Los actores maliciosos detrás del Servicio de Distribución de Tráfico VexTrio Viper (TDS) han sido vinculados con otros servicios similares como Help TDS y Disposable TDS, lo que indica que esta sofisticada operación cibercriminal funciona como una gran red dedicada a propagar contenido malicioso.

> *«VexTrio es un conjunto de compañías publicitarias maliciosas que difunden estafas y software dañino a través de distintos formatos de anuncios, incluyendo enlaces inteligentes (smartlinks) y notificaciones push,»* señaló Infoblox en un informe detallado.

Entre las empresas de tecnología publicitaria maliciosa que operan bajo VexTrio Viper se encuentran Los Pollos, Taco Loco y Adtrafico. Estas entidades forman parte de una red comercial de afiliados que conecta a actores de malware —cuyos sitios web son visitados por usuarios sin saberlo— con *"afiliados publicitarios"* que ofrecen diversas tácticas ilícitas como fraudes con tarjetas de regalo, aplicaciones maliciosas, páginas de phishing y estafas.

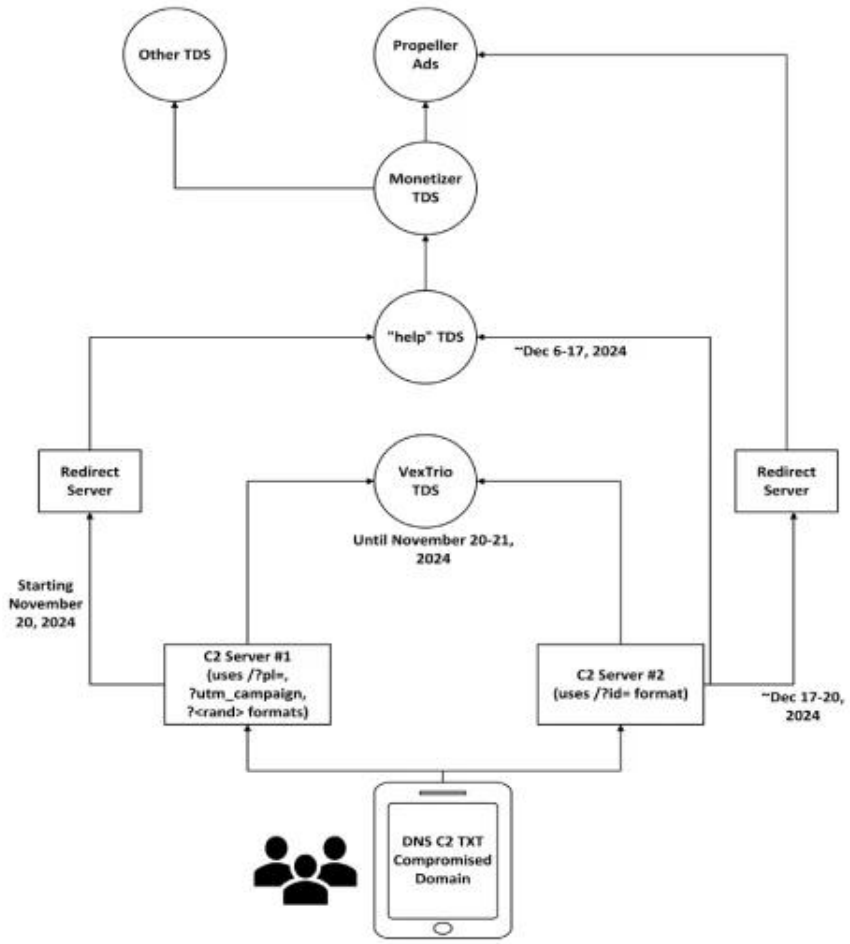
En otras palabras, estos sistemas de distribución de tráfico malicioso están diseñados para redirigir a las víctimas mediante enlaces inteligentes o promociones directas. Según la firma de inteligencia de amenazas DNS, Los Pollos recluta distribuidores de malware (también llamados afiliados publicadores) prometiendo ofertas lucrativas, mientras que Taco Loco se enfoca en monetización a través de notificaciones push y recluta afiliados en publicidad.

Un aspecto clave de estas campañas es la manipulación de sitios creados en WordPress para insertar código malicioso, encargado de iniciar la cadena de redirección que termina en la infraestructura de fraude de VexTrio. Algunos ejemplos de estos scripts son Balada, DollyWay, Sign1 y campañas usando registros DNS TXT.

> *«Estos scripts redirigen a los visitantes a diversas páginas fraudulentas mediante redes de intermediarios de tráfico relacionadas con VexTrio, una de las redes cibercriminales de afiliados más grandes conocidas, que utiliza técnicas avanzadas*

> *de DNS, sistemas de distribución de tráfico y algoritmos de generación de dominios para propagar malware y fraudes en redes globales,»* indicó GoDaddy en un informe publicado en marzo de 2025.

Las operaciones de VexTrio se vieron afectadas a mediados de noviembre de 2024, cuando Qurium reveló que la empresa suizo-checa Los Pollos formaba parte del ecosistema de VexTrio, lo que llevó a Los Pollos a interrumpir su servicio de monetización por enlaces push. Esta decisión provocó una migración masiva de cibercriminales que dependían de su red hacia servicios alternativos como Help TDS y Disposable TDS.



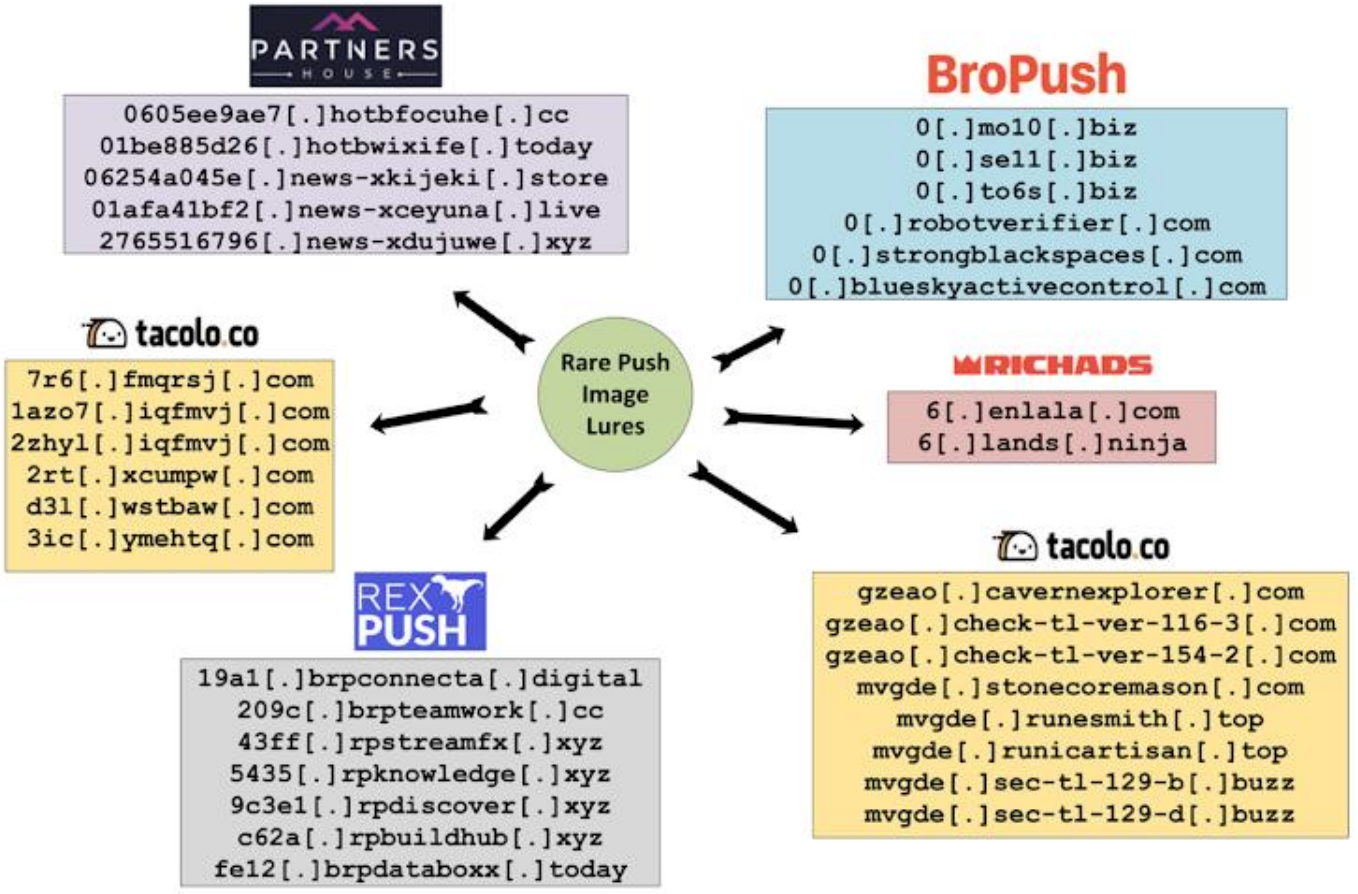
El análisis realizado por Infoblox de 4.5 millones de respuestas DNS TXT de sitios comprometidos durante seis meses reveló que los dominios utilizados en estas campañas podían agruparse en dos conjuntos, cada uno con su propio servidor de comando y control (C2).

> *«Ambos servidores estaban alojados en infraestructuras vinculadas a Rusia, pero no compartían ni el alojamiento ni las respuestas TXT. Cada conjunto utilizaba estructuras de URL de redirección diferentes, aunque ambos originalmente conducían a VexTrio y posteriormente a Help TDS«*, indicó la empresa.

Otras evidencias muestran que Help TDS y Disposable TDS en realidad son el mismo servicio, y que mantuvieron una *"relación exclusiva"* con VexTrio hasta noviembre de 2024. Help TDS, que anteriormente dirigía el tráfico hacia dominios de VexTrio, ha comenzado a utilizar Monetizer, una plataforma de monetización que emplea tecnología TDS para conectar tráfico web de afiliados con anunciantes.

> *«Help TDS tiene un fuerte vínculo con Rusia, ya que tanto el alojamiento como el registro de dominios suelen realizarse a través de entidades rusas. No cuenta con toda la funcionalidad avanzada del TDS de VexTrio y no tiene conexiones comerciales claras más allá de sus inquietantes lazos con VexTrio«*, dijo Infoblox, sugiriendo que sus operadores podrían actuar de forma independiente.

VexTrio es solo uno de varios servicios TDS que operan como compañías publicitarias comerciales. Otros ejemplos incluyen Partners House, BroPush, RichAds, Admeking y RexPush. Muchos de estos están orientados a servicios de notificaciones push, utilizando Firebase Cloud Messaging (FCM) de Google o scripts personalizados basados en la API Push para distribuir enlaces maliciosos por medio de notificaciones.



> *«Cientos de miles de sitios web comprometidos en todo el mundo redirigen cada año a las víctimas hacia la compleja red de VexTrio y sus afiliados,»* afirmó la empresa.
>
> *«VexTrio y las otras compañías de publicidad afiliada saben quiénes son los actores del malware, o al menos tienen suficiente información como para rastrearlos. Muchas de estas empresas están registradas en países que exigen algún grado de verificación de identidad (KYC), pero incluso sin esos requisitos, los afiliados publicadores son evaluados por sus gerentes de cuenta.»*