorpora notificaciones push, ventanas emergentes y redireccionamientos dentro de un navegador, y sirve anuncios incluso después de que el usuario abandone la página inicial. **Informes publicados recientemente:** • Lo molesto y lo malicioso: la inquietante relación entre los hackers de WordPress y una camarilla de adtech

Morphing Meerkat es un actor global de spam que está detrás de una avanzada plataforma de phishing como servicio (PhaaS). Este actor utiliza registros MX del DNS para identificar el proveedor de correo electrónico de la víctima y mostrarle dinámicamente páginas de inicio de sesión falsas. Morphing Meerkat se aprovecha de sitios web de WordPress comprometidos, así como de las vulnerabilidades de redireccionamiento abierto en servidores de adtech.

Informes publicados recientemente:

- Un relato de phishing sobre el abuso de DOH y DNS MX

ESTUDIO DE CASO: COORDINACIÓN ENTRE HACKERS DE WORDPRESS Y LA CAMARILLA VEXTRIO VIPER

Infoblox ha descubierto recientemente una compleja alianza entre hackers de **WordPress y una red de empresas de adtech malicioso**, entre las que destaca TDS de VexTrio.

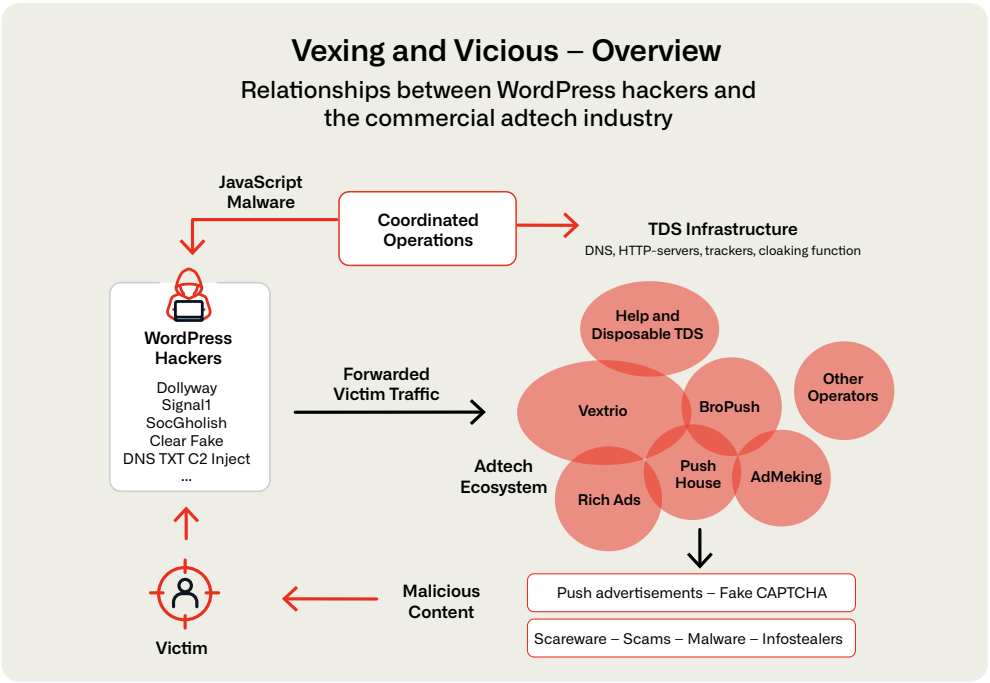


Figura 1. Relación entre los hackers de WordPress y la industria de adtech comercial

¿Qué sucedió?

- **Migración rápida:** cuando se desmanteló el TDS de VexTrio en otoño de 2024, varios actores maliciosos pasaron a la vez a un TDS aparentemente nuevo llamado “Help TDS”. Un análisis más detallado reveló que Help TDS no es independiente, sino que está estrechamente vinculado a VexTrio, con el que comparte infraestructura y componentes de software.
- **Operación coordinada:** Infoblox analizó 4,5 millones de respuestas de registros TXT del DNS de sitios web comprometidos durante seis meses, lo que reveló dos servidores de mando y control (C2) distintos, ambos alojados en una infraestructura conectada a Rusia, lo que indica una operación coordinada entre los hackers de WordPress y la camarilla de VexTrio.

- **Participación de empresas de adtech comercial:** Se descubrió que varias empresas de adtech, entre ellas Los Pollos, Partners House, BroPush y RichAds, estaban vinculadas a las operaciones de VexTrio. Estas empresas facilitaban la distribución de contenido malicioso a través de enlaces inteligentes y notificaciones push.

La investigación pone de relieve la naturaleza sofisticada y adaptable de las redes de ciberdelincuencia que se aprovechan de sitios web de WordPress comprometidos e infraestructuras de adtech comercial. También subraya la importancia de la telemetría del DNS y los esfuerzos de colaboración para descubrir y mitigar este tipo de amenazas.

SECCIÓN 3: TÉCNICAS MALICIOSAS DEL DNS

Los actores maliciosos mencionados en la sección 2 utilizan el DNS de diversas maneras y con objetivos específicos. Una vez que Infoblox descubre un dominio relacionado con una amenaza, los procesos de análisis y las revisiones de expertos asignan las técnicas maliciosas conocidas al dominio. La tabla siguiente ofrece una descripción general de las técnicas del DNS más comunes asignadas por Infoblox Threat Intel a los dominios relacionados con amenazas.

Técnicas del DNS y dominios relacionados con amenazas Periodo: de enero de 2025 a junio de 2025	
Dominios generados por algoritmos de máquinas (RDGA, DDGA y DGA)	54,7 %
Dominios utilizados para redirigir el tráfico	11 %
Dominios CNAME o alias	5,8 %
Dominios similares	5,1 %
Dominios secuestrados	5,1 %
Dominios utilizados en SMS maliciosos	4,2 %
Dominios creados como parte de un TDS	1,8%
Dominios utilizados para C2 y exfiltración	< 0,4 %

Tabla 2. Técnicas de DNS asignadas a dominios relacionados con amenazas

Muchas de estas técnicas se solapan durante una campaña de amenazas y pasan a formar parte de tácticas más amplias de los actores para alcanzar sus objetivos. En este informe, profundizamos en cuatro técnicas del DNS comunes, cómo se utilizan y por qué son peligrosas:

- Uso de dominios dentro de TDSs
- Secuestro de dominios para robar confianza
- Dominios similares para engañar a las víctimas
- Tunelización del DNS para C2 y exfiltración

LOS SISTEMAS DE DISTRIBUCIÓN DEL TRÁFICO PROPORCIONAN UN NIVEL DE EVASIÓN PELIGROSO

El DNS desempeña un papel fundamental en los TDS, al redirigir de forma encubierta a los usuarios a través de múltiples capas intermedias, a menudo sin su conocimiento, basándose en diversos atributos como la geolocalización, el tipo de dispositivo o la postura de seguridad. El DNS desempeña un papel fundamental a la hora de determinar cómo y adónde se enruta el tráfico de red. Los operadores de TDS legítimos se encuentran sobre todo en publicidad digital o adtech. El nombre "adtech" (abreviatura de "tecnología publicitaria") se refiere a las herramientas, las plataformas y el software utilizados para gestionar, distribuir y analizar campañas de publicidad digitales.

Al igual que la tecnología publicitaria legal conocida (p. ej., Google AdSense), el adtech malicioso distribuye el contenido adecuado al público indicado en el momento preciso para aumentar la eficacia de sus campañas. Este tipo de ciberamenaza corre a cargo de organizaciones especializadas con muchos afiliados y elevados recursos económicos.

Principales operadores de TDS por cuota de conexión	
Nombre del actor	**Conexión compartida**
Vextrio Viper	72,8 %
Vane Viper	68,4 %
Venal Viper	72,5 %
Actor no revelado	64,8 %
Vero Viper	60,5 %
Tiano Gambling	50,9 %

Tabla 3: Operadores de TDS y porcentaje de intentos de conexión de clientes recibidos

En el centro de estas actividades se encuentra un TDS que segmenta a las víctimas y las dirige a anunciantes maliciosos, al tiempo que envía a los investigadores de amenazas a un sitio web señuelo.

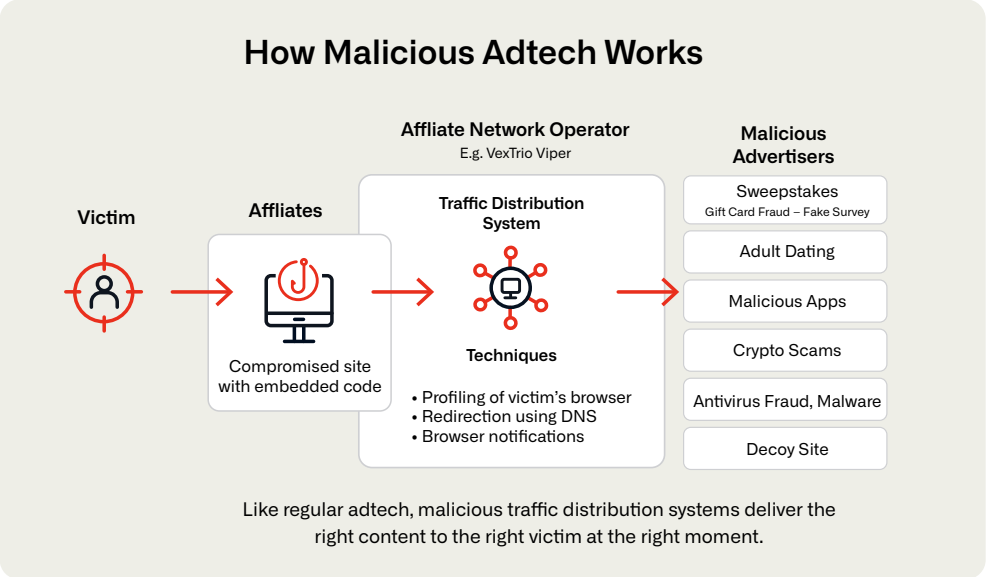


Figura 2: Visión general de los tres actores del adtech malicioso: afiliados, operadores y anunciantes maliciosos

Existen múltiples razones por las que la tecnología publicitaria maliciosa es perjudicial y debería ser un área importante de enfoque para los equipos de seguridad empresarial:

El adtech malicioso es un vector de amenazas infracomunicado y de rápido crecimiento

Los atacantes se aprovechan cada vez más de redes publicitarias maliciosas como servicio de bajo coste para distribuir malware y otros contenidos maliciosos. Estos anuncios pueden dar lugar a diversos tipos de ataques, como descargas inadvertidas, sitios de phishing, ladrones de credenciales y kits de explotación (véase la tabla 4: Operadores de TDS y contenido malicioso entregado).

Dado que la mayor parte del sector de la seguridad se basa en un enfoque de "paciente cero", que consiste en recopilar telemetría durante (p. ej., mediante sandboxing) o después (p. ej., mediante inteligencia forense) de un ataque, las contramedidas resultantes se limitan a lo descubierto desde el instante de compromiso inicial. Esta limitación hace que los TDS sean herramientas eficaces para evadir la detección, ya que los actores alteran continuamente el contenido malicioso que distribuyen, y redirigen a los investigadores de amenazas a sitios web señuelo. En consecuencia, los TDS se han convertido en una de las amenazas menos comunicadas en el sector de la ciberseguridad.

Infraestructuras a gran escala, difíciles de interrumpir

Las organizaciones que operan con adtech malicioso suelen crear infraestructuras a gran escala, que incluyen decenas de miles de dominios que cambian rápidamente, diseñados para redirigir a los usuarios y convencerlos de que acepten notificaciones push del navegador. Estas operaciones suelen subdividirse en múltiples entidades para llevar a cabo ciberdelitos y evitar el escrutinio legal. Algunos operadores, como VexTrio Viper, llevan años en activo y han alcanzado una gran rentabilidad, sin que sus actividades den señales de detenerse.

El adtech malicioso sirve como puerta de entrada al riesgo empresarial

El adtech malicioso engaña a las víctimas imitando marcas populares u ofreciéndoles contenidos a los que desean acceder, lo que las lleva a bajar la guardia y participar en interacciones de alto riesgo. Aunque estas amenazas suelen tener su origen en sitios web dirigidos a consumidores, pueden infiltrarse fácilmente en entornos corporativos, exponiendo los dispositivos personales de los empleados a contenidos maliciosos. Este método permite a los actores maliciosos llevar a cabo reconocimientos o suplantar notificaciones de la empresa, lo que aumenta el riesgo para las redes de una organización.

Operadores del DNS	Software malicioso	Estafas	Phishing	Dominio secuestrado
Vacant Viper	X	X		X
Vane Viper	X	X	X	
Vextrio Viper	X	X	X	X
Hasty Hawk			X	X
Sophisticated Chickens			X	X
Black TDS	X		X	
Parrot TDS	X			
R0bl0ch0n TDS		X		

Tabla 4. Operadores de TDS y contenido malicioso entregado

Ejemplo de TDS en funcionamiento:

Cuando una víctima visita un sitio comprometido desde un dispositivo móvil o un punto de conexión, el operador puede presentar un CAPTCHA falso para engañarla y forzarla a aceptar notificaciones push de un anunciante malicioso en el navegador. Estas notificaciones pueden distribuir contenido fraudulento adicional, como solicitudes para descargar software no verificado, compartir información personal o introducir las credenciales de la organización.

Cuando el TDS segmenta a las víctimas entrantes, es posible que los analistas del SOC o los investigadores de amenazas que utilizan herramientas de seguridad comunes no detecten estas notificaciones o contenidos maliciosos, sino que sean redirigidos a un sitio web falso que muestra material legítimo.

Debido a la superposición entre el uso profesional y personal de internet, la tecnología de publicidad maliciosa se ha convertido en un factor importante que contribuye a la ciberdelincuencia, especialmente en dispositivos móviles, tabletas, BYOD y activos desprotegidos.

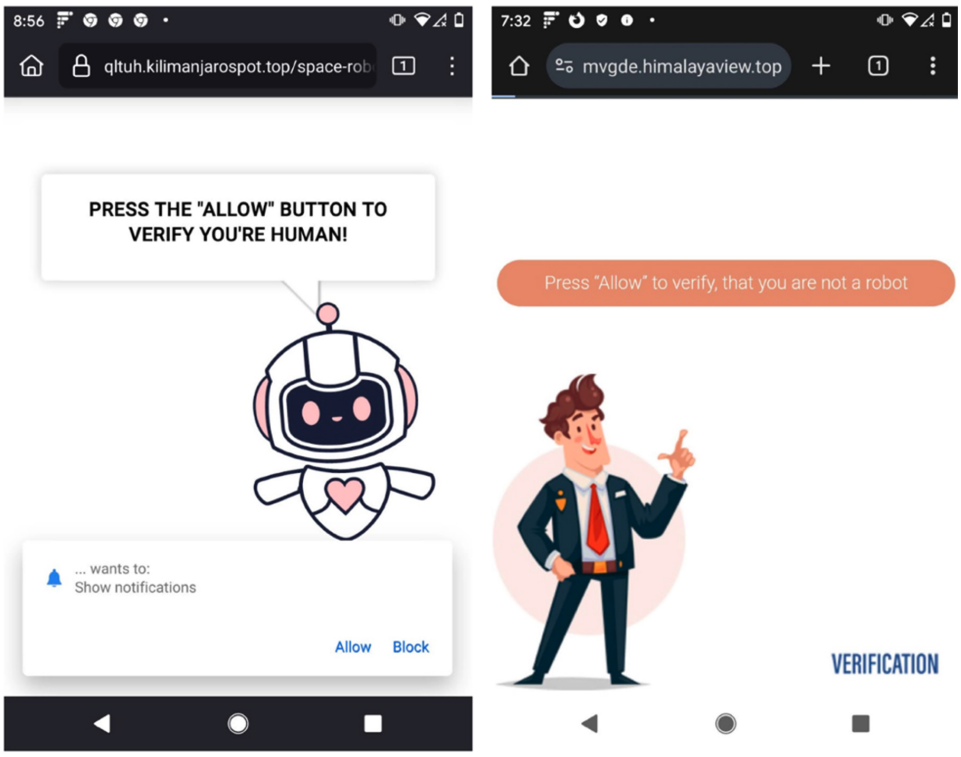


Figura 3: Ejemplos de la página de destino de VexTrio Viper, que lleva al usuario a aceptar notificaciones push en su equipo; ambos se vieron al navegar por `germannautica[.]com`

Dominios utilizados por los sistemas de distribución de tráfico

En los últimos 12 meses, Infoblox Threat Intel ha descubierto más de un millón de indicadores utilizados por 168 operadores de adtech malicioso en su TDS. Estos indicadores abarcan múltiples técnicas, entre las que se incluyen RDGA, redirecciones, dominios secuestrados, similares y otros.

Los TDS utilizados por los operadores de adtech malicioso pueden ser extensos. Muchos incluyen más de 10.000 dominios, y algunos superan los 100.000. Sin embargo, el tamaño de un TDS no se correlaciona necesariamente con su prevalencia o nivel de amenaza. Vigorish Viper opera una vasta red en crecimiento de 170.000 dominios activos, pero se centra principalmente en víctimas de China, Hong Kong y Macao. Venal Viper, aunque no se halla entre los cinco primeros en tamaño, es uno de los más consultados en las redes de clientes: el 65% de todos los clientes de Infoblox han consultado un dominio de Venal Viper en los últimos 12 meses.

Interrupción de los TDS

El adtech malicioso que utiliza TDS prospera porque se disfraza de publicidad legítima, engaña a las víctimas y evade la detección de las herramientas de seguridad que se basan en la identificación de conductas maliciosas conocidas a través de simulaciones o datos de pacientes cero. Por el contrario, los registros del DNS pueden revelar cuándo y cómo se configura una nueva infraestructura maliciosa.

Los investigadores que aprovechan los datos del DNS históricos y en tiempo real, combinados con ciencia de datos innovadora, pueden identificar dominios sospechosos o maliciosos antes de que se suministre cualquier carga útil, incluidas las utilizadas en adtech malicioso.

La inteligencia derivada del DNS arroja luz sobre la infraestructura que respalda una amenaza, como el funcionamiento del TDS y la forma en que redirige el tráfico. A diferencia de otras metodologías de seguridad, las implementaciones basadas en el DNS pueden descubrir adtech malicioso de forma proactiva y evitar que los puntos de conexión a internet interactúen con él.

En pocas palabras, al centrarse en la infraestructura del atacante, la protección basada en el DNS rompe la cadena de suministro entre los anunciantes maliciosos y las víctimas, ofreciendo protección a largo plazo, en lugar de limitarse a reaccionar ante las últimas cargas útiles.

SECUESTRO DE DOMINIOS PARA ROBAR CONFIANZA

Los actores de amenazas secuestran dominios existentes, en su mayoría para explotar la credibilidad y la confianza asociadas a los dominios legítimos. Una vez bajo el control del adversario, los dominios secuestrados pueden utilizarse para crear sitios de phishing convincentes, obtener prioridad en los motores de búsqueda, eludir los filtros de spam o ejecutar fraudes.

Infoblox Threat Intel descubrió múltiples formas en que los actores secuestran dominios y las herramientas que utilizan para engañar a los usuarios.

Ataques “Sitting Ducks”

Los ataques “Sitting Ducks” han ganado prevalencia en los últimos años. En 2024, Infoblox Threat Intel estimó que más de **un millón de dominios eran vulnerables a este ataque**. Durante una investigación en profundidad efectuada en la segunda mitad de 2024, **se descubrieron 70.000 dominios secuestrados de un total de 800.000** dominios vulnerables, lo que pone de relieve la magnitud del problema y la necesidad de adoptar medidas de seguridad sólidas.

Múltiples actores de amenazas utilizan estas técnicas de forma sistemática. La facilidad con la que se pueden ejecutar estos ataques, combinada con la dificultad que tienen los equipos de seguridad para detectarlos, los hace especialmente peligrosos.

Entre los actores que se sabe que explotan este ataque se encuentran VexTrio Viper, Vigorish Viper, Horrid Hawk y Hasty Hawk. Estos grupos han demostrado la eficacia de los ataques Sitting Ducks, lo que subraya la necesidad de aumentar la vigilancia y mejorar las prácticas de seguridad para contrarrestarlos.

CNAMES colgantes

A principios de 2025, actores de amenazas aprovecharon configuraciones de redireccionamiento en dominios de gran reputación, como `cdc[.]gov` y varias universidades estadounidenses, lo cual fue posible porque las organizaciones habían desactivado aplicaciones en la nube (p. ej., CDN) alojadas por proveedores externos (como Microsoft Azure) y habían dejado activos sus alias del DNS (registros CNAME).

Los actores de amenazas como Hazy Hawk aprovecharon este fallo en la higiene del DNS para crear nuevo contenido en la misma CDN. El motivo era sencillo: al aprovechar la reputación del alias del dominio original, podían engañar a Google y a otros motores de búsqueda para que indexaran el contenido malicioso y lo incluyeran en los resultados de búsqueda.

LOS DOMINIOS SIMILARES Y CON ERRORES TIPOGRÁFICOS ENGAÑAN A LOS USUARIOS

Los dominios similares son nombres de dominio ligeramente modificados que se registran para engañar a los usuarios. A menudo suplantan marcas legítimas, comunicaciones de empleados, cadenas de suministro u otros socios de confianza, lo que provoca problemas importantes.

Los atacantes utilizaron dominios similares en mensajes SMS, llamadas telefónicas, mensajes directos en redes sociales, correos electrónicos y códigos QR. Recientemente, se han centrado en la autenticación multifactorial (MFA), debido a su creciente adopción por parte de todo tipo de usuarios, desde jugadores hasta compradores de criptomonedas. Otros ejemplos incluyen eludir la MFA empresarial o el abuso de nombres de dominio correspondientes a plataformas de acceso de identidad populares.

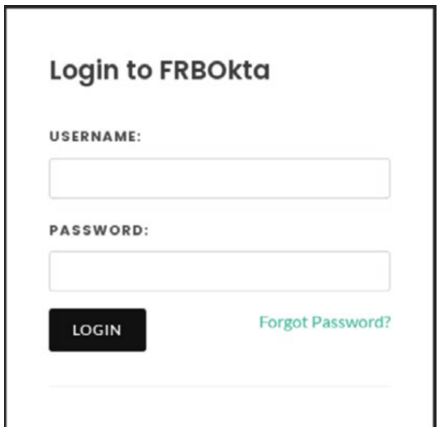


Figura 4. Mensaje de MFA desde un dominio similar

Los dominios similares se han convertido en un problema mucho mayor, ya que existen más de **1.500 dominios de nivel superior, lo que aumenta los costes para la mayoría de las organizaciones a la hora de supervisar todas las variantes.**

Además, en una organización puede haber varios grupos que registran dominios y faltar visibilidad sobre quién hace qué. Los equipos de seguridad pueden pensar que un dominio de aspecto similar ha sido creado por el servicio de asistencia técnica o el equipo de aplicaciones en la nube, pero en realidad el nuevo dominio puede haber sido configurado por un actor para suplantar su identidad ante los clientes.

La falta de experiencia de los equipos de seguridad a menudo les lleva a optar por soluciones rápidas a través de servicios gestionados. Desgraciadamente, los dominios similares no son un problema de fácil resolución. Incluso los equipos de seguridad más experimentados siguen encontrándose con ellos y su supervisión eficaz requiere una gran diligencia.

Infoblox: Técnicas de imitación identificadas	
	**Los homógrafos u homoglifos** utilizan caracteres visualmente similares de conjuntos de caracteres diferentes, como el alfabeto cirílico o el griego (p. ej., sustituyendo “O” por “0”). La técnica es eficaz porque los caracteres insertados no siempre se distinguen claramente.
	**Los typosquats** incluyen errores tipográficos engañosos mediante el registro de dominios muy similares a sitios web populares (p. ej., “`amazonn[.]com`” en lugar de “`amazon[.]com`”) para llevar a los usuarios a un sitio web fraudulento.
	**Los combosquats** combinan nombres de marcas o empresas conocidas con otras palabras clave, como “correo”, “seguridad” o “soporte”. El combosquatting es aproximadamente 100 veces más frecuente que el typosquatting.
	**Los soundsquats** son la forma más reciente de amenazas similares, que utilizan nombres de dominio que suenan similares cuando se pronuncian en voz alta (p. ej., “`hsbsee[.]com`” en lugar de “`hsbc[.]com`”). Engañan a los usuarios cuando utilizan dispositivos inteligentes, como Google Home, Siri y Alexa.

LA TUNELIZACIÓN DE DNS UTILIZADA POR ACTORES DE AMENAZAS, PENTESTERS Y HERRAMIENTAS DE SEGURIDAD LEGÍTIMAS

La tunelización del DNS codifica los datos dentro de las consultas y respuestas del DNS, lo que permite una comunicación encubierta que a menudo se aprovecha para operaciones C2 y exfiltración de datos.

Mientras que Infoblox observó más de 480 dominios únicos de tunelización del DNS en algunos meses, entre junio de 2024 y junio de 2025 se descubrieron una media de más de 100 dominios únicos relacionados con la tunelización del DNS al mes. Más allá de su uso por parte de los ciberdelincuentes, la tunelización del DNS también se utiliza en pruebas de penetración legítimas y en herramientas de seguridad. La siguiente lista ofrece una visión general de las herramientas de tunelización del DNS más habituales con capacidades C2.

+100

unique DNS tunneling domains found monthly—benign and malicious

- **Cobalt Strike** es una herramienta de pruebas de penetración muy utilizada por equipos rojos y actores maliciosos, que cuenta con un módulo C2 del DNS. Emplea consultas codificadas en hexadecimal con prefijos personalizables opcionales como “post”, “api” o “dx”.
- **Dnscat2** es una herramienta que sirve para crear túneles del DNS cifrados. Se incluye en METASPLOIT, herramienta de pruebas de penetración de código abierto.
- **DNS Exfiltrator** es una herramienta que codifica datos en consultas al DNS para su exfiltración, lo que ilustra el posible uso indebido del DNS en escenarios prácticos. Utiliza registros TXT, permite solo la comunicación unidireccional y se inicia a través de la línea de comandos. Infoblox no ha observado su uso por parte de ningún actor malintencionado y lo considera poco práctico debido a su mecanismo unidireccional.
- **Sliver** es un marco C2 multiplataforma con capacidades de tunelización del DNS, utilizado con frecuencia en simulaciones de adversarios y campañas maliciosas.
- **Weasel** es una herramienta de tunelización del DNS menos documentada, desarrollada por el equipo rojo de Facebook, que admite la exfiltración sigilosa de datos y C2. Se utiliza habitualmente en operaciones de equipos rojos especializados y emplea registros A y AAAA para las comunicaciones.
- **Pupy** es una herramienta de acceso remoto de código abierto y multiplataforma con soporte para tunelización del DNS, utilizada históricamente en campañas de espionaje contra entidades gubernamentales y corporativas. Utiliza registros A para las comunicaciones.
- **Iodine** es una conocida herramienta para tunelizar tráfico IPv4 a través del DNS, utilizada en pruebas de penetración y, en ocasiones, de forma indebida en ataques, por ejemplo, por parte de actores estatales con intenciones C2. Iodine utiliza registros A, TXT, CNAME y MX para comunicarse.
- **Recientemente han aparecido varias herramientas de pruebas de penetración automatizadas**, de proveedores como Cymulate y AttackIQ. Infoblox ha descubierto dominios relacionados con estos proveedores en redes de sus clientes.
- **Las herramientas antivirus y antispam** también utilizan el DNS como mecanismo para ver si un dominio o un hash de archivo puede ser malicioso. Una consulta puede tener el formato: “<domain>.<guid>.<avdomain>” o “<file hash>.<guid>.<avdomain>, y la respuesta será NXDOMAIN si el dominio o el hash del archivo no se encuentran en una lista conocida de malware o spam, o 127.0.0.X si se encuentran en dicha lista.

Los equipos de seguridad necesitan un bisturí para detener la tunelización del DNS

Comprender y mitigar la tunelización del DNS es esencial para proteger a las empresas frente a las ciberamenazas y garantizar el cumplimiento de los requisitos normativos, como la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) y el Reglamento General de Protección de Datos (RGPD). Debido al uso generalizado de las herramientas de tunelización del DNS, muchos equipos de seguridad tienen dificultades para supervisar y controlar eficazmente el tráfico del DNS.

Infoblox detecta a menudo la tunelización del DNS en redes, incluso en aquellas que cuentan con firewalls de última generación o tecnologías de tipo Secure Access Service Edge (SASE). Aunque estas tecnologías han mejorado en la detección de la tunelización del DNS, siguen existiendo complejidades. Las CDN, el uso de nuevos dominios similares y la expansión de herramientas DNS C2 legítimas complican la detección y el bloqueo de todas las actividades C2.

Como resultado, los equipos de seguridad necesitan herramientas precisas y específicas, en lugar de medidas amplias y generalizadas. Para hacer frente a este reto, son esenciales las soluciones de DNS protectoras que aprovechan el seguimiento activo de los actores maliciosos y las técnicas de aprendizaje automático continuamente actualizadas.

SECCIÓN 4: DESAFÍOS PARA LOS DEFENSORES

Además de las técnicas del DNS adversarias tradicionales, como los TDS, el secuestro de dominios, los dominios similares y la tunelización del DNS, los defensores —ya sean analistas del SOC, gestores de riesgos o CISO— se enfrentan a una serie de retos cada vez mayores.

Esta sección ofrece una visión general de las tendencias clave, como el uso de la IA adversaria, la protección de la marca y la creciente presión de las nuevas normas de cumplimiento. Y lo que es más importante, destaca las oportunidades que ofrece la inteligencia de amenazas derivada del DNS para combatir estos retos.

88%

of AI-generated malware evades detections[4]

LA IA ADVERSARIA ELUDE LOS CONTROLES DE SEGURIDAD EXISTENTES

La IA generativa (GenAI) —en particular, los modelos de lenguaje extensos (LLM)— está impulsando una transformación en ciberseguridad. Los adversarios se sienten cada vez más atraídos por la GenAI porque reduce la barrera para crear contenido engañoso y convincente. La utilizan para mejorar la eficacia de técnicas de intrusión como la ingeniería social y la evasión de la detección.

Para compensar estos nuevos retos de la IA, los equipos de seguridad necesitan un nuevo nivel de veracidad, como la telemetría basada en el DNS, que no pueda ser alterada u ofuscada por la IA y que proporcione suficiente transparencia en la cadena de custodia.

Ejemplos recientes de IA maliciosa: en estafas con deepfakes

A finales de 2024, el FBI advirtió que los criminales se utilizaba IA generativa para cometer fraudes a gran escala, lo que hacía que sus estratagemas fueran más creíbles.[5] Las herramientas de GenAI, como la clonación de voz, reducen significativamente el tiempo y el esfuerzo necesarios para engañar a los objetivos con mensajes de audio aparentemente fiables. Es especialmente preocupante la facilidad con la que los ciberdelincuentes pueden acceder a estas herramientas, junto con la falta de medidas de seguridad. La clonación de voz se ha utilizado en diversos escenarios, como vídeos deepfake a gran escala para estafas con criptomonedas y la imitación de voces durante llamadas telefónicas a destinatarios seleccionados.

Caso práctico: Reckless Rabbit utiliza deepfakes para atacar a víctimas de habla japonesa

Infoblox Threat Intel informó en septiembre de 2024 de una campaña de secuestro de cuentas de YouTube que utilizaba vídeos deepfake de Elon Musk para estafas con criptomonedas. Una técnica similar ha sido adoptada ahora por un actor rastreado conocido como **Reckless Rabbit**, que incrusta deepfakes directamente en sitios web fraudulentos.

Reckless Rabbit ha cambiado recientemente su enfoque hacia los **usuarios de habla japonesa**, promocionando planes de inversión falsos a través de artículos de noticias generados por IA. Estos sitios web incluyen vídeos deepfake de personajes públicos, como **Elon Musk** y **Masayoshi Son,** junto con reseñas positivas falsas para aumentar su credibilidad.

---

4 Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud. FBI Alert Number: I-120324-PSA, 3 de diciembre de 2024

5 AI Could Geneate 10,000 Malware Variants, Evading Detection in 88% of Case, Lakshmanan, Ravie, The Hacker News, 23 de diciembre de 2024.

Anteriormente, el actor se dirigía a **usuarios de Europa del Este** utilizando dominios basados en RDGA y anuncios de Facebook para atraer a las víctimas hacia contenidos de noticias falsas compuestos por texto sencillo e imágenes.

Figura 5. Página deepfake descubierta recientemente

Reckless Rabbit utiliza artículos falsos con vídeos deepfake y **subtítulos en japonés**, suplantando a importantes medios de comunicación como Yomiuri Shimbun. Estos artículos promocionan una plataforma de inversión falsa llamada **"Finance Legend"** con un botón de registro que redirige a un formulario de contacto. Es probable que el actor contacte luego con las víctimas para solicitarles depósitos, prometiéndoles altos rendimientos.

Chatbots impulsados por inteligencia artificial

Los actores suelen seleccionar cuidadosamente a sus víctimas y recopilar información sobre sus intereses, lo que les permite preparar estafas muy personalizadas. Tras un reconocimiento inicial, elaboran mensajes de smishing que conducen a las víctimas a conversaciones impulsadas por chatbots. Estas conversaciones pueden prolongarse durante semanas e incluir pasos inusuales, como pedir un "me gusta" en YouTube o una republicación en las redes sociales, tácticas diseñadas para evaluar la susceptibilidad de la víctima. Con cada interacción positiva, el actor manipula un "saldo de cuenta" falso para que aumente. Cuando la víctima intenta retirar el dinero, el actor solicita acceso a su cuenta de criptomonedas, abusando de la confianza construida a lo largo del tiempo para robar los fondos de la víctima. Los chatbots impulsados por IA permiten a los actores automatizar estas conversaciones y ampliar sus operaciones de manera eficiente.

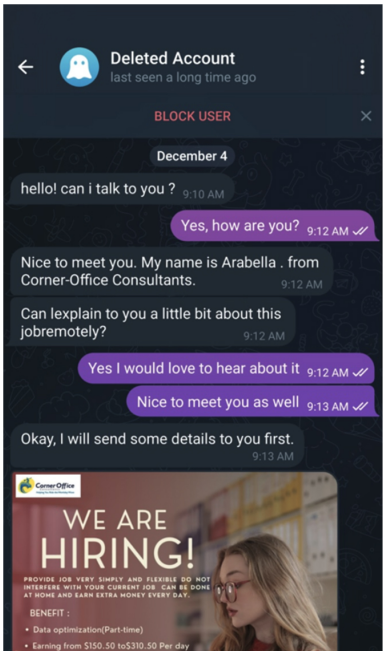


Figura 6. Ejemplo de mensajería de chat adversario, utilizando una combinación de IA/LLM junto con interacciones semiautomáticas de chatbots.

Ofuscación y evasión de código

Los actores de amenazas utilizan cada vez más GenAI para ofuscar, reutilizar y ensamblar software malicioso de nuevas formas con vistas a evadir la detección. Este enfoque acelera la creación de campañas de amenazas y reduce las habilidades técnicas necesarias para construir cadenas de infección eficaces. Según una investigación de HP Wolf Security, la evasión de amenazas basadas en el correo electrónico ha aumentado aproximadamente un 11%.[6] Mientras tanto, un destacado proveedor de seguridad informó recientemente de que un algoritmo LLM codicioso cambiaba el veredicto de su propio modelo clasificador de malware de malicioso a benigno en el **88%** de los casos,[7] un indicador significativo de la eficacia con la que la IA adversaria puede explotar los modelos de detección actuales.

PROTEGER LA REPUTACIÓN DE LA MARCA Y LA ORGANIZACIÓN

La reputación de las marcas y las organizaciones es un activo estratégico. Una reputación sólida genera confianza en los clientes, mejora la credibilidad en el mercado, atrae socios e inversores y respalda el valor de la marca a largo plazo. Según Forbes, "los líderes empresariales consideran sistemáticamente la reputación como su activo más valioso".[8] Sin embargo, proteger una marca dentro del DNS presenta varios retos:

- **Visibilidad limitada más allá del perímetro:** la supervisión de dominios requiere el seguimiento no solo de los dominios propios, sino también de miles de posibles dominios similares o suplantaciones. Por ejemplo, Infoblox detectó 28.331 dominios similares en mayo de 2025.
- **Los dominios similares creados por personas siguen siendo difíciles de detectar:** los dominios similares son seleccionados e imitados cuidadosamente por personas, lo que a menudo supera la capacidad de detección de los sistemas automatizados.
- **La supervisión manual de dominios agota los recursos:** los equipos de seguridad suelen carecer de los recursos necesarios para supervisar manualmente las alertas y responder de forma eficaz. Sin automatización, la supervisión de dominios se convierte en una tarea poco eficiente que requiere mucho esfuerzo.
- **Las barreras jurisdiccionales dificultan la aplicación de la ley:** el 87% de los dominios de alto riesgo descubiertos están registrados con entidades sancionadas por la Oficina de Control de Activos Extranjeros (OFAC), donde no se aplican las leyes de Estados Unidos o de la Unión Europea (UE).

28,331
lookalike domains detected by Infoblox in May 2025

Para superar estos obstáculos, los equipos de seguridad y marketing deben asociarse con expertos en el DNS que tengan una visibilidad profunda de su uso global y puedan beneficiarse de la inteligencia basada en el DNS. Esta colaboración les permite supervisar, detectar y corregir amenazas a los activos digitales que reflejan la reputación o la marca de la organización.

PRESIONES DE CUMPLIMIENTO Y DESAFÍOS DE DNS PARA LOS EQUIPOS DE SEGURIDAD

Los equipos de redes y seguridad se enfrentan a una presión cada vez mayor debido a la evolución de las mejores prácticas y a las nuevas normativas, como **la NIS2 de la UE** y **la NIST SP 800-81 Rev. 3**, que se aplican a todos los sectores y requieren una supervisión más amplia, incluida la infraestructura del DNS.

6 Hackers Use Image-Based Malware and GenAI to Evade Email Security, Coker, James, Infosecurity Magazine, 16 de enero de 2024.

7 AI Could Generate 10,000 Malware Variants, Evading Detection in 88% of Case, Lakshmanan, Ravie, The Hacker News, 23 de diciembre de 2024.

8 The Importance Of Brand Reputation: 20 Years To Build, Five Minutes To Ruin, Blanchard, Paul, Forbes, 27 de diciembre de 2019.

Estos marcos presentan varios retos:

- **Complejidad operativa:** NIS2 exige evaluaciones de riesgos, notificación de incidentes las 24 horas del día y supervisión continua, requisitos que resultan difíciles de cumplir para los equipos que carecen de visibilidad centralizada o automatización. NIST SP 800-81 Rev. 3 exige, además, la implementación de servidores del DNS dedicados y el cifrado del tráfico del DNS interno y externo.
- **Herramientas fragmentadas:** las herramientas existentes suelen estar fragmentadas entre entornos locales, en la nube y remotos, lo que crea discrepancias en las políticas y lagunas en la visibilidad. Las políticas del DNS (p. ej., las zonas de política de respuesta o RPZ) deben aplicarse de forma coherente para evitar interrupciones.
- **Recursos limitados:** los equipos del SOC se ven desbordados por el volumen de alertas y carecen de información contextual. El énfasis de NIS2 en la detección temprana y la respuesta rápida supone una carga adicional para equipos ya sobrecargados de por sí, especialmente los que carecen de visibilidad en la capa del DNS.
- **Restricciones presupuestarias:** el cumplimiento normativo requiere invertir en herramientas, formación y registros de actividad del DNS. Sin embargo, las organizaciones deben justificar estos costes en un contexto de presupuestos más ajustados, aunque registrar la actividad del DNS sea fundamental para el análisis forense y la respuesta a incidentes.

Los equipos de seguridad precisan un enfoque sencillo para atender los nuevos requisitos de cumplimiento normativo. La activación de la inteligencia predictiva sobre amenazas y la implementación de controles a nivel del DNS no solo simplifican el cumplimiento de la norma NIST SP 800-81 Rev.3 y NIS2, sino que también se alinean con marcos de seguridad más amplios, como el Marco de Ciberseguridad del NIST (CSF) y la confianza cero. Y lo que es más importante, se mejora la prevención global de amenazas y la visibilidad, y se reducen los esfuerzos de las operaciones de seguridad.

PRÓXIMOS PASOS

Infoblox ofrece a los profesionales de la seguridad múltiples opciones para explorar la inteligencia sobre amenazas elaborada por expertos y proteger su entorno con inteligencia predictiva.

Para investigadores de amenazas:

- Obtenga más información sobre la investigación en https://www.infoblox.com/es/threat-intel/.
- Hable con nosotros en Mastodon en infobloxthreatintel@infosec.exchange.
- Acceda a nuestra investigación e indicadores en GitHub en https://github.com/infobloxopen/threat-intelligence/.

Para los equipos de seguridad:

- Solicite un taller de seguridad sobre el DNS en https://insights.infoblox.com/es-resources/esr/infoblox-workshop-security-workshop-es.
- Más información sobre Infoblox Threat Defense en https://www.infoblox.com/es/products/threat-defense/.

TERMINOLOGÍA UTILIZADA

Adtech: abreviatura de **tecnología publicitaria,** se refiere al **software, las herramientas y las plataformas** que utilizan las marcas, las agencias, los editores y las plataformas para planificar, ejecutar, gestionar y analizar **campañas publicitarias digitales.** Es la columna vertebral del ecosistema publicitario online.

BYOD: traiga su propio dispositivo

C2: mando (o comando) y control

CDN: una red de distribución de contenido es una **red de servidores distribuidos geográficamente** que trabajan juntos para entregar contenido digital (como sitios web, vídeos, imágenes y scripts) **de forma rápida, fiable y segura** a los usuarios en función de su ubicación.

CNAME: un registro de nombre canónico es un tipo de **registro del DNS** (**Domain Name System**) que **asigna un nombre de dominio** (**un alias**) **a otro nombre de dominio** (**el nombre canónico).** Se utiliza para redirigir un dominio o subdominio a otro dominio, en lugar de apuntar directamente a una dirección IP.

DDGA: algoritmo de generación de dominios de diccionario

DDI: **DNS, DHCP y gestión de direcciones IP** (**IPAM):** tres servicios de red críticos que funcionan conjuntamente para proporcionar **una gestión automatizada y centralizada de los espacios de direcciones IP y la resolución de nombres** en redes empresariales.

DGA: algoritmo de generación de dominios

DNS: Domain Name System (sistema de nombres de dominio)

Consultas al DNS: una **consulta al DNS** (consulta al Domain Name System) es una solicitud efectuada por un dispositivo (normalmente un ordenador o teléfono móvil) para traducir un **nombre de dominio legible por humanos** (como www.google.com) en una **dirección IP legible por máquinas** (como 142.250.190.68) para que pueda conectarse al servidor correcto en Internet.

RGPD: Reglamento General de Protección de Datos

HIPAA: Ley de Portabilidad y Responsabilidad del Seguro Médico estadounidense

LLM: modelo extenso de lenguaje

MFA: autenticación multifactor

Abuso de MX: se trata de actividades maliciosas que explotan o hacen un uso indebido de los registros MX (intercambio de correo).

NIST: Instituto Nacional de Estándares y Tecnología

NOD: dominios recién observados

OFAC: **Oficina de Control de Activos Extranjeros**, división del **Departamento del Tesoro de EE. UU.** Administra y aplica las **sanciones económicas y comerciales** basadas en la política exterior y los objetivos de seguridad nacional de Estados Unidos.

OSINT: inteligencia de fuentes abiertas

PCI DSS: norma de seguridad de datos de la industria de tarjetas de pago

PhaaS: phishing como servicio

RDGA: algoritmo de generación de dominios registrados

SASE: Secure Access Service Edge

TDS: sistema de distribución del tráfico

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

Versión: 20250730