VexTrio's Affiliation with Website Malware Actors

blogs.infoblox.com/threat-intelligence/vexing-and-vicious-the-eerie-relationship-between-wordpress-hackers-and-an-adtech-cabal/

Infoblox Threat Intel June 12, 2025

Executive Summary

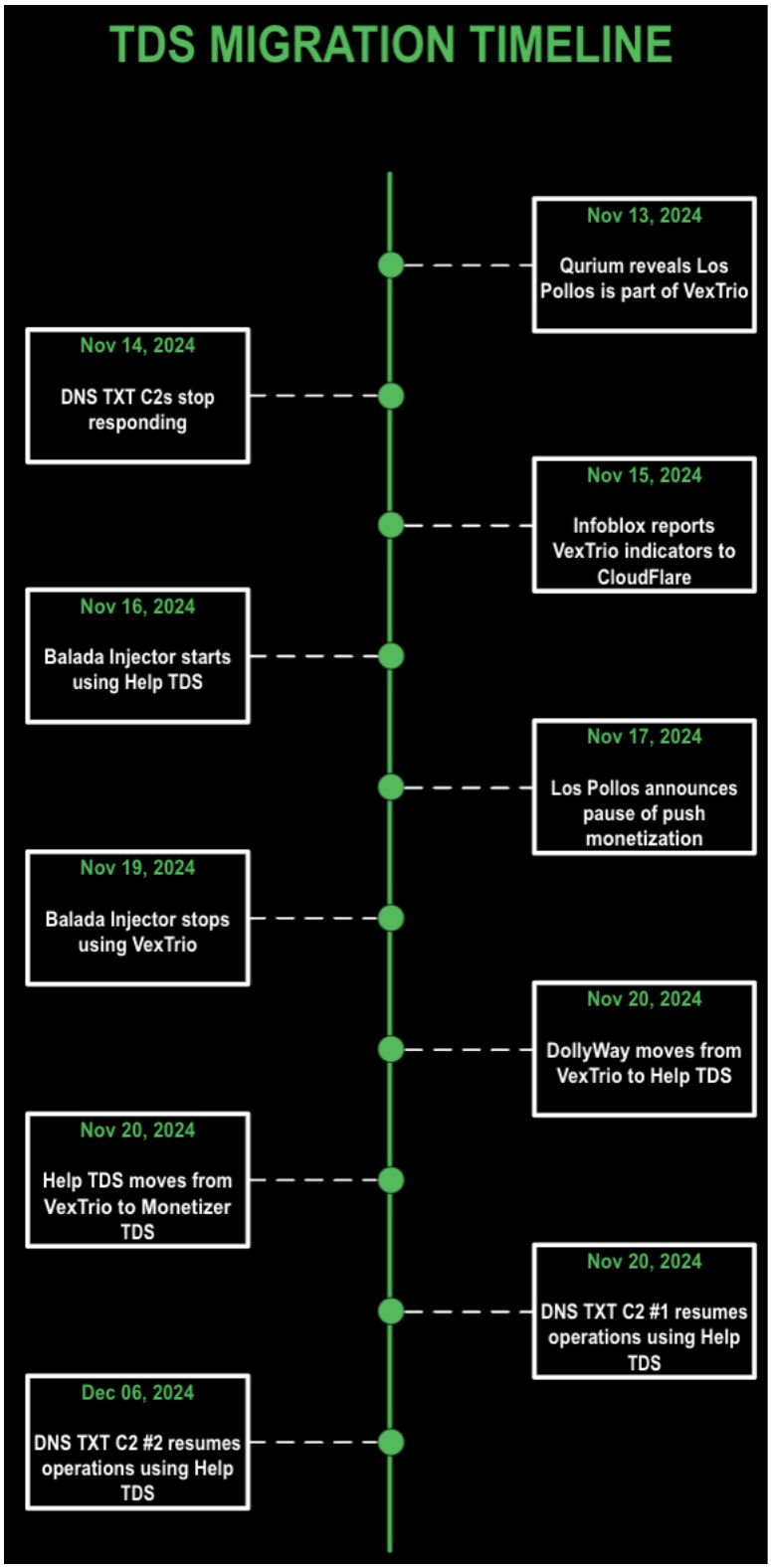
What started out as an observational study—perturb VexTrio and see how they adapt—led to a series of surprising revelations. When their traffic distribution system (TDS) was disrupted, multiple malware actors that depended on it all migrated to a "new" TDS, but it was the same TDS! Originally thought to be an independent TDS, we found evidence that suggested otherwise. Several commercial TDSs were discovered to share software elements with VexTrio and benefited from VexTrio's long, exclusive relationship with website malware actors. Finally, it became clear that the use of malicious adtech could be the downfall of dominant malware campaign operators, as the VexTrio cabal can identify them.

On November 13, 2024, Qurium researchers exposed that the Swiss-Czech adtech company Los Pollos was part of VexTrio, the largest and oldest known malicious TDS. Qurium made this connection after discovering that the Russian disinformation actor Doppelganger was using Los Pollos "smartlinks" in their operations. A few days later, we coordinated with Qurium and released a set of domains to a variety of security industry partners. We hoped this one-two punch would temporarily disrupt VexTrio and that we could gain a better understanding of their relationship to website malware actors by watching them recover.

We didn't have to wait long for a response. On November 17, Los Pollos announced that they would halt their so-called push link monetization; users were told that these links would deactivate "soon." But what does that really mean? As it turned out, within a few days, compromised websites all over the world that had been exploited with different WordPress vulnerabilities and ostensibly by different malware actors, were

updated in exactly the same way. For example, researchers at GoDaddy **detailed how DollyWay**, a malware that has consistently redirected victims to VexTrio throughout its eight years of activity, suddenly stopped doing so on November 20, 2024 and began routing visitors to what appeared to be a new TDS, dubbed the Help TDS.

But DollyWay was not the only one that changed to direct victims to the Help TDS. Since late-2015, many different malware strains infected WordPress sites and redirected visitors to VexTrio. In their 2024 annual report, GoDaddy found that nearly 40 percent of compromised websites that redirected visitors sent them to VexTrio via Los Pollos smartlinks. These compromises led to several types of website injections, including those GoDaddy refers to as Balada, DollyWay, and Sign1, as well as unnamed injection campaigns. By the end of November, all these actors, which previously led to VexTrio, began using Help TDS, or halted their operations altogether.
Los Pollos had shuttered their push monetization, but they are just one entity in a sprawling criminal enterprise that makes up VexTrio. Had VexTrio really thrown in the towel? We needed to determine whether Help TDS was independent. Naturally, we turned to DNS as a primary source for our research.



To study how malware actors adjusted to the disruption and changed to the Help TDS, we considered a specific type of WordPress compromise. These campaigns used DNS TXT records as a mechanism for command and control (C2), a technique in which the C2 server encodes a URL in a TXT record and the compromised site redirects to that URL. The DNS query contains encoded information about the website visitor in the hostname, which allows the C2 server to determine how to respond.

By analyzing 4.5 million DNS TXT record responses from compromised websites covering a six-month period (that included November 17) we discovered that the domains used in the DNS TXT record campaigns fell into two distinct sets, each with a distinct C2 server. Both servers were hosted in Russian-connected infrastructure, but neither their hosting nor their TXT responses overlapped. Each set maintained different redirect URL structures, even though they both originally led to VexTrio and subsequently to the Help TDS. These findings shed new light on the DNS TXT malware campaigns that were not previously reported and provided further evidence that a coordinated move to the Help TDS occurred in multiple, seemingly independent, malware campaigns after the November 17 announcement.

We then dug into the Help TDS and its relationship to VexTrio. It turned out that Help TDS is not new but has been intertwined with VexTrio for years. GoDaddy researchers had highlighted that Help resembled another TDS they had called the Disposable TDS; this too has long been interwoven with VexTrio. Our results indicate that the Disposable and Help TDSs are one and the same, and that they had a seemingly exclusive relationship with VexTrio until November.

Digging further, we uncovered many other TDSs that shared a surprising number of characteristics with VexTrio. These characteristics include common files and URL structure that hint at the possibility of a shared code lineage. While the identity of the Help TDS operator remains elusive, we unmasked many commonly seen TDSs as commercial adtech firms, including Partners House, BroPush, and RichAds. As Los Pollos push monetization ended, we've seen an increase in fake CAPTCHAs that drive user acceptance of push notifications, particularly from Partners House. The relationship of these commercial entities remains a mystery; while they are certainly long-time partners redirecting traffic to one another, and they all have a Russian nexus, there is no overt common ownership.

The malware actors' choice to use commercial adtech could be their Achilles heel. As we uncovered the relationships between the website hackers and the VexTrio cabal, we realized that unique identifiers for each malware operator exist for each of the companies. These firms vet network affiliates before allowing them to join—we know, we've tried—and they maintain personal information about the affiliates and their payments that could lead to their identities. The true test of whether they are abused services will be their willingness to turn in the malicious actors who haunt the internet and have stolen untold money from victims worldwide.

A Little Lingo

This paper relies on understanding some terminology that originates in the advertising world. Most importantly, a **TDS** is essentially a smart routing system for directing website visitors to content. This blog on how TDSs deliver malicious content and this one on the malicious adtech industry provide more background and terminology on the topic.

To briefly recap: a malicious TDS is one that is designed to deliver harmful content to users, whether that be malware, like information stealers, or scams. For example, when a malware operator compromises a website, they want to maximize their profits and hide their activity; redirecting visitors through a TDS accomplishes both of those goals. A TDS is said to "cloak" a domain, or a domain is said to be "**cloaked**," when its malicious nature is hidden from users.

A TDS can be simple and controlled by the malware operator. They could design their own, as it is believed SocGholish has done, or they could use a commercial tracker which can be leveraged as a TDS, like Keitaro. But if they want website visitors to see a wide variety of potential content, directing the user traffic through a commercial **affiliate network**, like Los Pollos, is a smart strategy. While the industry term for the delivered content is "advertisements," the content they deliver rarely resembles common advertisements.

Figure 1 shows a high-level view of how affiliate advertising networks are used by website malware actors and many others. The malware distributors are technically "**publishing affiliates**" of the network, which will typically pay them based on "actions" that the visitor, better referred to as victim, will take, including providing email or credit card information. The advertisers themselves are malicious actors and their content is designed for deception. They are sometimes called **advertising affiliates** or partners.

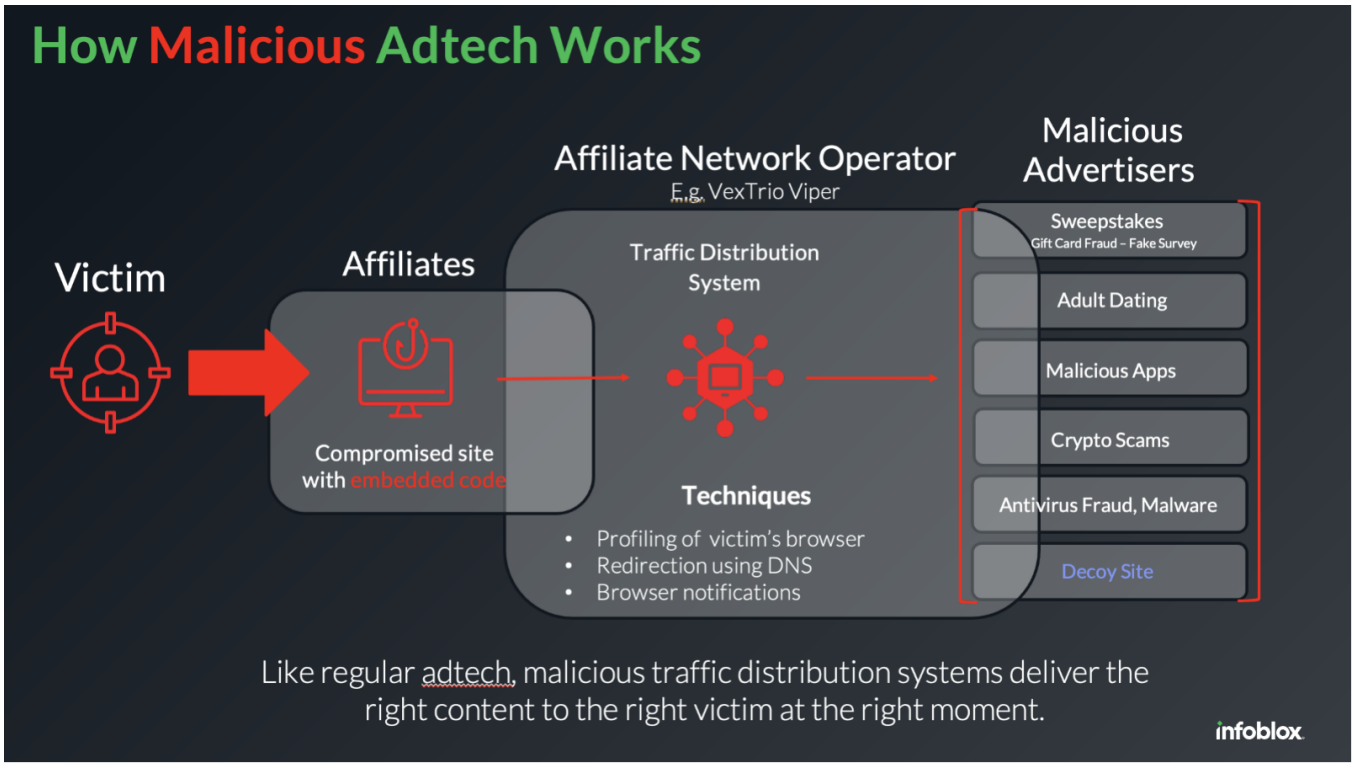


Figure 1. A high-level picture of the role of affiliate networks in malicious adtech

We consider **malicious adtech** to be commercial operators who consistently deliver malicious content. In most cases, these firms have a closed advertising pool; unlike Google advertising, they cannot claim they were duped. Instead, they boast to prospective publishing affiliates about their highly effective advertising, called offers.

Malicious adtech often consists of multiple companies that service different parts of the industry. For instance, Los Pollos recruits publishing affiliates with promises of high-paying offers, while their sister company Taco Loco specializes in push monetization and recruits advertising affiliates, including those from Los Pollos. This combination ensures that VexTrio, the controller of both firms, maximizes profits.

The way malware operators like those deploying the DollyWay campaigns integrate with malicious adtech is through a single link. That link, called a **smartlink** or **direct offer**, drives traffic into the adtech TDS. The final content is often referred to as verticals with benign names like "mainstream dating" and "sweepstakes;" these are scams, fake apps, or malware download sites.

DNS TXT Record Campaigns

Our initial research started from a specific WordPress malware that we track via DNS.

DNS TXT records were designed to support online mail operations, but have long been used for other purposes, good and bad. Many actors over the years have encoded a "next stage" response for a piece of malware, turning the authoritative DNS name server into a rudimentary C2 server. WordPress malware campaigns that leveraged DNS TXT records in this way to redirect victims to VexTrio were **first reported by Sucuri** in August 2023.

In these campaigns, the threat actors used malicious scripts to look up DNS TXT records that contained a Base64-encoded URL. The scripts would redirect the visitor based on those responses. Several months later, **Sucuri identified** a switch by the actors to server-side redirection. **We also published** findings on these campaigns in collaboration with Randy McEoin in January 2024.

GoDaddy's 2024 annual report found that nearly 25,000 websites were infected with this malware and they noted that "evolution throughout 2024 demonstrated increasing complexity, particularly in its shift from client-side JavaScript injections to stealthier server-side PHP redirects in March." They further emphasized that these changes were done with an eye toward operational security and "Perhaps most notably, the campaign maintains persistence through automated bot networks that actively monitor and reactivate disabled malicious plugins, making complete removal particularly challenging."

Our analytic systems track the communication between the compromised websites and the C2 servers through DNS, allowing us to identify new C2 servers and redirects as they come online. We also use these detections to understand the historical connections between the C2 servers and the redirects. Through monitoring DNS queries, we've been able to find sites for which there was no public evidence of the compromise. Additionally, we made ourselves victims of many sites and tracked **the lingering impacts** on our devices.

In a longitudinal study of DNS TXT record queries and responses over six months, August to December 2024, we assessed how the Los Pollos decision to halt their "push monetization" offering impacted the malware operations. The **last date we observed a TXT record response** that led to VexTrio was November 21, 2024, after which they redirected victims to the Help TDS. We focused on three major questions about the threat actors deploying the DNS TXT record malware:

- How did the C2 domains relate to the redirection URLs?
- How did the C2 behavior change in late November?
- How might this impact VexTrio?

C2 Clusters

An analysis of over 4.5 million DNS queries revealed that there are two distinct sets of C2 servers. While all of these led to VexTrio prior to their operational changes, the two C2 sets used different hosting, redirected to distinct domains, and utilized separate URL formats. Figure 2 shows the C2 servers and the domains observed in the redirections that were stored in the DNS TXT records.

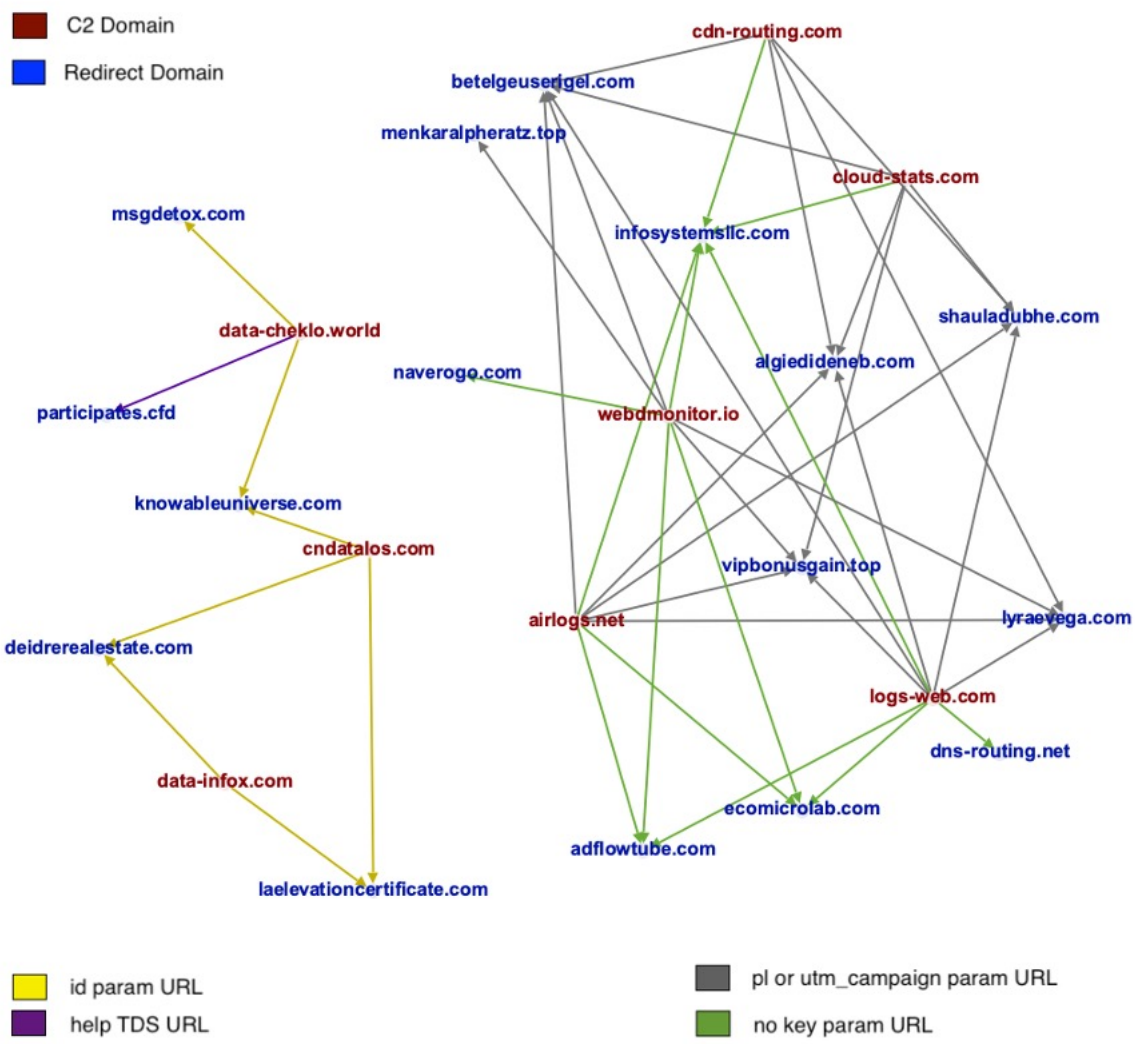


Figure 2. C2 responding with redirect domains in DNS TXT

The redirections from the DNS TXT records all lead to a TDS. Based on our research, we can group the URLs into five distinct types, two of which were first seen on, or after, November 20, 2024 (see Table 1).

URL parameter	Notes
pl=	Parameters like this **example**. These are classic VexTrio URLs that lead to fake captchas and requests for push monetization.
id=	Parameters like this **example**. These traditionally redirected to URLs with pl= parameters, but were later seen directing victims to other TDSs, like this example.
utm_campaign=	This **example**
No parameter	This **example** and this **example**.
URLs with no parameter and containing the /help/ path	Seen briefly in December 2024.

Table 1. The URL parameters observed in TXT records responses from malicious nameservers used in DNS TXT campaigns between August and December 2024

Notably for these TXT record campaigns, not only the domains but also the TDSs divide into distinct sets, meaning that differently formatted URLs are seen in each group. However, they all led to VexTrio prior to November 20, sometimes through a second redirection. The affiliates associated with this TXT record malware have been around for some time. Set #1 has user id pe7k605 in Los Pollos smartlinks and was **first seen in May 2019**. Set #2 uses the push link URL format with pl parameter CHil7Gh3GUyTa8XGgNqDyQ and was **first seen in August 2023**.

The C2 sets also used distinct hosting. In Table 2, we show hosting information based on historical DNS records for this dataset. The full set of C2s and redirect domains observed over the past few years is larger.

C2 Domains	Server IPs	Redirect Domains	URL Format
cndatalos[.]com data-cheklo[.]world data-infox[.]com	46[.]30[.]45[.]27 65[.]108[.]195[.]250	knowableuniverse[.]co deidrerealestate[.]co msgdetox[.]com participates[.]cfd	?id=/help/?
airlogs[.]net cloud-stats[.]com cdn-routing[.]com logs-web[.]com webdmonitor[.]io	185[.]11[.]61[.]37 185[.]234[.]216[.]54 185[.]161[.]248[.]253 95[.]216[.]232[.]139 95[.]216[.]232[.]139	betelgeuserigel.com vipbonusgain.top infosystemsllc[.]com adflowtube[.]com ecomicrolab[.]com lookup-domain[.]com dns-routing[.]com web-hosts[.]io	?pl=?utm_campaign?<rand>

Table 2. Relationships between C2 domains, server IP addresses, and redirect domains in DNS TXT record responses observed in the period August to December 2024

C2 Behavior Changes

Despite independent hosting and redirects, both sets of DNS TXT C2 servers changed their behavior in the same way, albeit at slightly different times. Figure 3 shows how a visitor to a compromised website would be led to malicious content over time.

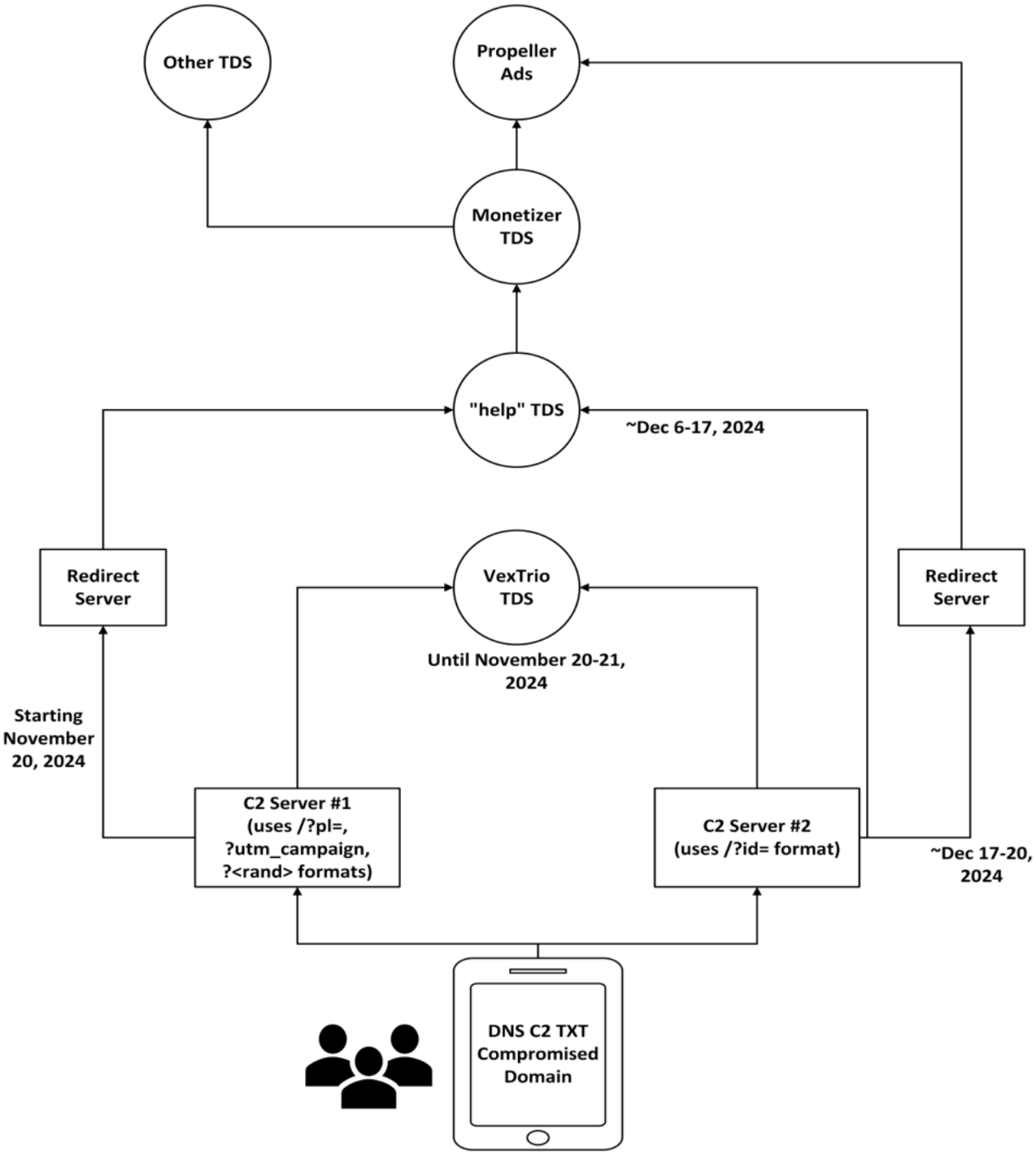


Figure 3. Changes in behavior over time from the two independent C2 sets

Figure 3 shows us that following the announcement from Los Pollos that push link monetization would cease, the two C2 servers changed the DNS TXT responses to send victims to the Help TDS, either directly or indirectly. One set (the one including data-cheklo[.]world), stopped responding between November 22 and December 6. It was later seen on a new server, 46[.]30[.]45[.]27, in the provider Iron Hosting. The second C2 also changed hosting, but to Chang Way 185[.]11[.]61[.]37.

There are a few exceptions. We saw limited instances where the Iron Hosting server bypassed the Help TDS and instead redirected victims directly to Vane Viper, which delivered malware. Further, GoDaddy researchers have reported rare cases where the DNS TXT malware sent victims to a different compromised site and subsequently redirected to a tech support scam.

As of late December, the smaller C2 set containing data-cheklo[.]world appears to have been shut down. However, the larger set containing webdmonitor[.]io continues to send victims to the Help TDS and malicious content through May 2025.

The DNS records show that the two C2 servers are likely operated by independent groups, although they are coordinated in the malware and the content they serve. GoDaddy reported that the DollyWay malware actor converted to the Help TDS on November 20, the same day that the first TXT C2 server set did. Although there are indications of independent operations, there are also clear signs of coordination.

What is this Help TDS? And given the many options for affiliate marketing programs, why did the hackers all choose the same TDS?

Nothing New Under the Sun

Los Pollos stopped push monetization, but Los Pollos is just one small piece of VexTrio. We suspected that the Help TDS was somehow connected to VexTrio, and we were right. Not only was the Help TDS intrinsically linked to VexTrio, but we were also able to tie VexTrio to other mysterious TDSs that have been active in the environment for several years. GoDaddy researchers had speculated that the Disposable TDS had evolved into the Help TDS, but they are more like siblings; all these TDSs ran concurrently and shared characteristics. We can demonstrate these connections “six ways to Sunday,” as they say, but we will only be publicly disclosing a small set of evidence.

Let’s take a look at the relationship between the different URL forms we’ve seen in the DNS TXT responses over time.

TDS Behavior over Time

Though it seemed to appear out of nowhere, the Help TDS is not new at all: it has been around since at least 2017. While this TDS is now redirecting users through the Monetizer TDS, we found many past instances where the Help TDS redirected to VexTrio. Figure 4 shows the TDS behavior based on redirect URL patterns as well as sample scans that show the relationship between the TDSs at different times.

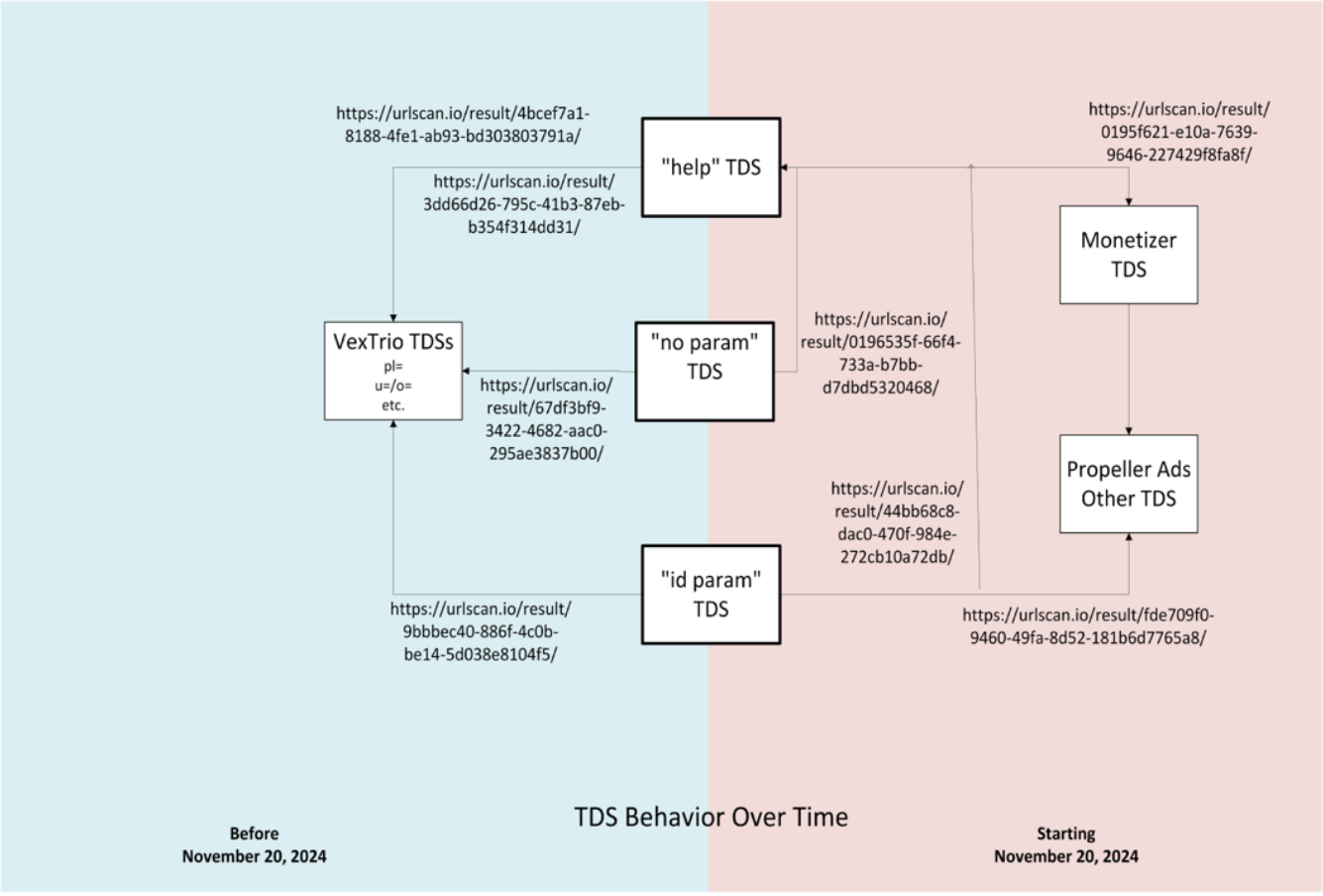


Figure 4. Transition of TDS redirection behavior over time from the three major URL forms seen in compromised websites’ DNS TXT record responses

GoDaddy had reported that before DollyWay malware actors adopted VexTrio’s Los Pollos links, the malware actor had exclusively used the Disposable TDS. The URLs for **Disposable TDS** had the format:

<random_label>.<tld>/index/?<numbers>

The TLDs were managed by Freenom and were offered for free, including tk, gq, and cf.

We almost immediately located sample redirection chains that connected the Disposable TDS to VexTrio as well. **The scan** in Figure 5 included redirection from the disposable TDS to a Los Pollos smartlink, but also included an early version of the Help TDS format using the Disposable TDS domains. From there, we isolated several other samples that showed the same relationships.

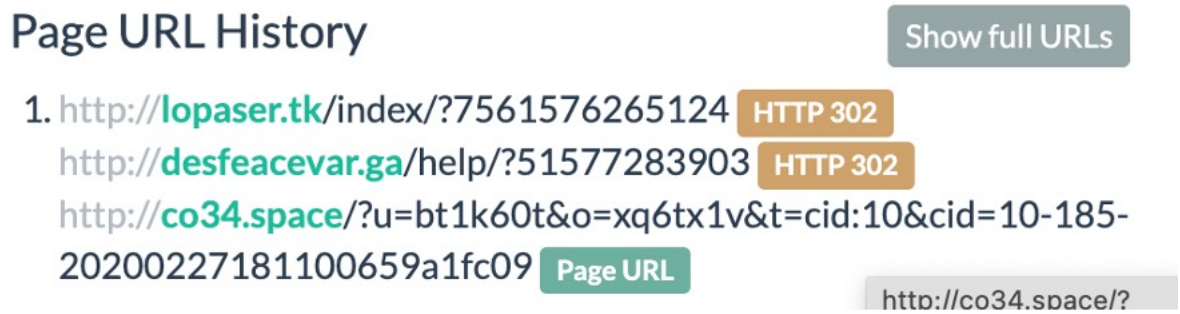


Figure 5. Redirection from the Disposable TDS to a Los Pollos smartlink. Source: https://urlscan.io/result/4bcef7a1-8188-4fe1-ab93-bd303803791a/

Historical scan records allow us to connect the WordPress malware actors across their shift from VexTrio smartlinks to Monetizer in late November 2024. In the example redirection from Figure 5, the domain co34[.]space is used for a VexTrio smartlink for the Los Pollos affiliate identified by the parameter u=b1tk60t. But this URL also includes custom affiliate-established parameters: t, used for campaign names; and cid, a click id for postbacks.[1] The format of the values for those parameters is identical to modern Monetizer URLs like this one:

hXXps://somenth[.]bilitere[.]shop/?utm_medium= {traffic_source_id}&utm_campaign=cid:11005&cid=11005-14814-202505160707555c5e

which is connected to WordPress malware campaigns.[2] It appears that the Los Pollos custom tracker (t=) value cid:11005 is associated to the larger DNS TXT record set that includes ecomicrolab[.]com. Within the Monetizer network, the same threat actor has an affiliate source id (utm_medium=) 9eb2bcdc89976429bc64127056a4a9d5d3a2b57a. The first example of a Monetizer URL formatted in this manner we have observed coincided with the change of adtech providers in November 2024.

Once you've seen a handful of samples like this, it begs the question of just how strong the relationship is between the Help, Disposable, and VexTrio TDSs. When we say VexTrio TDS here, we are referring to several different TDSs operated by the VexTrio enterprise. Beyond Los Pollos, which was revealed in publications by Qurium and GoDaddy, as well as social media posts by us, VexTrio controls other adtech companies and the TDSs that enable their operations. These include Taco Loco and Adtrafico.

DNS Connections between Multiple TDSs

It turns out there are DNS connections between the VexTrio TDS and the other malicious TDSs. But determining whether the relationship is due to presence in the TDS or a relationship with the affiliate can be challenging. Affiliate advertising programs like Los Pollos and Monetizer allow for the use of custom domains, which are owned by the affiliate rather than the company. This can be done via DNS CNAME records or DNS A records. While this allows us to track the relationship with an affiliate and different TDSs, unfortunately, it also obscures the true nature of the relationship between the domain owner and the TDS.

We have seen custom domains overlap in a few different ways. In some cases, the domain owner assigns a hostname to the affiliate program. For example, the domain owner of oktrkme[.]com, which we believe is owned by a Mexican marketing agency, appears to have been an affiliate of both Los Pollos and Monetizer. The domain name date[.]oktrkme[.]com was seen resolving in the IP address space controlled by VexTrio, while the domain name mnz.oktrkme[.]com resolved to Monetizer IP addresses in late April 2025.

While oktrkme[.]com seems to be owned by an affiliate, others are more complicated. The domain purinagun[.]ru was registered in April 2024 through the Russian Registrar (reg[.]ru) and was used in both Los Pollos smartlinks and the Help TDS. In this case, no hostnames are involved, but it is possible there was a DNS CNAME assignment at the time, making it impossible to validate from DNS alone whether the domain was directly controlled by both TDS operators. Shared IP addresses between purinagun[.]ru and pacocha[.]shop create another similar connection between the two TDSs. And a third domain, prefez[.]shop, draws in a third TDS that we had dubbed the News TDS, which we now know is controlled by the commercial adtech firm Partners House (see Figure 6).

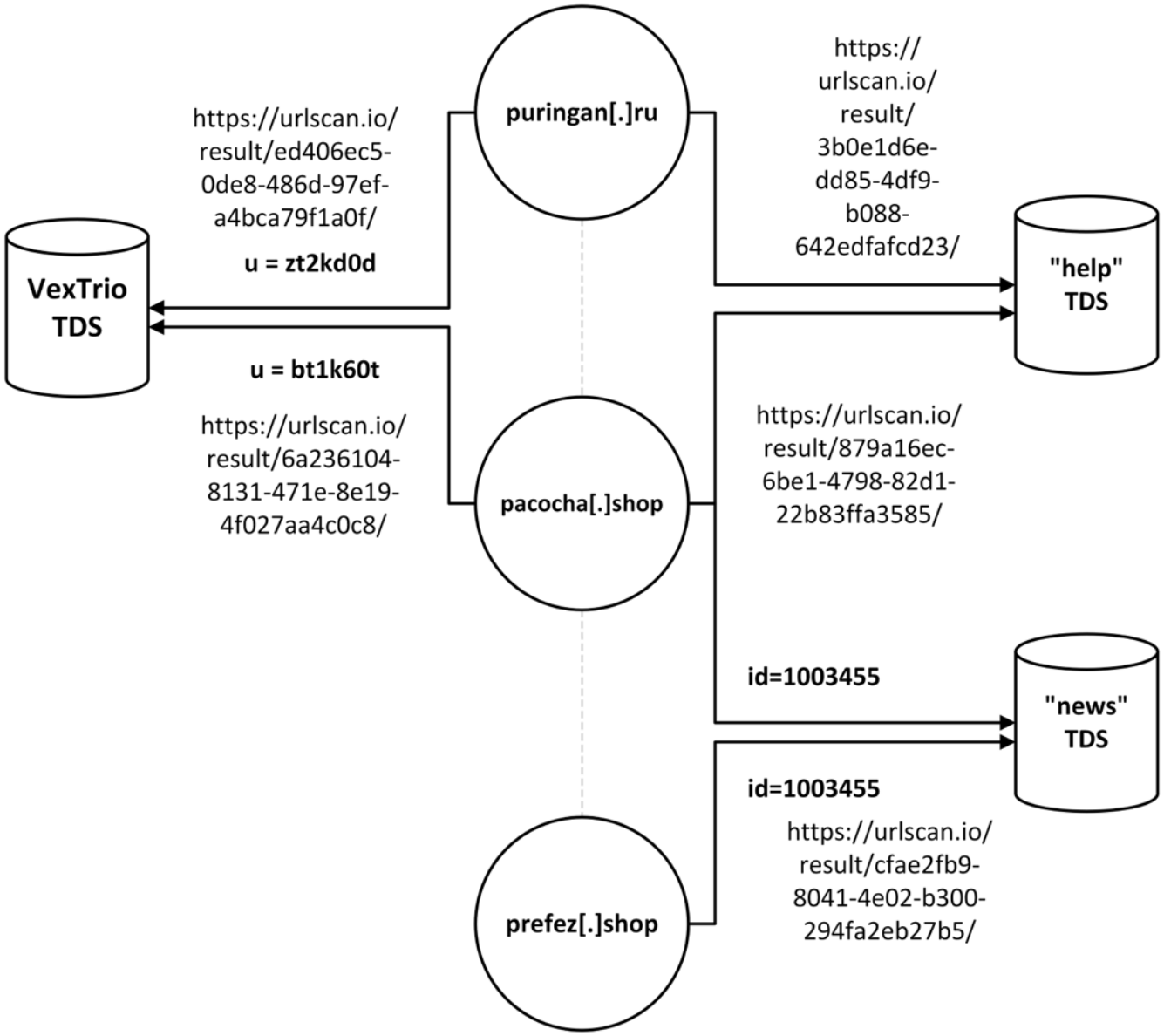


Figure 6. The relationship between select domains seen in TDS URLs and the TDS

The reuse of domains across different TDSs complicates analysis of the underlying relationship between the TDSs themselves, but it does provide an effective mechanism to tie affiliate actors, such as those compromising websites, over time. In this case, we can tie together:

- The Los Pollos affiliate with id u=bt1k60t and u=zt2kd0d
- Partners House affiliate with id 1003455
- Monetizer affiliate id 9eb2bcdc89976429bc64127056a4a9d5d3a2b57a

We can see that malware actors have adopted a small set of TDSs consistently over time, but is there more to be learned about the relationship between the TDS themselves? We went back to the Help TDS to look for answers.

Help TDS Affiliations

The Help TDS emerged on our radar when Los Pollos stopped their push monetization offering in late November 2024, but they have been present in the environment since at least November 2017. We saw from sample data that several TDSs had interactions with each other over time, as we showed earlier in Figure 4. What other affiliations exist?

To understand how the Help TDS has interacted with other known threat actors, we considered approximately 10,000 website interactions over the last six years that included Help TDS in a redirection chain. The visits could have resulted in a decoy landing page, such as Google or TikTok, but they could also land at malicious content. We used every redirection seen in the scans and enriched that with our internal knowledge about DNS actors. Figure 7 is a summarized visualization of more than 120,000 URL redirections and the known entities involved.

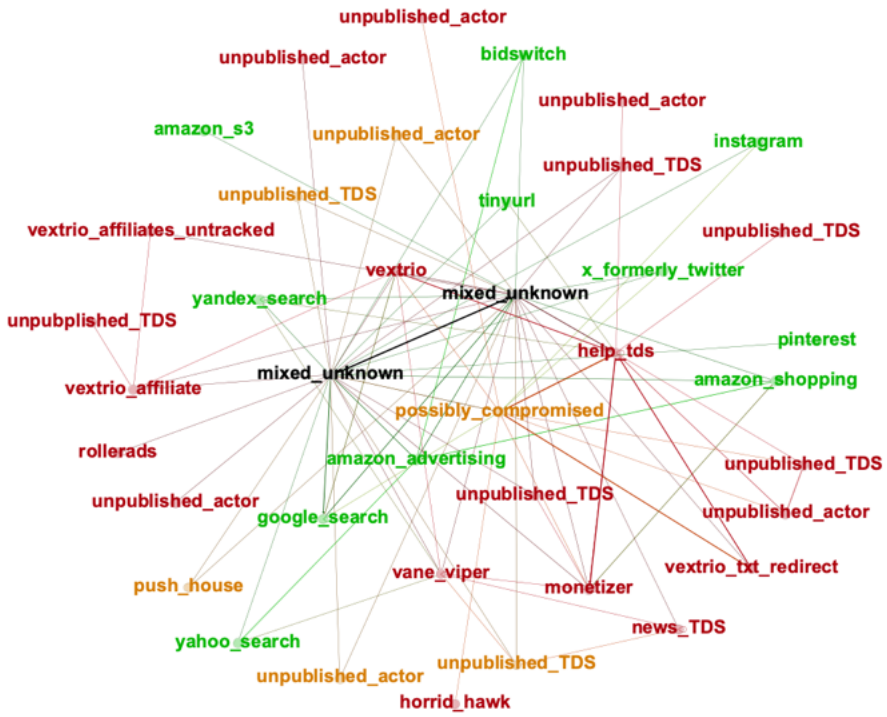


Figure 7. Relationships between DNS actors or clusters of activity seen in scans that involve the Help TDS between November 2017 and May 2025. Labels in red are actors Infoblox considers malicious, orange are suspicious, and green are known legitimate.

Figure 7 illustrates the interactions between VexTrio, the Help TDS, the News TDS (Push House), and a handful of other advertising and TDS operators over a long period of time. We also see some interactions by criminal actors like Horrid Hawk, who are known for domain hijacking. Other DNS threat actors, some of which are TDS actors, that we track but have not published, appear in the graph as well. Long historical relationships like those discovered in this analysis have helped us validate theories about TDS affiliations but also uncover several new TDS operators.

A Common Codebase

Once we had established connections between several TDSs via compromised website redirections, we looked to see if we could tie the TDSs together in more concrete ways. We were able to identify strong relationships between the Help, Disposable, and VexTrio TDSs through their historical use of scripts, images, and URL structure.

It turns out that the Help and the Disposable TDSs are essentially the same. At various points since 2017:

- They both used rare sweepstake lure images that appear to be exclusive to a relatively small group of threat actors, including VexTrio.
- Both of their servers hosted VexTrio-exclusive JavaScript that are important to the functionality of its sweepstake scams.
- They both used the same URL structure and parameter names.

For most of its history, Help TDS has operated as a straightforward redirector, like Keitaro. However, we did find evidence that several years ago, the TDS domains were simultaneously used to serve lure pages. Searching back to 2019, we discovered many instances of both Help TDS and Disposable TDS directly serving sweepstakes scam content. This included rare lure images that appear to be only used by a small group of entities, including VexTrio (see Figure 8).

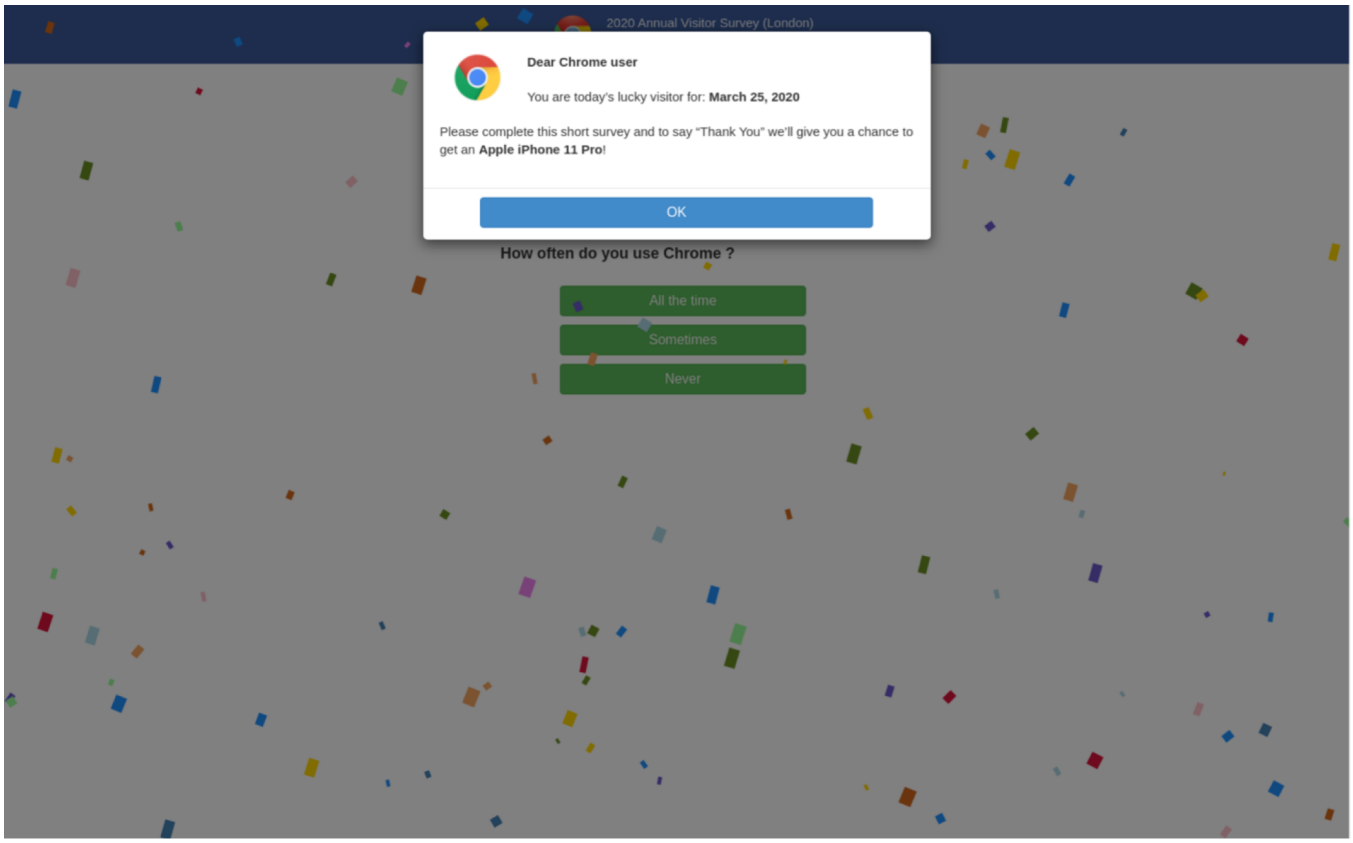


Figure 8. Rare sweepstake image lure used by VexTrio, Help, and Disposable TDSs

The websites that served the sweepstakes content even showed identical URL structures and parameter names between both TDSs. This indicates that both systems are using common technology. Figure 9 shows the identical URL pattern used by both TDSs for serving scams to web visitors.

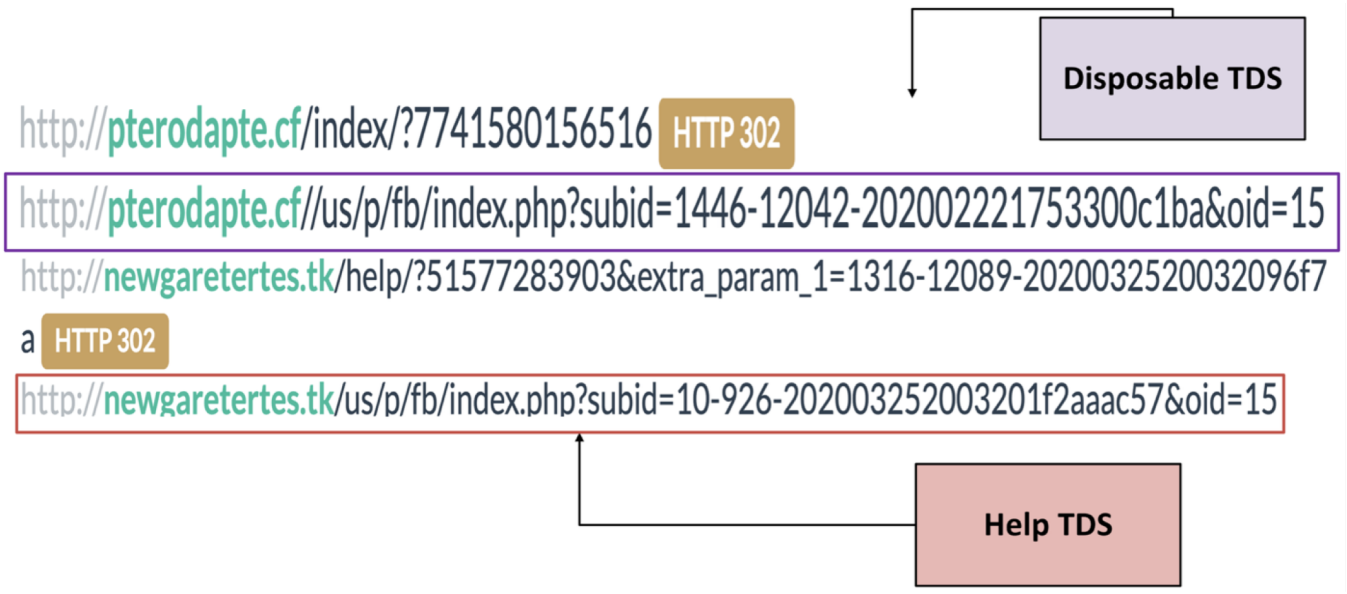
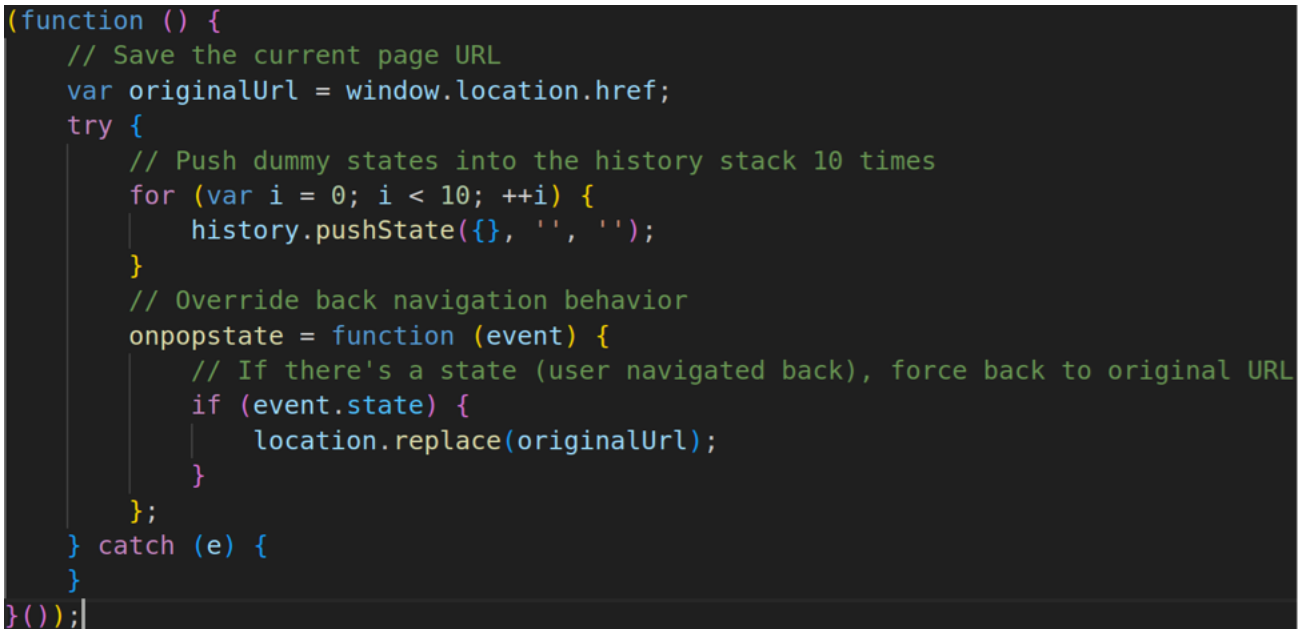


Figure 9. Identical URL pattern between Help and Disposable TDSs

In combination with the rare lure images, both Help and Disposable TDSs executed two pieces of rare JavaScript. VexTrio is the only other actor we have seen use these particular scripts. Furthermore, like VexTrio, Help TDS and Disposable TDS host the scripts directly on their servers. This means that they are not merely running the code from a remote server but have full possession of the scripts. The threat actors typically obfuscate the JavaScript to hinder analysis by security researchers (see Figure 10 for a simple interpretation of one). This script prevents a web user from navigating backward in their browser history (e.g., by clicking on the back button). Instead, the user will reload the current page in their browser instead of the previously visited page.



```
(function () {
    // Save the current page URL
    var originalUrl = window.location.href;
    try {
        // Push dummy states into the history stack 10 times
        for (var i = 0; i < 10; ++i) {
            history.pushState({}, '', '');
        }
        // Override back navigation behavior
        onpopstate = function (event) {
            // If there's a state (user navigated back), force back to original URL
            if (event.state) {
                location.replace(originalUrl);
            }
        };
    } catch (e) {
    }
}());
```

Figure 10. JavaScript prevents navigation to previous pages via the back button

The second script tries to detect when the victim is leaving the current webpage without clicking a link or submitting the scam form. Under such circumstances, the script will launch the confirmation message, “You are about to leave this page!” and then quickly reload the page after a short delay. The overall goal is likely to discourage or interrupt the user from leaving the page without participating in the scam (see Figure 11).

```
try {
    function addLoadEvent(func) {
        var oldonload = window.onload;
        if (typeof window.onload != 'function') {
            window.onload = func;
        } else {
            window.onload = function () {
                oldonload();
                func();
            };
        }
    }
    window._link_clicked = false;
    window.onbeforeunload = function (event) {
        if (window._link_clicked)
            return null;
        setTimeout(function () {
            location.reload(true);  //window.location.href = '/web/';
        }, 10);
        window.onbeforeunload = function () {
        };
        return 'You are about to leave this page!';
    };
    addLoadEvent(function () {
        var anchors = document.getElementsByTagName('a');
        var forms = document.getElementsByTagName('form');
        for (i = 0; i < anchors.length; i++) {
            anchors.item(i).addEventListener('click', function (event) {
                window._link_clicked = true;
            });
        }
        for (i = 0; i < forms.length; i++) {
            forms.item(i).addEventListener('submit', function (event) {
                window._link_clicked = true;
            });
        }
    });
} catch (o) {
}
```

Figure 11. JavaScript prevents page exit without participation in scam

For the past several years, Help TDS has redirected traffic to VexTrio and more recently Monetizer. The Help TDS has a strong Russian nexus, with hosting and domain registration frequently done via Russian entities. It does not have the full-blown functionality of the VexTrio TDSs and has no obvious commercial ties beyond its eerie connections with VexTrio. On the other hand, Help TDS and Disposable TDS are used extensively, if not exclusively, by website malware operators, including those who run the DNS TXT record campaigns and **DollyWay**.

TDS Resource Connections

We expanded our relationship analysis to other TDSs that showed varying levels of similarity with VexTrio. The TDS operators left digital traces of their public personas in DNS, and we used that information to connect several TDSs to commercial entities, including the News TDS.

The connections between these TDS are not limited to redirections within URLs from compromised sites; they also share several rare artifacts not found elsewhere on the internet. In the phishing landscape, threat actors commonly adopt phishing toolkits used by other cybercriminals because it is relatively easy to upload the phishing web materials on a web-hosting service and run a functioning website. On the other hand, operating a high-availability TDS is complicated; it requires a deeper tech stack, such as clusters of web servers, web tracking systems, real-time bidding logic, affiliate payment models, and sometimes, advanced DNS configurations. While phishing kits are available for sale, the same is not true of TDSs and we were surprised to find common TDS components across multiple commercial entities.

We have discovered a set of web resource files used by VexTrio TDSs and several others, including those run by the commercial entities Partners House, BroPush, and RichAds. The resources are important dependencies for the TDS, such as enticing images for luring web users, JavaScript for tracking, or browser cookie installers. The rarity of these files suggests that these firms share code lineage possibly through partnerships or common developers. We are not publicly releasing the full details of these artifacts.

The files are utilized by approximately 20 distinct TDS networks even though there is little overlap in the structure of their respective URLs, the company ownership, or hosting. Table 3 describes a subset of the systems that we identified, including their URL structure, parameter names, and parameter value descriptors.

Estimated Deployment Date	TDS Name / Attribution	TDS URL Format	Example T
May 2019	BroPush	hXXps://{domain}/?p=[a-z][0-9]{23}&sub1={source_id}&sub2={site}	robotverifie
March 2021	BroPush	hXXps://{domain}/?auf=[a-z][0-9]+&p=[a-z]{1,2}&sub1={source_id}&sub2={feed_name}	di4[.]biz
June 2023	BroPush	hXXps://{domain}/?start=[12]&s=[a-z]{1}&t={campaign_id}&sub1={source_id}	w-news[.]b
April 2019	VexTrio TacoLoco	hXXps://{domain}/ (lure_name:eyes-robot|space-robot|blue-robot|office-robot |allow-button)/?pl=[a-z][A-Z]{22}&sm={subscribe_method}&nrid={nrid}&hash={hash}&exp={epoch_expiration}	mvgde[.]m
March 2017	VexTrio Los Pollos	hXXps://{domain}/?u=[a-z][0-9]{7}&o=[a-z][0-9]{7}&t={campaign_name}	scoretoppri
October 2020	VexTrio LosPollos	hXXps://{domain}/smartlink/?a=[0-9]{6}&sm=[0-9]{5}&mt=[0-9]{2}&s1={tracker}	cdsecurecl
October 2021	Unknown	hXXps://{domain}/[a-z0-9-]{43}/?clck=[a-z0-9]{32}&sid=[0-9]{8}	phenotypel
December 2021	Admeking	hXXps://{domain}/?lp=[a-z0-9]{6}&actoken=[a-z0-9-]{36}&sid={source_id}	news-abcd
December 2018	VexTrio TacoLoco	hXXp://{domain}/(bot-check-[0-9]+| video-[0-9]+|adult-web[0-9]+|age-check-[0-9]+|porno-land-[0-9]+|checking-browser-[0-9]+)?h=[a-z=]{68}	i8b[.]wstba
August 2024	Partners House	https://{domain}/?fingerprint=[a-z0-9]{32}&i=[0-9]{1}&id=[0-9]{7}&traceId={trace_id}	702942e07
July 2022	BroPush	hXXps://{domain}/go/[a-z0-9]{18}?sub2={feed_name}	siteforyou3
November 2019	disposable TDS	hXXp://{freenom_domain}/index/?[0-9]{11,14}	ritardalarm
March 2020	Help TDS	hXXp://{domain}/index/?[0-9]{11,14}&extra_param_1=[a-z][0-9]{20}	f68wy7o9e
August 2024	Partners House	“news” TDS	hXXps://{d 9]+&p1=[0- 9]+&traceI 0cc79f766
July 2024	Partners House	hXXps://{domain}/click/ssp/?id={base64_encoded_victim_details}	epicclicks[.
September 2019	Partners House	hXXps://{domain}/16/?site=1000619&sub1={site}&sub2={hour}&sub3={browser}&sub4={click_number}	rpn-news3
August 2022	RichAds	hXXps://{domain}/?q={click_id}&s={traffic_source}&var={u_id}&geo={geo}	6[.]lands[.]
February 2024	RichAds	hXXps://{domain}/cl?c=[0-9]{8}&p=[0-9]{8}&cid={click_id}&sub1=[a-z0-9]{22}	sweetrnd[.]
December 2019	RexPush	hXXps://{domain}/(lure_name:adult_video_[0-9]{1}|check_age)/[0-9]{4}/[a-z0-9]{32}/?sub3={browser_info} &sub2={os_info}&click_id={click_id}	b9ab1[.]rpb
February 2017	Monetizer / Advertizer	hXXps://{domain}/utm_medium=[a-z0-9]{40}&utm_campaign=cid:[0-9]{5}&{optional_params}	someth[.]

Table 3. Different TDS URL structures that share rare artifacts and/or have been utilized by WordPress attackers for affiliate advertising networks

Sharing Lures: By Design or Coincidence?

There is a common denominator among six different TDSs, including those that we confirmed as VexTrio, Partners House, and RichAds. In a large portion of their cyber campaigns, these systems all used the same set of template images for luring web visitors into clicking a fake CAPTCHA button. The button deceptively gives permission to the advertising network to send notifications to the victim’s browser at any time. All of the systems are operated by affiliate programs that specialize in distributing links to content via push notifications. Figure 12 shows a set of image lures that are hosted directly on the six TDS servers. It is compelling that:

1. The six TDSs share image lures that are not just visually identical, but their SHA256 file hash values match. This means that the images show the exact same size and dimensions, resolution, etc.

2. A very small number of TDSs use these images as lures.
3. In nearly all attack instances across the six TDSs, the images are named 1.png, 2.png, logo.png, bot.png, or man.png.
4. All six TDSs use fraudulent methods for subscribing internet users to malicious push notification advertisements.
5. All six TDSs are operated by large public affiliate networks that specialize in push advertising.
6. These affiliate networks use similar methods and technologies for sending notifications to their subscribers (i.e., victims).
7. The affiliate networks commonly run PowerDNS, an open-source software suite for managing DNS servers.

logo.png: 

man.png: 

robot.png: 

Figure 12. PNG images used by push advertisement affiliate networks

After we identified the six TDSs that share the common lure, we pivoted on their DNS and web signatures to find the rest of their lure templates. Virtually all the template images serve a false message that tricks users into subscribing to malicious push notifications. These messages are almost always related to a fake CAPTCHA test or access to enticing but non-existent content. Figure 13 is a collage we created using various “safe for work” lure images that were historically used by the six TDSs.

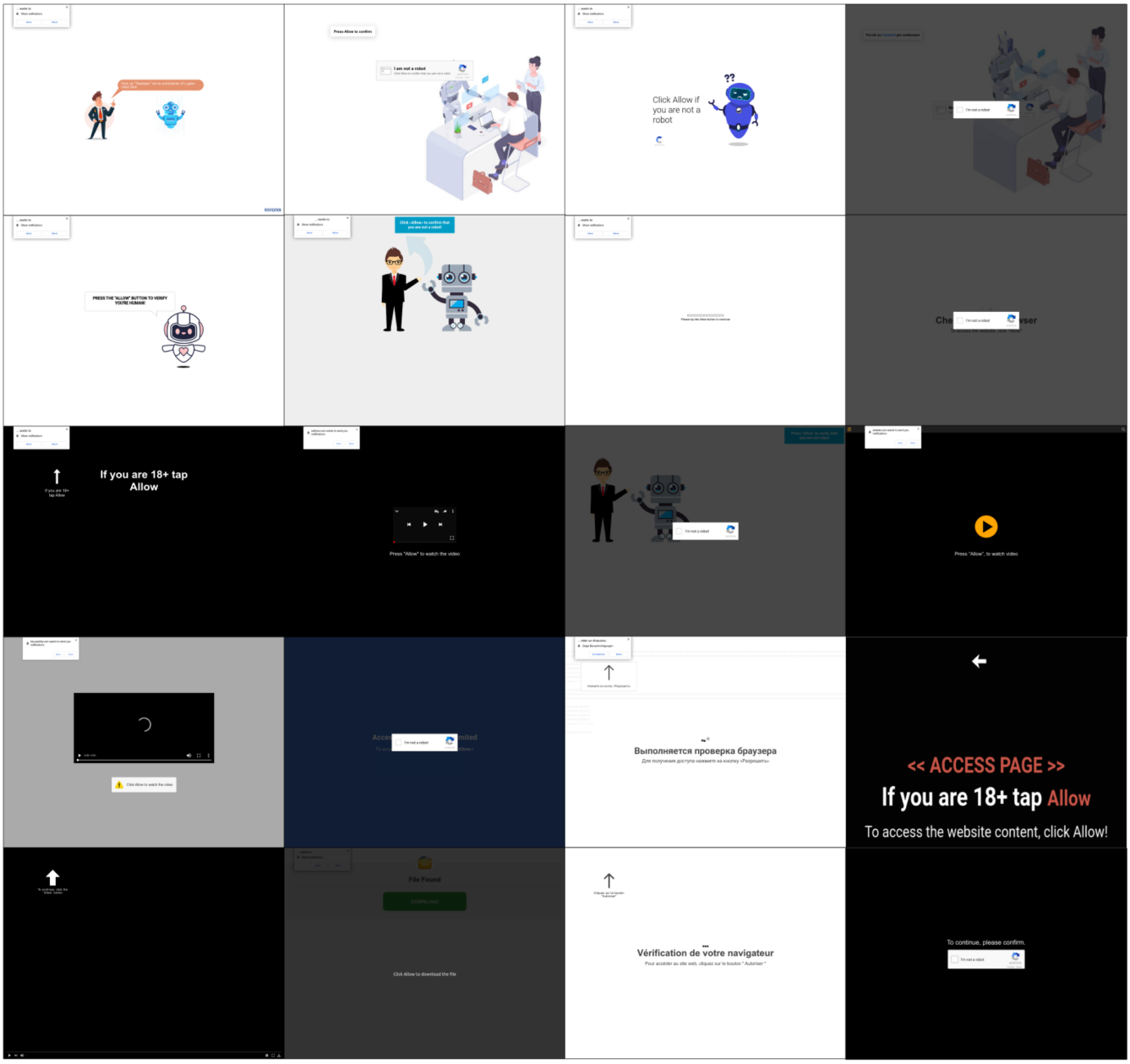


Figure 13. Collection of non-offensive push notification templates used by VexTrio and closely related TDSs

Identification via DNS

In addition to the lure images, we analyzed JavaScript related to notification subscriptions and DNS patterns to identify the public aliases associated with these TDSs. The networks use multiple systems that show different URL structures in HTTP traffic. This variation challenges relationship analysis between the multiple TDSs. Figure 14 shows five different push advertising affiliate programs that use various technologies but format their DNS resource names similarly. We used passive DNS and unique JavaScript to determine the identities of the TDS operators: Partners House, BroPush, VexTrio's TacoLoco, REXPUSH, and RichAds.

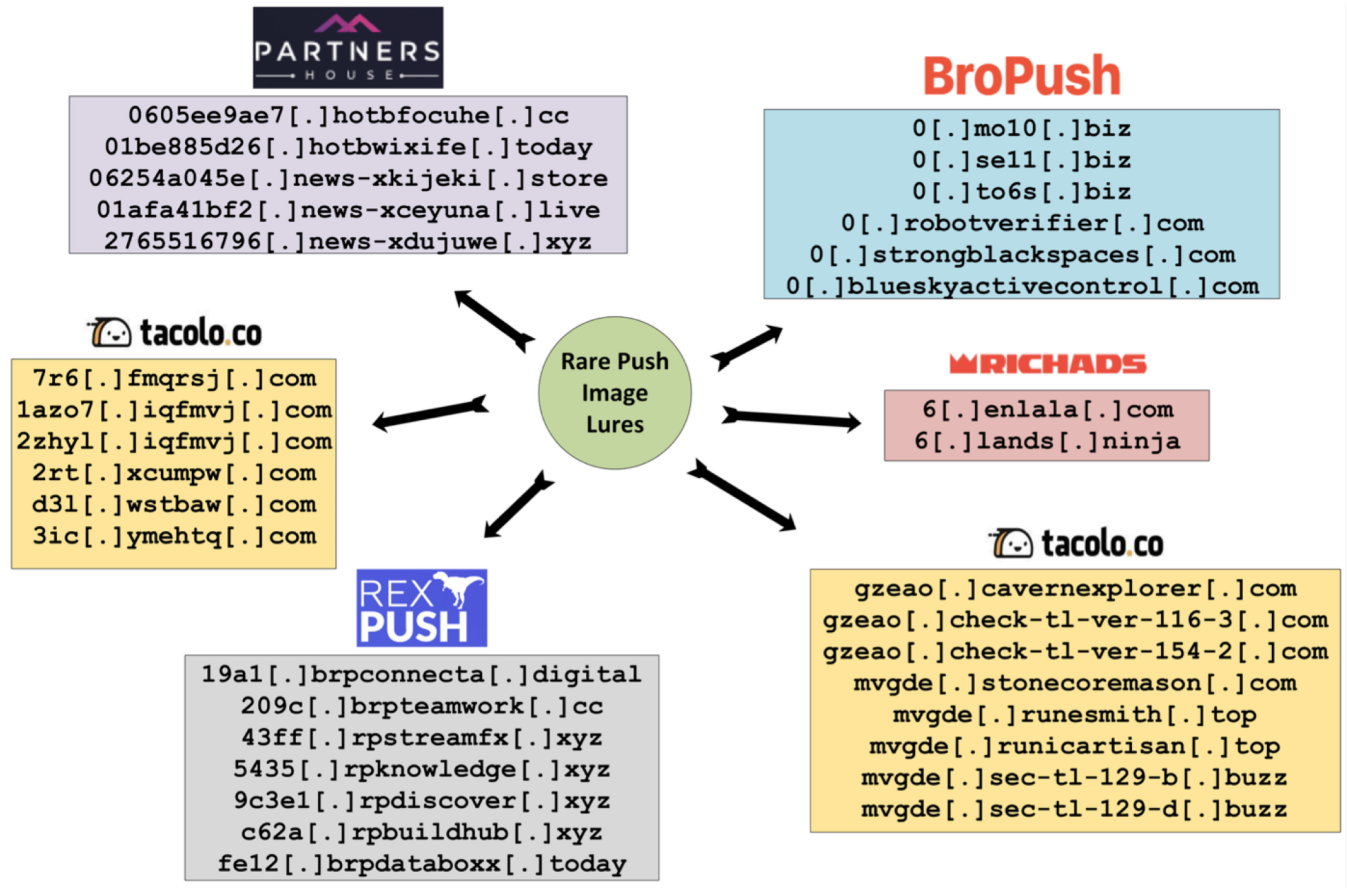


Figure 14. Adtech networks whose TDS share rare images, scripts, and DNS patterns

We also realized that both VexTrio and Partners House run PowerDNS, an open-source DNS server software, on their servers. Although PowerDNS does not explicitly identify itself in responses to network requests, we discovered indicators of its usage in the DNS SOA records of many VexTrio and Partners House TDS domains. Figure 15 shows the indicator a.misconfigured.powerdns.server.hostmaster in a response to a DNS SOA query for the VexTrio TDS domain ospeau[.]com. This occurs when the administrator loads a zone into PowerDNS and the zone contains domains with a missing or invalid SOA value. As a result of the threat actors' server misconfigurations, we were able to identify several of their IP addresses associated with PowerDNS.

Figure 15. PowerDNS indicator in a DNS SOA response from VexTrio TDS

Cybercriminals rarely install and configure PowerDNS on their web servers; deploying it properly requires relatively high-level knowledge of DNS. Evidently, DNS is integral to VexTrio and Partners House's cyber operations. PowerDNS is capable of dynamically responding to queries for specific domain name patterns, which can be a powerful tool for a TDS threat actor that aims to control the traffic to their infrastructure.

Push Advertising Is Popular

RichAds, BroPush, Partners House, VexTrio's TacoLoco, and RexPush specialize in push advertisements. The backbone of the adtech business is the push notification service. Between these firms, we detected two kinds of technologies used to fraudulently subscribe users to notifications. These services also enable the company to push notification messages to their victims indefinitely until their subscription is terminated (i.e., browser notification permissions are removed). The first is sending notification messages via Firebase Cloud Messaging (FCM), a service provided by Google that allows developers to push notification messages to apps on Android, iOS, and the web. Pushing messages via FCM is a powerful distribution method because it bypasses security firewalls as victim browsers receive notifications from Google's servers rather than the servers controlled by the threat actors. Second, affiliates have also used custom-developed scripts that leverage the Push API, a browser feature that enables web applications to receive notifications from a server.

In most instances, the script that subscribes users to the threat actor's notification server (e.g., FCM, custom server) is hosted on the TDS server. The operators typically complicate code analysis of the script by using open-source obfuscation tools such as obfuscator[.]io. Several years ago, VexTrio deployed content delivery network (CDN) servers to serve web resources (e.g., push subscription scripts) that are mission critical to their fraudulent push advertising activities. Figure 16 shows a common configuration in a VexTrio push subscription script. The CDN server cdn[.]jmp-assets[.]com has been in service for nearly two years and is still currently active. As of this writing, the domain jmp-assets[.]com is currently ranked in the top 100,000 of all domains, according to VirusTotal. This underscores the threat actor's broad attack distribution and access to scalable, high-capacity infrastructure.

```
var partyId = 'Q0Q6cUlBOExyZ20=';
var cdnServerUrl = 'https://cdn.jmp-assets.com/prod';
var apiServerUrl = 'https://notification-centr.com';
var swScope = '/';
var customWorkerJS = 'service-worker.js';
```

Figure 16. Critical VexTrio server domain configurations in push subscription code

One hard limitation of FCM is that it doesn't have a built-in feature to directly track which users or devices are subscribed to specific topics, nor can it serve a statistical history of previously sent messages. To overcome this, adtech operators such as VexTrio have implemented their own tracking mechanisms for keeping tabs on current subscribers and historical subscriptions. Figure 17 shows custom code that VexTrio developed. This application sends information about the victim (e.g., browser language preference, system information, device type) and their unique FCM token id to a special, VexTrio-controlled tracking server (e.g., notification-centr[.]com). Subsequently, VexTrio uses all this information to send targeted advertisements to the subscribed victims via push notifications.

```
function sendMessageToServer(eventType, token, reqId) {
    console.log("reqId:" + reqId + " eventType: " + eventType + " token: " + token);
    messageBody['tokenId'] = token;
    if (notBlank(typeof dmpSegments !== 'undefined' && dmpSegments)) {
        messageBody['segments'] = dmpSegments.split(',');
    }

    messageBody['urlParams'].s2 = reqId;

    return fetch(apiServerUrl + '/api/subscribe/' + eventType, {
        method: 'post',
        headers: {
            'Content-type': 'application/json',
            'Authorization': 'Basic ' + partyId
        },
        body: JSON.stringify(messageBody)
    }).then(function (response) {
        if (response.status !== 200) {
            throw new Error("Error Send Subscription To Server");
        }
        return response.json();
    }).then(function (data) {
        logger('Response Received: ', data);
        pushConfig.sid = data.sid;
        if (data.urlParams !== undefined) {
            addDataToDB(data, data.sid, token, reqId);
        }
        if (data.sid) {
            messageBody['urlParams'].sid = data.sid;
            setCookie("sid_" + getSubdomain(), data.sid);
            cookieMatching(data.sid);
            subscriptionSuccess();
        } else {
            subscriptionFailed("SubscriberId is undefined.");
        }
    }).catch(function (e) {
        logger("Error Send Subscription To Server: ", e);
    });
}
```

Figure 17. A VexTrio code function that tracks user push subscription activity

Although these adtech firms are registered in different countries and appear to be commercially independent, the artifacts we have disclosed here, and others we have not, indicate that the TDSs at the core of each company's operation are intricately related. That said, the exact nature of their relationship is unclear. What is clear is that these enterprises are benefiting from and enabling a wide range of cybercrime, including the exploitation of millions of websites that feed victims into their lair.

Who Are the TDS Operators?

Connecting a TDS definitively to an adtech firm or other actor is tricky business, but we've identified quite a few.

Mapping TDS URL patterns to public affiliate network entities is uniquely challenging because so much of their infrastructure is kept secret and hidden behind proxies (e.g., Cloudflare) or bulletproof hosting. For example, most affiliates of these advertising networks are unaware of their deeper-level business practices, let alone any notable fraction of their total domain assets. Adtech operators typically share a small number of "front-end" TDS domains with their publisher affiliates. They do not widely share information about mission-critical and central servers in the network. Additionally, they use a diverse set of server software and URL parameters that make it extra difficult to group and categorize different TDSs under one network label. Viewed holistically, the networks exhibit traits consistent with an advertising operation. Moreover, their use of lookalike domains and script names that mimic advertising technology further obscure their activity within legitimate web advertisement traffic.

Despite these circumstances, we've achieved accurate identification thanks to the adtech operators' habitual configuration practices in DNS, reuse of rare web artifacts, lack of clearing digital traces of their previous activities, and other IT shortcuts that gave us opportunities to track and identify them. For example, we analyzed and grouped the TDSs by common subdomain patterns, identical or highly similar push

subscription scripts, as well as by linking their old domains in passive DNS to cached webpages promoting their public business names. Table 4 lists several public names of TDS operators that are either owned by VexTrio or appear to show close partnerships with them.

Operators	TDS Description
VexTrio companies, including Los Pollos, Taco Loco, and Adtrafico	VexTrio is a group of malicious adtech companies that distribute scams and harmful software via different advertising formats, including smartlinks and push notifications.Example params: u=, o=, pl=
Possibly independent operator in VexTrio circle; Identity unknown	Help TDS and Disposable TDS run Keitaro software on their servers and previously redirected victims to VexTrio infrastructure. They also distributed rare scam content used by VexTrio.Example paths: /help/, /index/
Partners House	Partners House is owned by Push House and is a push advertising platform that tricks users into subscribing to its push notifications via fake CAPTCHAs and adult-themed lures.Example params: fingerprint=, id=, traceId=, drs=
BroPush	Push advertising platform that tricks users into subscribing via lures related to fake CAPTCHAs, adult content, cinema, music, and news.Example params and folders: p=, /go/
RichAds	Distributes advertising via Telegram Mini Apps, push advertising, pop ads, and native ads.Example params: q=, s=, var=, geo=
RexPush	A push advertising affiliate that uses adult-themed and robot CAPTCHA lure images to trick users into subscribing to their notifications.Example params: sub3=, sub2=, click_id=
Pushtorm	Pushtorm is a push notification service that enables website owners to subscribe web visitors to push notifications and send them targeted messages. Pushtorm users can also sell excess traffic within the service. This service is heavily used by Rich Audience and there are indicators that Pushtorm is controlled by them.Subscription server: hXXps://pushtorm[.]net/System/AddSubscriber
Rich Audience	Platform connects publishers and advertisers, and distributes ads via formats: display, video, rich media, and native.Example params: domain=, clickid=, extclickid=
Monetizer/Advertizer	A monetization platform that uses TDS technology to connect web traffic from publisher affiliates to advertisers.Examples params: utm_medium=, utm_campaign=

Table 4. Concise table summary of advertising affiliate networks that we identified via TDS DNS analysis

Who Are the Website Hackers?

The adtech firms know.

Hundreds of thousands of compromised websites around the world every year redirect victims to the tangled web of VexTrio and VexTrio-affiliate TDSs. Not just last year, but every year since 2017, possibly as early as 2015. We have identified, in collaboration with other researchers, several hundred unique VexTrio affiliate ids associated with these hackers. These affiliates include “no name” actors, like the GitHub repo actor described earlier, and “big name” threat actors, like SocGholish and ClearFake. So, how can the affiliates be identified?

VexTrio and the other affiliate advertising companies know who the malware actors are, or they at least have enough information to track them down. Many of the companies are registered in countries that require some degree of “know your customer” (KYC), but even without these requirements, publishing affiliates are vetted by their customer managers. Typically, affiliates must demonstrate how they will publish smartlinks that lead into the network’s TDS. While there are some claims that it is easy to pass the vetting process, there are even more bewildered wannabe affiliates who are rejected. Los Pollos collects information like Telegram accounts and pays affiliates via cryptocurrency wallets.

Many advertising networks argue that they can’t be responsible for malicious affiliates who abuse their systems; after all, they just provide a connection between a publisher and an advertiser. But these claims fall flat for companies like Los Pollos. They both vet their publishing affiliates and claim the highest quality advertising in return for traffic. As a result, they not only have the information that can lead to the disruption of global WordPress hackers, but they also know the identities of the scam artists to which they connect innocent website visitors.

Indicators

A selection of current and historical indicators related to the malicious advertising affiliate networks that we described in this paper are available on our GitHub repo **here**. We have also included a table (see Table 5) of sample affiliate parameters connected to website compromises or malicious link distribution. Table 6 contains TDS domains that we described in this paper and are related to malicious adtech affiliate programs.

Affiliate Parameter	Notes
u=pe7k605	VexTrio affiliate associated with DNS TXT record campaigns. First seen 2019.
pl=CHiI7Gh3GUyTa8XGgNqDyQ	VexTrio affiliate associated with DNS TXT record campaigns. First seen 2023.
utm_medium=9eb2bcdc89976429bc64127056a4a9d5d3a2b57a	Monetizer affiliate associated with DNS TXT record campaigns. First seen November 24, 2024. This appears to be Los Pollos affiliate bt1k60t.
sub1=ct1qt1t109qc73fj4fsg	Partners House affiliate associated with DNS TXT record campaigns in November 2024.
id=1003455	Partners House affiliate that appears to be the same as Los Pollos affiliate (u=bt1k60t) and associated with DNS TXT record campaigns. Seen October 2024.

Table 5. Unique parameters for various malicious “publishing” affiliates

Domains	TDS Domain Owner
6[.]enlala[.]com 6[.]lands[.]ninja	RichAds
0[.]mo10[.]biz 0[.]se11[.]biz 0[.]to6s[.]biz 0[.]robotverifier[.]com 0[.]strongblackspaces[.]com 0[.]blueskyactivecontrol[.]com	BroPush
0605ee9ae7[.]hotbfocuhe[.]cc 01be885d26[.]hotbwixife[.]today 06254a045e[.]news-xkijeki[.]store 01afa41bf2[.]news-xceyuna[.]live 2765516796[.]news-xdujuwe[.]xyz	Partners House
7r6[.]fmqrsj[.]com 1azo7[.]iqfmvj[.]com 2rt[.]xcumpw[.]com d3l[.]wstbaw[.]com 3ic[.]ymehtq[.]com 2zhyl[.]iqfmvj[.]com gzeao[.]cavernexplorer[.]com gzeao[.]check-tl-ver-116-3[.]com gzeao[.]check-tl-ver-154-2[.]com mvgde[.]stonecoremason[.]com mvgde[.]runesmith[.]top mvgde[.]runicartisan[.]top mvgde[.]sec-tl-129-b[.]buzz mvgde[.]sec-tl-129-d[.]buzz	VexTrio
19a1[.]brpconnecta[.]digital 209c[.]brpteamwork[.]cc 43ff[.]rpstreamfx[.]xyz 5435[.]rpknowledge[.]xyz 9c3e1[.]rpdiscover[.]xyz c62a[.]rpbuildhub[.]xyz fe12[.]brpdataboxx[.]today	REXPUSH

Table 6. TDS domains operated by various advertising affiliate networks

Footnotes

1. **https://help.scaleo.io/article/414-los-pollos-affiliate-network**
2. **https://urlscan.io/result/0196d747-03d5-774f-9c16-8f5eab774d2b**