infoblox

Threat Intel

DNS PREDATORS ATTACK: VIPERS AND HAWKS HIJACK SITTING DUCKS DOMAINS

Authors:
Infoblox Threat Intel

TABLE OF CONTENTS

INTRODUCTION

It all began with a lookalike domain. The domain was crafted to look like a Slack hosting resource, but it was hosted in Russia. Simple phishing? Maybe. Except there was also a curious redirect chain. A long-registered CBS Interactive domain was being used to redirect potential victims to a fake Slack portal.[1] Could the TV network really have dropped the domain? Nope, it was still registered with Mark Monitor. However, reviewing the DNS resolution history, it was clear that after being idle for some time, the domain began resolving in Russia. It must have been hijacked. Back in January 2024, hijacking a high-value domain like `clickermediacorp[.]com` was assumed to be a sign of credential theft. We reported the hijacking to both the registrar and the DNS provider and moved on.

A few months later the topic of mysterious domain hijacking came up again. Researchers at Proofpoint were tracking a criminal traffic distribution system (TDS) called 404TDS that was connected to the distribution of malware and other malicious content. Our expertise is in DNS threat detection, and where others see malware to reverse engineer or web pages to dissect, we see actor fingerprints in how they configure DNS records and leave a trail of queries in the wake of their operations. We love TDS actors because a TDS is inherently woven into DNS configurations, and we're often able to see patterns that let us monitor the TDS as it evolves rather than wait for malicious payloads. We figured there must be a DNS signature for 404TDS.

1 https://urlscan.io/result/8ee644c6-2ad3-4cd9-a0e6-e05ad01ade5d/

As we began searching for a mechanism to track the 404TDS, it quickly became apparent that all the domains had been hijacked, including clickermediacorp[.]com. But the range of these hijackings was unusually broad, and the explanation of credential theft, or registrar hacks, didn't make sense. We teamed up with an Eclypsium researcher and began trying to find an explanation for the widespread domain hijacking tied to 404TDS.

We discovered that misconfigured DNS name servers were the common factor in all of the hijackings and that we could take over misconfigured domains at certain providers with a few button clicks. Even though we are DNS threat experts, this was new to us. And not just us—before publishing in July 2024, we talked to a broad set of people in government and industry, in threat research and networking. No one we spoke to for the first few months was aware of the attack vector and certainly not its mass exploitation. Brian Krebs remembered that he had covered a large campaign that used the technique, but at the time of his reporting, it looked like an issue at a single registrar and not a systemic problem.[2] We finally unearthed Matt Bryant's original reporting of the vulnerability, which we had coined Sitting Ducks, and realized actors had likely used the attack vector for at least eight years without detection.[3]

Our first paper about Sitting Ducks was intended to raise awareness of a little-known hijacking technique and to provide concrete actions for domain owners and registrants to take to secure their domains. We hoped it would spur action and not just by criminals. In our research, we have found that these vulnerable domains are often the result of mergers, acquisition, and history lost to personnel changes. While the domain clickermediacorp[.]com was secured after our July report, unfortunately, other CBS domains remain vulnerable. *If you are reading this Paramount Global and need help, give us a shout.* We worked with one victim organization to fix their domains because they had lost knowledge of the domains, but also the registrar credentials. And in the most alarming case, we worked with owners of .gov to fix their configurations.

Since our initial publication, we have identified nearly 800k vulnerable registered domains. Roughly nine percent (70k) of those vulnerable domains were subsequently hijacked. We know these numbers do not accurately reflect the attack surface: they are derived from a limited monitoring system. The challenge with a Sitting Ducks attack is that it is easy to perform and very hard to detect. Cybercriminals have used this vector since at least 2018 to hijack over 80k domain names, including those owned by well-known brands, non-profits, and government entities.

Sitting Ducks is not the only configuration-oriented attack vector we have seen this year: there were also multiple types of CNAME hijackings and even a WHOIS server takeover reported.[4,5] At a high level, governments and standards bodies also have roles to play in protecting users from these kinds of attacks. National and multinational organizations should both raise awareness and incentives to reduce risks for all configuration-related issues, including security requirements that incorporate safeguards from attacks like DNS hijacking. Unfortunately, many government organizations, including the U.S. Cybersecurity and Infrastructure Security Agency (CISA), focus on software vulnerabilities, and as a result, configuration vulnerabilities do not qualify for designation of a CVE, regardless of their potential criminal impact. For example, even registrants of a .gov TLD are only required to use a "competent" DNS provider. We have found that the consequence is that certain registrars create a lame delegation for new domain registrations by forcing a name server setting to be configured before the DNS provider records are established. It's a race against the clock, but one we have observed time and again. The lack of attention paid to these kinds of issues

2 https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

3 https://thehackerblog.com/floating-domains-taking-over-20k-digitalocean-domains-via-a-lax-domain-import-system/

4 https://labs.guard.io/subdomailing-thousands-of-hijacked-major-brand-subdomains-found-bombarding-users-with-millions-a5e5fb892935

5 https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/

allows their exploitation to continue largely unabated. Hopefully, we will begin to see both awareness training and proactive measures developed to address not just the Sitting Ducks attack vector but also the entire class of configuration vulnerabilities.

An all-too-common reaction is to point the finger back at the domain holder for ultimate responsibility to maintain their domain configurations. This may be true, but at the same time, both registrars and DNS providers can play a critical role in reducing cybercrime by making these types of hijacks harder to perform or easier to remediate. During our research, we reported Sitting Ducks hijackings to both registrars and DNS providers, but it was largely dismissed and not actioned, even though we provided evidence of the attacks. In many cases, we were unable to inform domain holders because they had used private registration information. In multiple cases when we did interact with compromised domain holders, they were unaware that they owned the domains, the memory and documentation lost over time and corporate mergers. The inability to reach domain holders implies that realistically, to reduce crime, both registrars and DNS providers should take a more active role in responding to information from threat intelligence organizations and minimize abuse of their platforms and users.

While researching the attack vector, we discovered over a dozen independent actors who were exploiting it. In this paper, we discuss several of those, including the operator of 404TDS and VexTrio Viper. We also introduce two new actors that we track: Horrid Hawk and Hasty Hawk.

The goal of this paper is to demonstrate specific ways in which these hijacked domains are used so they can be more readily identified and shut down. We will share:

- How to avoid a Sitting Ducks attack and identify a compromised domain
- How various threat actors leverage Sitting Ducks attacks to create an infrastructure resistant to security vendor detection
- How some Sitting Ducks threat actors affiliate with each other, indicating some kind of information sharing or underground economy for hijacked domains
- How some domains tied to major brands are hijacked repeatedly, often by different threat actors
- And how DNS is central to the detection and tracking of these persistent threat actors.

THE SITTING DUCKS ATTACK VECTOR

First, let's start with a recap. In July, we jointly published a report with Eclypsium on a widely exploited and underreported attack vector we call Sitting Ducks.[6] With this attack, the malicious actor gains full control of the domain by taking control of its DNS configurations. They can also hijack the domain without using credential theft or gaining access to the domain owner's registrar account—very sneaky. In most cases, these domains, or subdomains, have been forgotten by their original owner so the attack goes unnoticed. We have seen over a dozen threat actors abusing these hijacked domains to conduct a variety of criminal activities such as malware distribution, command and control (C2), phishing, traffic distribution system (TDS) operations, and more.

A Sitting Ducks attack takes advantage of misconfigurations in the DNS settings for a domain, specifically when the DNS points to the wrong authoritative name server. There are a few conditions that need to be met for an attacker to hijack a domain this way:

A registered domain or the subdomain of a registered domain uses or delegates authoritative DNS services to a different provider than the domain registrar; this is called **delegation**.

6 https://blogs.infoblox.com/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

- The delegation is **lame**, meaning the authoritative name server(s) of the record do not have information about the domain and cannot, therefore, resolve queries.
- The authoritative DNS provider is **exploitable**, meaning the attacker can "claim" the domain at the provider and set up DNS records without access to the valid owner's account at the domain registrar.

Figure 1 shows a common Sitting Ducks attack sequence. There are several variants of this type of attack, none of which requires compromising legitimate DNS infrastructure, thereby making it fundamentally different from better-known DNS hijacking techniques. Variations within this attack include redelegation to another DNS provider and partially lame delegation, meaning that only some of the authoritative name servers are misconfigured. The low technical barrier to entry gives many different cybercriminal groups the opportunity to exploit the vulnerability. This results in more attack instances that are difficult to detect because of the positive reputation that many of these hijacked domains have.

While Sitting Ducks attacks are easy to perform and difficult to detect, they are also entirely preventable with correct configurations at the domain registrar and DNS providers. Not all DNS providers are exploitable, however. After evaluating about a dozen of them, we've confirmed that hundreds of domain hijackings occur every day on exploitable providers: we've identified approximately 800k registered domains with lame delegations since August, but the true number is much higher; we have not included vulnerable subdomains and we limited our search to sample certain providers.

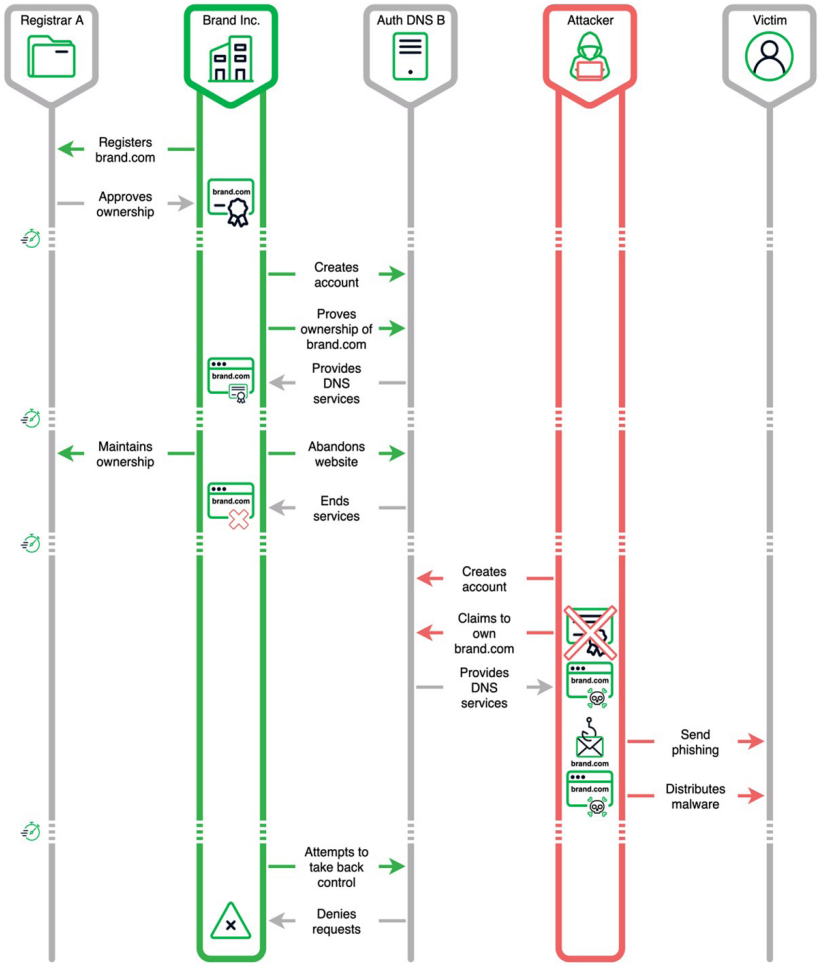

Figure 1. A common Sitting Ducks attack sequence

It is still unknown how threat actors identify vulnerable domains across providers. We have implemented multiple discovery methods, and through those, found that between six to ten percent of the domains assigned to exploitable DNS providers on a given day were lame. Some exploitable providers had significantly larger numbers of vulnerable domains, and given that our testing was limited, the true exploitable landscape is probably much larger than we know today. Overall, we estimate that over 1M registered domains are vulnerable to a Sitting Ducks attack on a given day. Most vulnerable domains we have discovered have name servers assigned to one of a small handful of DNS providers.

Now, let's take a look at some of the actors using this attack vector.

VACANT VIPER

What's in a Name?

Vacant Viper is the name we've given to the threat actor that operates the 404TDS, first reported by Proofpoint.[7] As a practice, Infoblox doesn't rename established actors or infrastructure components. When we refer to 404TDS, we're discussing the TDS itself, and when we refer to Vacant Viper, we're discussing the actor who hijacks domains for 404TDS and engages in other malicious activities like spam.

While studying 404TDS for a DNS signature that could predict a domain would become part of the TDS infrastructure, we realized the domains were hijacked. Moreover, looking carefully at the compromised domains, it seemed the actor was up to more than just operating a criminal TDS. We named the hijacking actor Vacant Viper, using our viper category as a nod to the TDS origins.

Vacant Viper is one of the earliest known threat actors to exploit Sitting Ducks and has hijacked an estimated 2500 domains each year since December 2019. This actor uses hijacked domains to run malicious spam operations, deliver porn, establish remote access trojan (RAT) C2s, and drop malware such as DarkGate and AsyncRAT, along with their 404TDS operations.[8] Their reported affiliates include TA-866 and TA-571.

Vacant Viper abuses DigiCert DNS companies but prefers free accounts at DNS Made Easy, which are available for a thirty-day trial period and require only an email address to set up. However, they have also hijacked domains at Constellix, a premium DNS service that requires engagement with sales representatives before a free trial. Since we first reported on Sitting Ducks attacks in July 2024, the actor has adjusted their techniques but continues to operate exclusively on this set of providers. The amount of hijacking they conduct varies over time but, for example, we identified approximately 100 domains hijacked by Vacant Viper in the first two weeks of October 2024.

Vacant Viper does not hijack domains for a specific brand connection, but instead for a set of resources that have high reputations and will not be blocked by security vendors. Vacant Viper also hijacks some domains repeatedly over time. For example, `clickermediacorp[.]com` was seen in January 2024 as part of the 404TDS and associated with a phishing campaign mimicking Slack, but the domain was previously used in January 2020 to deliver a variety of content, including pornography and bitcoin scams.

A key feature of a TDS is to have affiliates: suppliers who send traffic into the TDS, and customers who receive traffic from the TDS. In the advertising world, the goal of a TDS is to maximize profits, that is, to route users to the ad they are most likely to like. The goal of a criminal TDS is similar: lure users with content they are most likely to want to consume, then

7 https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

8 https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

route them to the malicious content, whether that be a malware download, a fake login page, or a gift card scam.

The following examples of 404TDS attack chains show redirection techniques used both by the TDS and their affiliates, including how Vacant Viper uses hijacked domains in the 404TDS.

One domain that Vacant Viper hijacked and used in the 404TDS is `mcpennsylvania[.]com`, a domain registered by McDonald's with corporate registrar CSC Corporate Domains and assigned to name servers on DNS Made Easy, a subsidiary of DigiCert.[9] Vacant Viper has hijacked this domain repeatedly over the last few years, and it has a lame delegation as of this writing. Most recently, we observed this McDonald's domain redirecting to `ncbtv[.]com` (formerly operated by an IPTV service provider), which was registered with GoDaddy in 2011, originally with a Chinese email address. Ironically, this domain too, now covered under private registration, also appears to have been hijacked with a Sitting Ducks attack multiple times, possibly as early as 2017. Most recently, `ncbtv[.]com` has been associated with VexTrio Viper, a threat actor who uses hijacked domains to host dating sites and other content. Assuming this actor is independent of Vacant Viper, we can see that threat actors who use Sitting Ducks attacks cooperate with each other and likely share knowledge and/or resources for vulnerable domains.

In June 2023, when Vacant Viper hijacked `mcpennsylvania[.]com`, they used it for 404TDS in an AsyncRAT malware attack chain and leveraged two different mechanisms (meta refresh and HTTP refresh) to redirect the user:[10]

- The URL `hXXps://mcpennsylvania[.]com/y0t/gojhuovy` showed a 404 (Not Found) error, but behind the scenes a meta refresh was performed to redirect the user via the HTML meta tag:
  - `<meta http-equiv="refresh" content="0;hXXps://ecole-artcom[.]com/wdown">`
- The second URL `hXXps://ecole-artcom[.]com/wdown/` responded with no content except a refresh HTTP header, which effectively redirected the user again to a third URL
- The third URL `hXXps://www[.]mediasimulasi[.]com/wazxd` dropped a JavaScript file named Information_28_jun_1220107.js, which then went on to download files associated with AsyncRAT[11]

While it is unknown who controls the landing domains, they have been observed only in connection with 404TDS. We show the headers for the `mcpennsylvania[.]com` attack chain in Figure 2.

9 https://who.is/whois/mcpennsylvania.com

10 https://urlscan.io/result/14797fe3-beaf-4949-9d04-6edcf94b25aa/#transactions

11 https://github.com/executemalware/Malware-IOCs/blob/main/2023-07-05%20AsyncRAT%20IOCs

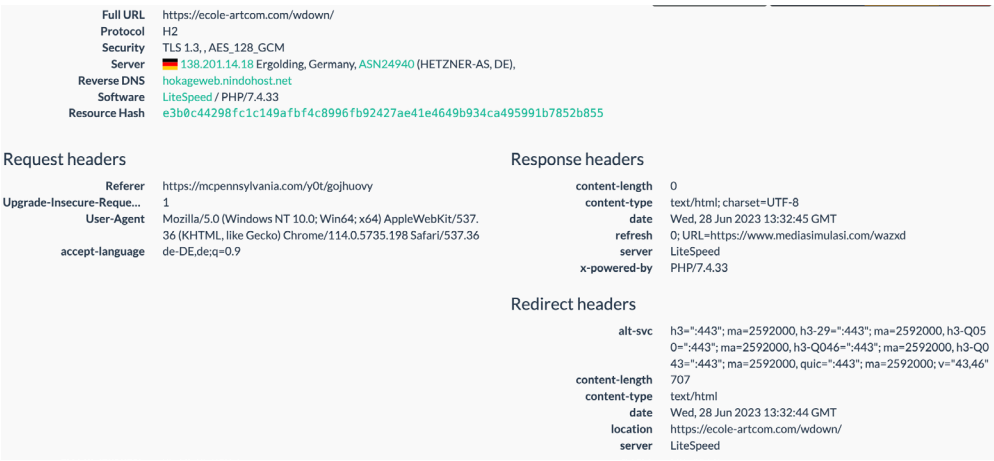

Figure 2. Refresh headers redirected users to hXXps://www[.]mediasimulasi[.]com/wazxd

Vacant Viper also used the HTML meta refresh technique in attack chains that distributed DarkGate malware through malicious spam attachments. The redirection chain for DarkGate malware delivery[12] is similar to that of the one above for AsyncRAT, but does not include the HTTP refresh method:

1. The user attempts to reach afarm[.]net resulting in a 404 Not Found error
2. TDS URL hXXps://afarm[.]net/uvz2q then redirects to https://wercosliuhqgheirn[.]com/ via the HTML meta refresh method <meta http-equiv="refresh" content="0;hXXps://wercosliuhqgheirn[.]com/">
3. The user is redirected to hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php which downloads the following file containing DarkGate malware:

Filename	SHA-256 Hash
08-May-24-document-53aa77b6.jar	f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a

The eight domains in Table 1 all follow the same redirection pattern to deliver the same JAR file associated with DarkGate.[13] We've seen six of these domains in similarly named spam file attachments, e.g., may-document_85138492.pdf, in May 2024. All of these files are distributed as attachments to malicious spam emails with a similar generic body message referencing an attached bill or expense document that the user is encouraged to open so that they can provide payment.

aerospaceavenue[.]com	affiliatebash[.]com
affixio[.]com	amikamobile[.]com
adventsales[.]co[.]uk	afcmanager[.]net
afarm[.]net	adztrk[.]com

Table 1. Hijacked domains Vacant Viper used to distribute DarkGate malware

12 https://urlscan.io/result/1f4d4a62-8a6f-4452-b64c-1d38b3cd6086/#summary

13 https://bazaar.abuse.ch/sample/f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a#intel

While Vacant Viper research led to our (re-)discovery of the Sitting Ducks attack vector, it also allowed us to tie other threat actors to the attack vector. Some of these actors were being tracked, and some were not. In general, we have found it extremely difficult to discover a compromised domain by itself; we have used threat actor behavior to back into a signature that can then be tracked. For threat actors that leverage DNS hijacking, we use the naming category of a hawk.

Why a Hawk?

These threat actors swoop in and hijack vulnerable domains, much like hawks dive down to snatch their prey.

HORRID HAWK

Horrid Hawk is a DNS threat actor that has been hijacking domains and using them for investment fraud schemes since at least February 2023. They are interesting because they use hijacked domains in every step of their recent campaigns, and they craft convincing lures about non-existent government investment programs or summits. They embed the hijacked domains in short-lived Facebook ads that target users in over 30 languages spanning multiple continents. We track Horrid Hawk through DNS and have identified nearly 5k of their hijacked domains.

A Horrid Hawk attack chain involves two different hijacked domains; most often they have been hijacked from a few DNS providers: Linode, TierraNet, and A2 Hosting. After they hijack a domain, Horrid Hawk re-configures the A record IP address to a different dedicated server. The actor assigns one of the domains to a TDS server that shields the landing webpage from security researchers and filters out unwanted web visitors. Horrid Hawk assigns the other domain to the landing webpage that hosts fraudulent investment content. Early in their history, Horrid Hawk also registered their own lookalike domains that fit with the government investment themes, such as `oil-poland[.]site` and `balticpipe[.]playroom8[.]site`. The actor used these domains for their landing webpages that hosted content related to gas project scams. Figure 3 shows the timeline of two domains that they hijacked and used together in an attack.

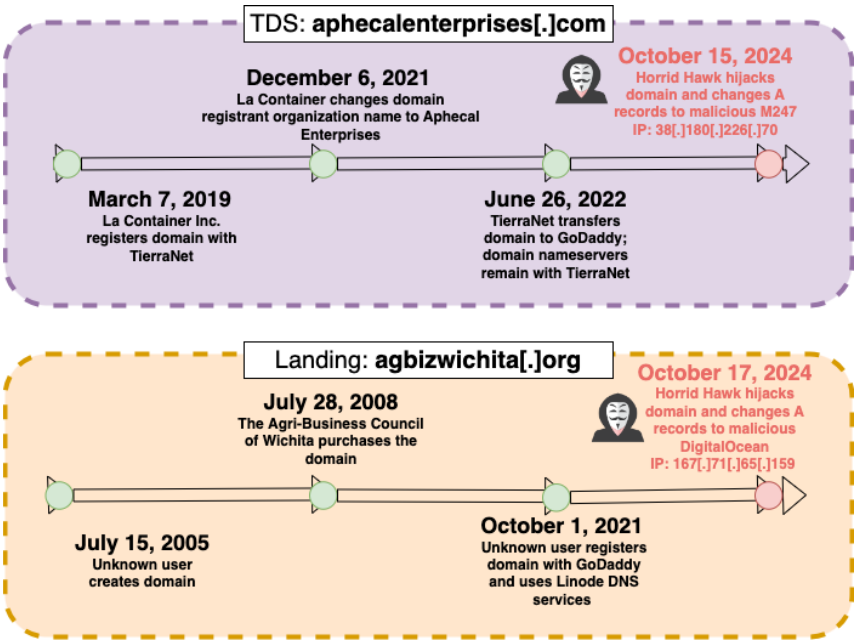

Figure 3. Domain hijacking timeline of `aphecalenterprises[.]com` *(TDS) and* `agbizwichita[.]org` *(landing page domain)*

Horrid Hawk preys on consumers around the world. They begin their attacks by creating many Facebook ads like the one in Figure 4, which targets users in Poland and advertises a fake government-funded gas project, the Baltic Pipe. The image used in the Facebook ad contains a message that urges users over 50 to click the ad link and read the contents of the web article. This Facebook ad campaign reached over 13k internet users. Although the example that we use in this section is a campaign that targets senior Polish-speaking users, Horrid Hawk also employs phishing lures in English, Italian, Turkish, Spanish, and many other languages.

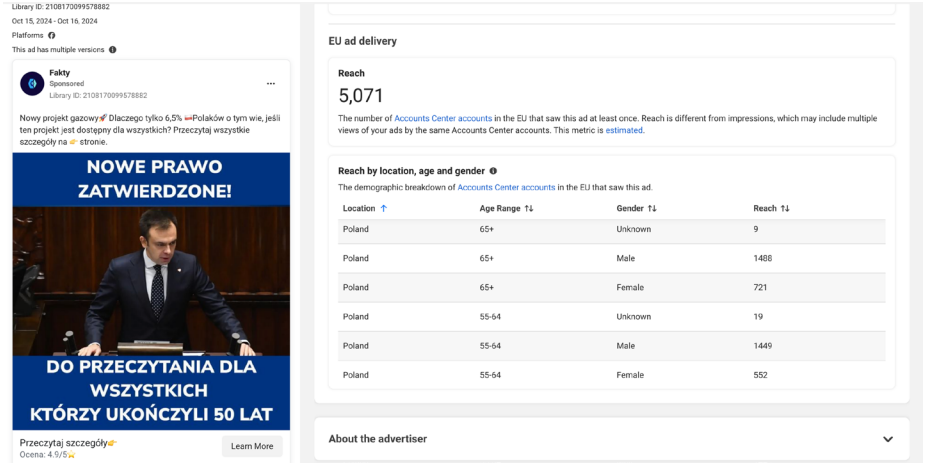

Figure 4. Example of a Horrid Hawk Facebook advertisement targeting Polish-speaking users who are mostly over the age of 55

The advertisement link shown in Figure 4 points to `hXXps://aphecalenterprises[.]com/`, a URL used by the Horrid Hawk TDS server. This system is important to the threat actor because it protects the scam landing page by profiling web visitors and filtering out irrelevant and unwanted guests, such as security researchers and web-scraping bots. The server uses geolocation information to determine the next URL location for the web visitor. For example, if a user navigates to `hXXps://aphecalenterprises[.]com/` from a Poland-based IP address, Horrid Hawk will redirect them to the government-themed scam web page located at `hXXps://agbizwichita[.]org/9fMS3XSS`. The random URL path 9fMS3XS is only temporary, and this website will load a static file (/lander/long-ready-2_0/index.html) that is referenced by the base HTML href attribute. Figure 5 is the webpage we saw when this URL was still active.

Figure 5. Politically themed scam webpage (`hXXps://agbizwichita[.]org/lander/long-ready-2_0/index.html`) targeting Polish-speaking users

If the website visitor's IP address is in a country that is irrelevant to Horrid Hawk's target audience, those users will usually be redirected to a decoy web page that uses the same TDS domain. For example, when we visited `aphecalenterprises[.]com` with an IP address outside of Poland, the TDS served us a benign webpage imitating an online apparel store. Figure 6 shows the URL structure and contents of the decoy web page. URLs for decoy webpages contain a file name with the static prefix `w-{country code}-`. The country code in this instance was "pl", an abbreviation for the target country Poland and the "w" possibly stands for white cover or white label.

Figure 6. A decoy webpage served by Horrid Hawk TDS for non-targeted web visitors

The most prevalent theme we've seen on the various webpages has been related to "The Baltic Pipe Project," an investment scheme that claims Polish citizens who invest in new gas pipelines can earn large sums of money. In the above example that involves the `agbizwichita[.]org` landing page, Horrid Hawk uses a scare tactic taking advantage of people's natural fear of missing out (FOMO). The webpage claims that citizens who do not participate in the government-funded gas project will incur a 55% increase in gas-related expenses. Similar to investment campaigns operated by another investment scheme actor we reported on this year, Savvy Seahorse,[14] the Baltic Pipe campaigns ask the user to enter their personal details, including name, email, and phone number, in an embedded form to register for the investment opportunity. Users are then informed they will be contacted for additional information before they can access the "investment platform." See Figure 7. Although other threat actors run Baltic Pipe scams, Horrid Hawk stands apart in their use of Sitting Ducks attacks to hijack domains.[15]

14 https://blogs.infoblox.com/threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/

15 https://urlscan.io/result/61541987-122b-484d-acdc-290f02f98a8b/

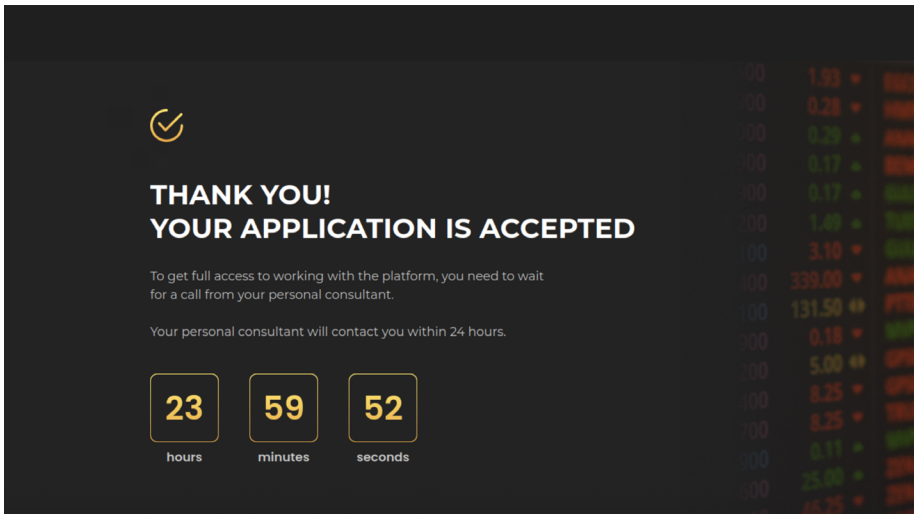

Figure 7. A typical Horrid Hawk response page delivered after a victim successfully registers on the scam websites

HASTY HAWK

Hasty Hawk is another threat actor we discovered during our research into Sitting Ducks hijackings. Since at least March 2022, Hasty Hawk has hijacked over 200 domains to operate widespread phishing campaigns that primarily spoof DHL shipping pages and fake donation sites to support Ukraine. The actor exploits many providers, including HawkHost, Maria Hosting, and DigitalOcean. Hijacked domains are often reconfigured via DNS to host content on Russian ASNs such as PROTON66 or BEGET, but the actor has also been known to use other providers such as OVH. Hasty Hawk uses Google ads and possibly other means such as spam messages to distribute malicious content.

Hasty Hawk's fully qualified domain names (FQDNs) tend to follow a few patterns such as the following:

- `dhl.<random numbers>.<hijacked domain>`
- `dhl-id<random numbers>.<hijacked domain>`
- `<random numbers/letters>.dhl.<hijacked domain>`

Figure 8 shows the DNS record changes for `thebagshelf[.]com` from its creation date and the day it was hijacked by Hasty Hawk. Similar to Horrid Hawk, Hasty Hawk also re-configures the A record address to a server that is dedicated to the actor. In addition to the DHL subdomain name prefixes such as `dhl[.]3204[.]thebagshelf[.]com`, we've observed other static subdomain name prefixes on these servers including `id-f<random number>.<hijacked domain>` (e.g. `id-f0596[.]successbusinesspages[.]com`).

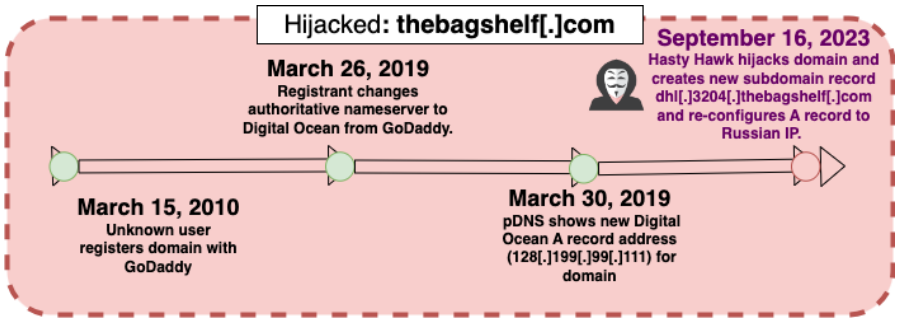

Figure 8. Domain hijacking timeline for `thebagshelf[.]com`

Hasty Hawk recently switched many of their DHL-themed webpages to fake donation sites that are mirror copies of the legitimate site, supportukrainenow[.]org, run by the Global Shapers organization[16] to support Ukraine during the war (see Figure 9). The actor has also created pages spoofing the European Union with another fake donation site that targets Europeans looking to support victims of the war.

Figure 9. Fake donation site spoofing supportukrainenow[.]org

Hasty Hawk uses a TDS to route users to different webpages that vary in content and language depending on their geolocation, and possibly other user characteristics. When users see different content based on the device they use, their location, or at different times, it is a clear indication that a TDS is at work in the background, ensuring that victims are routed to the page that profits the criminals most. Hasty Hawk also switches some of their domains back and forth between various campaign themes. Let's look at the example in Figure 10 of geolocation-based redirections and changes in webpage content over time for the FQDN dhl[.]3204[.]thebagshelf[.]com.

16 https://www.globalshapers.org/home

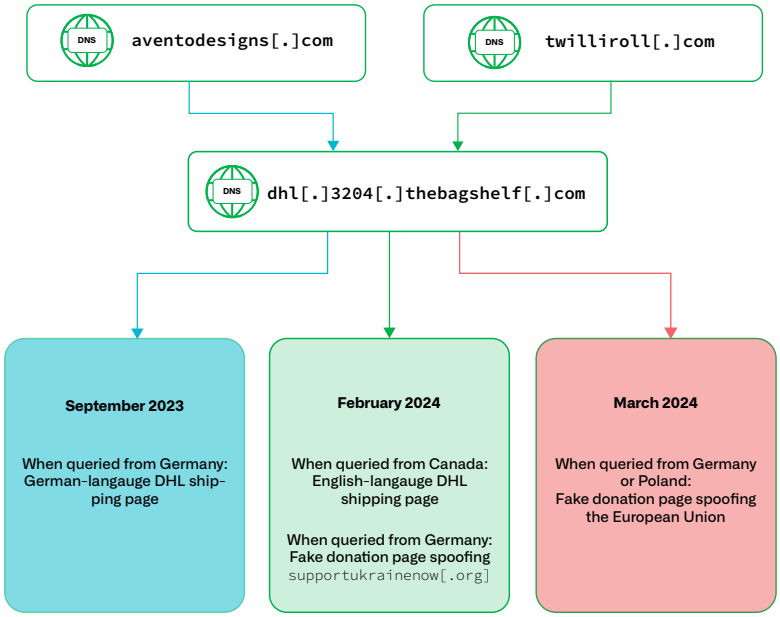

Figure 10: Example of redirections toward `dhl[.]3204[.]thebagshelf[.]com` *and some of the webpages the actor has displayed over time*

1. **September 2023** – The FQDN hosts a German-language DHL shipping page. Users were redirected there from `aventodesigns[.]com`.[17]
2. **February 2024** – The FQDN hosts both an English-language DHL shipping page (redirected from `twilliroll[.]com`) for users in Canada and the fake donation page spoofing `supportukrainenow[.]org` for users in Germany.
3. **March 2024** – The FQDN switches IPs from `91[.]212[.]166[.]71` to `91[.]212[.]166[.]14` and hosts the Ukraine support page spoofing the European Union for users in Germany and Poland.

Hasty Hawk continued to change the campaign themes for this single FQDN over the course of 2024. As of September, the FQDN was hosting the English-language DHL shipping page shown in Figure 11 or redirecting to a CAPTCHA page requiring the user to "complete the security check to access `dhl[.]com`," redirecting to the legitimate DHL website as a decoy.[18]

17 https://urlscan.io/result/520f01c1-c3cf-48ad-9295-95bbd671ea50

18 https://urlscan.io/result/1998c142-5292-4895-98bd-17c04394286b

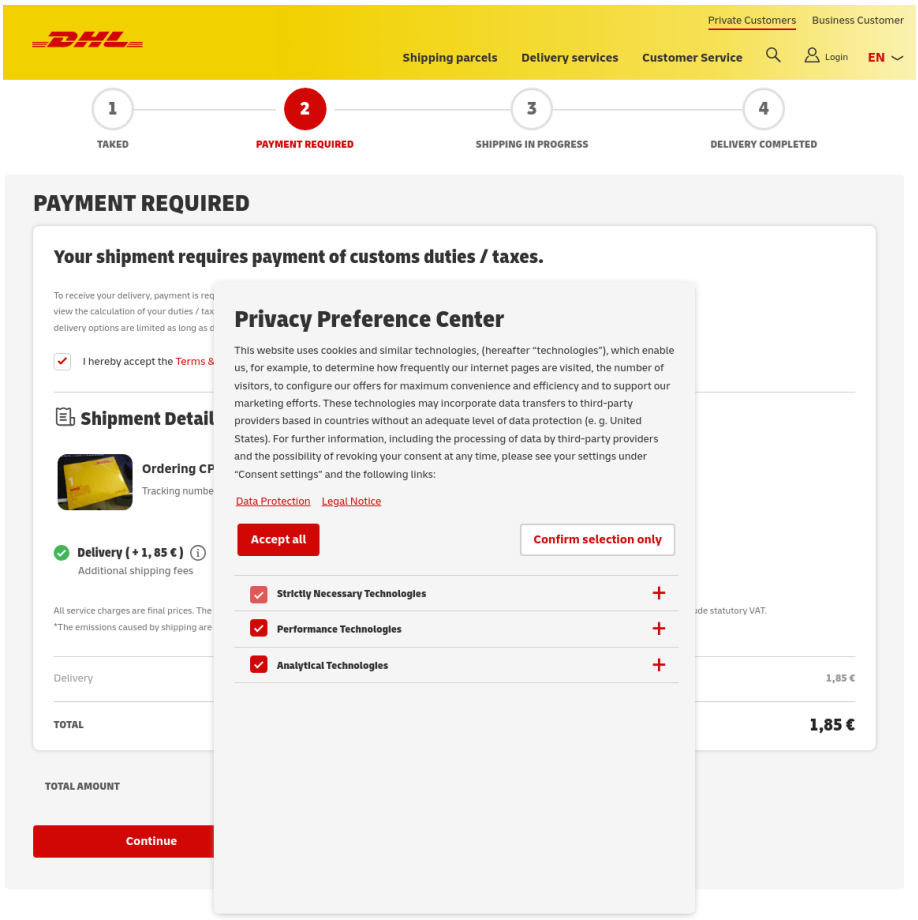

Figure 11. DHL phishing page for `dhl[.]3204[.]thebagshelf[.]com` *in September 2024*

VEXTRIO VIPER AND AFFILIATES

As our research led us to discover more and more Sitting Ducks-hijacked domains, we recognized some as being part of the massive VexTrio Viper TDS infrastructure since early 2020. These domains initially stood out to us because of their age, but once we discovered they were hijacked, the missing piece fell into place. Essentially, VexTrio Viper uses hijacked domains in their TDS in a similar way to Vacant Viper. VexTrio runs the largest cybercriminal affiliate program routing compromised web traffic from over 65 affiliate partners, some of whom have also stolen domains via Sitting Ducks for their own malicious activities.

VexTrio has hijacked lame domains that were once delegated to DigiCert/DNS Made Easy (DME), Constellix, and DigitalOcean nameservers to operate their TDS servers. The hijacked domains route traffic to their downstream malicious content publishers, or their own malicious sites, which host fake dating and gift card scams, fake robot CAPTCHA notifications, etc.

One of the more notable examples is `mpinc[.]com`. We've confirmed that VexTrio hijacked the domain in August 2023, but they may have compromised it as early as April 2022. The original owner of this domain is MPR Associates, an organization focused on education research. This domain was mostly active in the 1990s and 2000s before it was acquired in 2013 by RTI International (`rti[.]org`), a nonprofit research institute specializing in social, scientific, and health issues. The domain was switched over to DME nameservers in late 2015. According to pDNS, `mpinc[.]com` was parked at a DigitalOcean IP (`157[.]230[.]67[.]179`) for three months starting in January 2022 before it was hijacked in April 2022 by a threat actor,

most likely VexTrio. While under VexTrio's control from August to October 2023, the domain redirected users to one of the actor's commonly used fake dating sites shown in Figure 12.[19,20] Currently, `mpinc[.]com` is in lame status and not delegated to an authoritative DNS server.

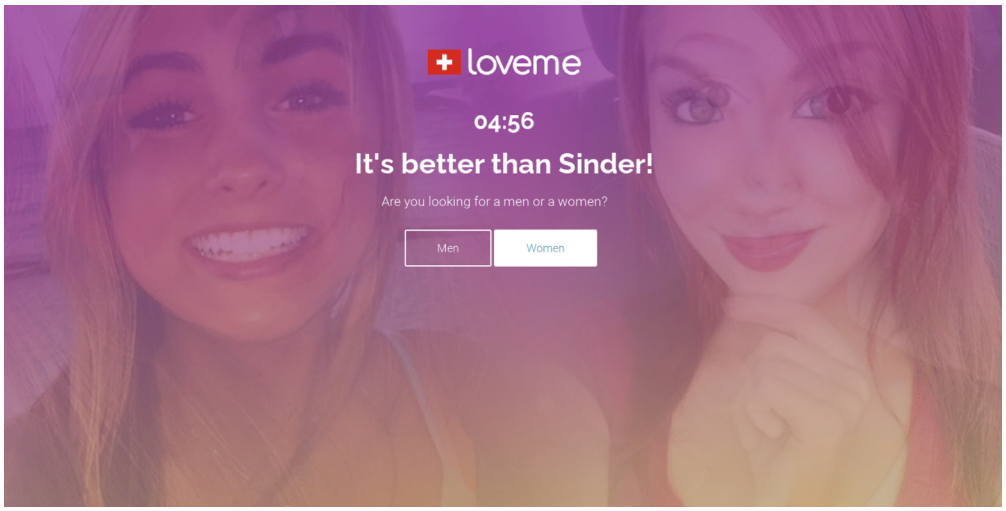

Figure 12. Fake dating webpage for hijacked domain `mpinc[.]com`

VexTrio also hijacked `iccps[.]org`, a domain previously used for the annual ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). The domain was registered as early as September 2009 by a professor at Carnegie Mellon University. According to WHOIS information, we assess this domain, once delegated to DME nameservers, became exploitable starting in early August 2023. VexTrio then used it in their TDS infrastructure, routing users to their campaigns from September to October 2023. It then resolved to the DigitalOcean IP address used for expired domains, and then eventually was parked on a Bodis IP, where it currently remains. ACM/IEEE now uses `iccps[.]acm[.]org`[21] for their conference.

VEXTRIO VIPER AFFILIATES USE ANTIBOT CLOUD

We've also seen VexTrio Viper affiliates exploit Sitting Ducks. Many of them use AntiBot Cloud, a Russian antibot service, as a method to filter out bots and traffic from security researchers. The functionality of AntiBot includes the ability to set rules to block certain bot services or users based on their information such as their IP geolocation and user-agent. Users can run this service for free locally with limited bot protection or upgrade to the cloud premium version. On the surface, AntiBot Cloud doesn't appear to be inherently malicious, but the majority of the user base appears to be cybercriminals. The service, favored by Russian and other Eastern European cybercriminals, was originally written in Russian, later expanded to English content, and features the Russian Ruble as one of its primary payment options (see Figure 13). AntiBot appears to be managed entirely by one person using the alias MikFoxi, who self-advertises as a freelance programmer. It's also important to note that only the affiliates and not VexTrio Viper themselves use AntiBot – blocking AntiBot will not block VexTrio. The FQDNs for the AntiBot cloud service include:

19 https://urlscan.io/result/7948b668-5226-4670-9b54-63d1da91fee2

20 https://iccps.acm.org/2025/

21 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

- hXXps://antibotcloudapi[.]com/9.php
- antibotcloudapi[.]com
- antibot[.]cloud
- antibotcloud[.]com
- ipv4[.]mikifox[.]com
- ipv6[.]mikifox[.]com
- admin[.]mikifox[.]com

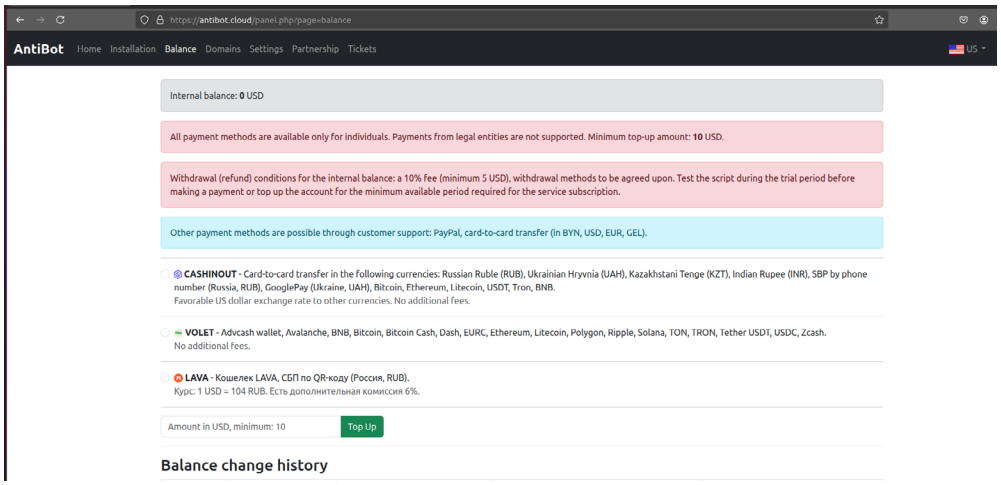

Figure 13. AntiBot payment options, including the Russian Ruble

One affiliate using AntiBot hijacked missouri[.]com[22] via DME in October 2022, but this domain may have been previously stolen by other threat actors even earlier. While the domain was controlled by this affiliate, users were redirected to a fake dating site operated by VexTrio Viper. Prior to the first hijack, the website that used missouri[.]com was developed by State Ventures, LLC and was possibly related to the State of Missouri. The domain previously showed a large number of subdomain records dedicated to Missouri cities and counties. The cached data shows it was a site rich with content related to the state's businesses and tourism, as shown in Figure 14 below. Additionally, the former Missouri Lottery website was potentially assigned to the subdomain lottery[.]missouri[.]com. Their content is now hosted at molottery[.]com, which also uses DME name servers.

22 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

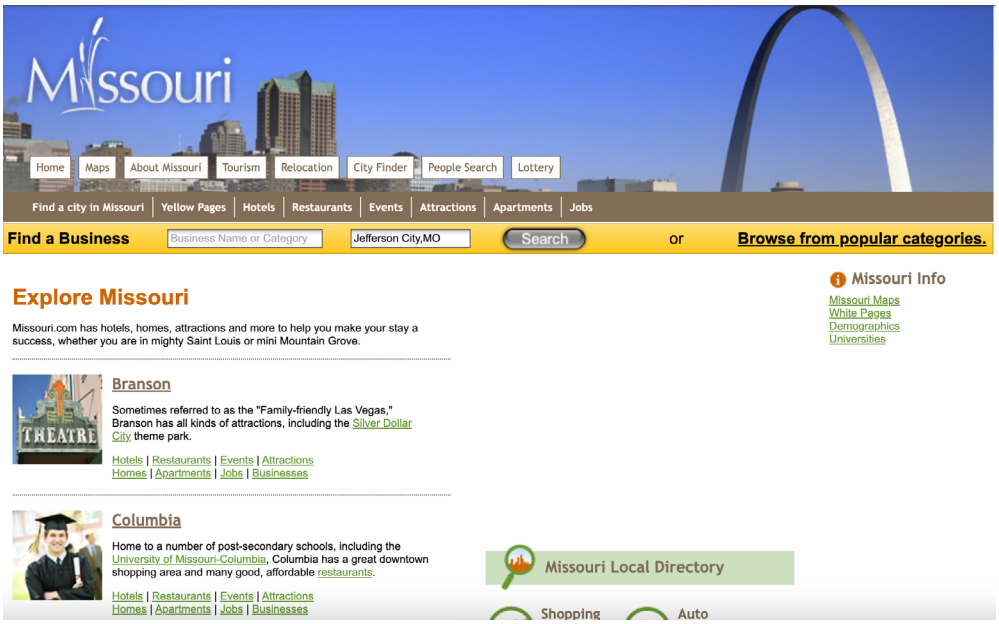

Figure 14. Web page for `missouri[.]com` *in September 2018, possibly the official page for the State of Missouri before being hijacked*

VEXTRIO GOREFRESH AFFILIATE

GoRefresh is a VexTrio Viper affiliate that operates fake online pharmaceutical campaigns and participates in other affiliates' campaigns such as online gambling or dating scams. GoRefresh has hijacked domains from vulnerable DNS service providers DME and GoDaddy. This affiliate uses these hijacked domains to redirect compromised web traffic to VexTrio and other affiliates, as well as to its own pharma landing pages.

Similar to Vacant Viper, GoRefresh typically responds to users with a HTTP 404 Not Found error response status code. Alternatively, when they dedicate a resource as a redirector, they forego providing the traditional HTTP 302 redirect response and instead "refresh" the victim's webpage to the next URL via an HTML meta refresh. An example of this HTML code redirection:

```
<meta http-equiv="refresh" content="0;http://vipshopevent[.]su">
```

ROTATIONAL HIJACKING

A common occurrence we've seen while researching Sitting Ducks is rotational hijacking: when one domain is hijacked by multiple actors over time. Threat actors often use exploitable service providers that offer free accounts like DNS Made Easy as lending libraries, typically hijacking domains for 30 to 60 days; however, we've also seen other cases where actors hold the domain for a long period of time. After the short-term, free account expires, the domain is "lost" by the first threat actor and then either parked or claimed by another threat actor.

We've seen VexTrio Viper affiliates do this quite frequently, especially when hijacking domains that were previously compromised by Vacant Viper. As an example, in Figure 15 below we show the hijacking timeline for `mcpennsylvania[.]com`, which was first hijacked by Vacant Viper and later by a VexTrio Viper affiliate. According to WHOIS information, the registrar (CSC Digital Brand Services) and name server provider (DME) remained largely unchanged throughout the various hijackings.

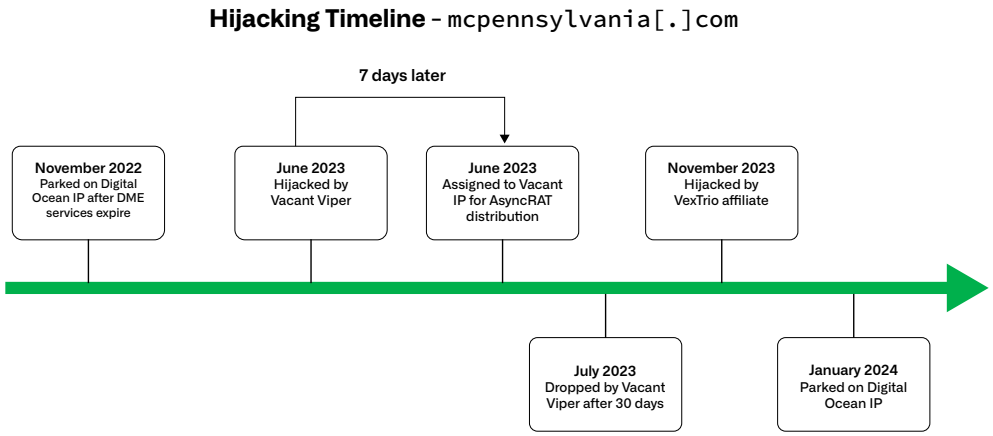

Figure 15. Hijacking timeline for mcpennsylvania[.]com

CONCLUSION

The threat actors we've profiled are just a sample of those who have capitalized on this powerful and obscure attack vector. While the effects of the Sitting Ducks attack vector are far-reaching, they are also entirely preventable, if complicated to address. Actors will continue to exploit this attack vector if no active efforts are made for mitigation and, ultimately, prevention. As we shared in our disclosure blog, everyone has a role in stopping Sitting Ducks attacks—from authoritative DNS providers and registrars to government organizations and standards bodies. We need better ways to detect hijackings and mitigate them as quickly as possible. Legitimate domain registrants need to not only maintain their DNS records but be responsive to reports of abuse, as do both registrars and providers.

Because this attack is so hard to detect, there is little doubt that threat actors will continue to leverage it. We have found several actors who have hijacked domains and held them for extensive periods of time, but we have been unable to determine the purpose of the hijack. These domains tend to have a high reputation and are not typically noticed by security vendors, creating an environment where clever actors can deliver malware, commit rampant fraud, and phish user credentials without consequences. Hopefully, as the threat intelligence community becomes more aware of the technique, they will highlight actor usage and allow for tracking and remediation of hijacked domains.

While Infoblox products are not vulnerable to Sitting Ducks, our customers may still be impacted depending on how they have chosen to operate DNS for the domains they register. Therefore, we recommend all domain name owners, especially those who use third-party DNS systems and are unaware of their service status, evaluate their risk level by following the three questions in Figure 16.

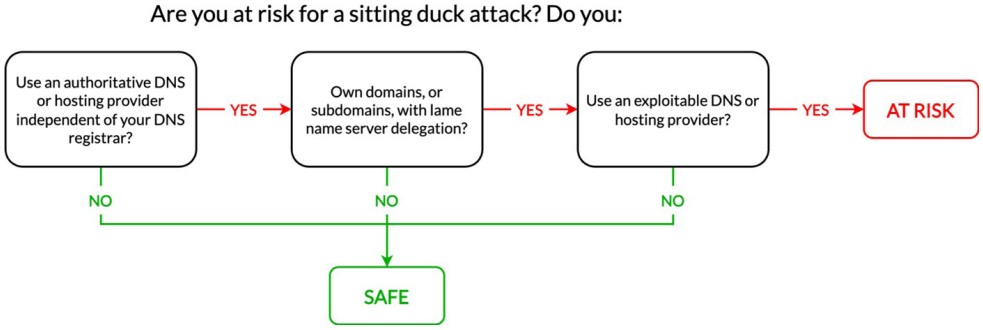

Figure 16. Three questions to determine if you're at risk for a Sitting Ducks attack

SITTING DUCKS VICTIMS

The hijacked domains that we described in this report belonged to legitimate organizations across various industry verticals. A domain can have multiple different owners during its lifetime. The following listing includes the legitimate owners that we identified before their domains were hijacked.

Hijacked Domain	Legitimate Domain Owner
agbizwichita[.]org	Agri-Business Council of Wichita
alonbyacarian[.]com	Acarian Systems Alon Capri Loudspeakers
aphecalenterprises[.]com	Aphecal Enterprises Inc.
clickermediacorp[.]com	CBS Interactive
iccps[.]org	International Conference on Cyber-Physical Systems
jmnet[.]com	JM Eagle
mbhs[.]com	MISSISSIPPI BAPTIST HEALTH SYSTEMS, INC.
mcpennsylvania[.]com	McDonald's Corporation
missouri[.]com	State Ventures, LLC and possibly State of Missouri
mosaicmedicalsupply[.]com	Mosaic Medical Supplies (orthopedic and cosmetic supplier)
mpinc[.]com	MPR Associates (law firm)
mstouchenaturals[.]com	MS TOUCHE
mygemcon[.]com	Gemcon Group
ncbtv[.]com	NCBTV (IPTV service provider)
successbusinesspages[.]com	Success Business Pages (Online business directory)
thebagshelf[.]com	Thai online apparel store
tmsec[.]com	T&M USA (Private Security & Investigations Company)
uni-t[.]com	Bridgestone - Firestone Tire Sales Company

INDICATORS OF ACTIVITY

The table below provides indicators of activity (IOAs) used by these threat actors; for more, go to the Infoblox Threat Intelligence GitHub repo: `https://github.com/infobloxopen/threat-intelligence/tree/main`.

Indicator	Type	Note
oil-poland[.]site balticpipe[.]playroom8[.]site	Domain	Lookalike domains registered by Horrid Hawk and used in their campaigns
mstouchenaturals[.]com covidianmuseum[.]com alhej[.]com agbizwichita[.]org aphecalenterprises[.]com	Domain	Hijacked domains used in Horrid Hawk campaigns
thebagshelf[.]com successbusinesspages[.]com aventodesigns[.]com twilliroll[.]com	Domain	Hijacked domains used in Hasty Hawk campaigns
aerospaceavenue[.]com affixio[.]com adventsales[.]co[.]uk afarm[.]net affiliatebash[.]com amikamobile[.]com afcmanager[.]net adztrk[.]com clickermediacorp[.]com mcpennsylvania[.]com	Domain	Hijacked domains used in Vacant Viper campaigns
mpinc[.]com iccps[.]org jmnet[.]com ncbtv[.]com uni-t[.]com tmsec[.]com mbhs[.]com	Domain	Hijacked domains used in VexTrio Viper campaigns

Indicator	Type	Note
missouri[.]com mcpennsylvania[.]com	Domain	Hijacked domains used in AntiBot Cloud affiliate campaigns
mosaicmedicalsupply[.]com	Domain	Hijacked domains used by VexTrio GoRefresh affiliate
vipshopevent[.]su	Domain	Domain used in VexTrio GoRefresh pharma campaigns
alonbyacarian[.]com fixedsights[.]com mygemcon[.]com sauda-pati[.]com tewksenterprises[.]com ummatie[.]com xiangmanlou[.]com	Domain	Hijacked domains used by health scam actor
hXXps://ecole-artcom[.]com/wdown/ hXXps://www[.]mediasimulasi[.]com/wazxd	URL	URLs associated with AsyncRAT download
https://wercosliuhqgheirn[.]com/ hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php	URL	URLs associated with DarkGate download
hXXps://antibotcloudapi[.]com/9.php antibotcloudapi[.]com antibot[.]cloud antibotcloud[.]com ipv4[.]mikifox[.]com ipv6[.]mikifox[.]com admin[.]mikifox[.]com	FQDN	FQDNs used in AntiBot Cloud service

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: 20241030v1