infoblox

Threat Intel

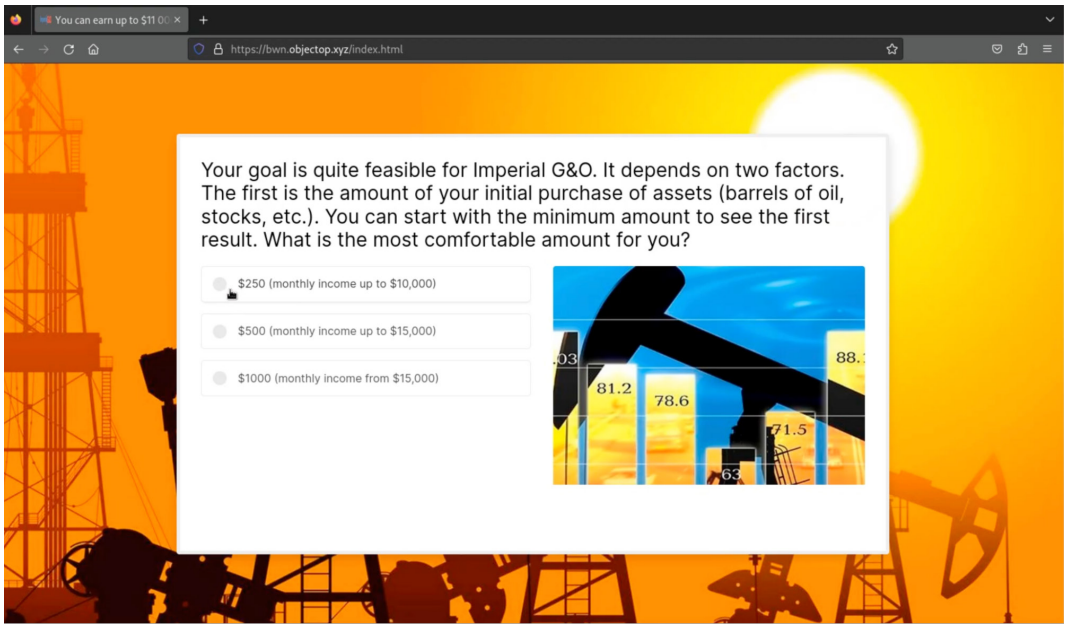
BEWARE THE SHALLOW WATERS: SAVVY SEAHORSE LURES VICTIMS TO FAKE INVESTMENT PLATFORMS THROUGH FACEBOOK ADS

Authors:
Stelios Chatzistogias
Laura da Rocha
Darby Wise

TABLE OF CONTENT

EXECUTIVE SUMMARY

DNS threat actors never cease to surprise us. Every day, we learn about creative, new campaigns they have devised to exploit victims. Investment scams are one of these. The US Federal Trade Commission reported that more money was lost to investment scams in the US during 2023 than any other type of scam, totaling over USD $4.6 billion dollars stolen from victims.[1] Savvy Seahorse is a DNS threat actor who convinces victims to create accounts on fake investment platforms, make deposits to a personal account, and then transfers those deposits to a bank in Russia. This actor uses Facebook ads to lure users into their websites and ultimately enroll in fake investment platforms. The campaign themes often involve spoofing well-known companies like Tesla, Facebook/Meta, and Imperial Oil, among others.



Savvy Seahorse's campaigns are sophisticated. They involve advanced techniques such as incorporating fake ChatGPT and WhatsApp bots that provide automated responses to users, urging them to enter personal information in exchange for alleged high-return investment opportunities. These campaigns are known to target Russian, Polish, Italian, German, Czech, Turkish, French, Spanish, and English speakers, while specifically protecting potential victims in Ukraine and a handful of other countries.

Savvy Seahorse abuses the Domain Name System (DNS) in an obscure way: they leverage DNS canonical name (CNAME) records to create a traffic distribution system (TDS) for sophisticated financial scam campaigns. As a result, Savvy Seahorse can control who has access to content and can dynamically update the IP addresses of malicious campaigns. This technique of using CNAMEs has enabled the threat actor to evade detection by the security industry; to our knowledge, this is the first report to focus on the use of CNAMEs as a TDS engineered for malicious purposes.

In this paper, we introduce the concept of a CNAME TDS and discuss how Savvy Seahorse uses CNAME records to conduct large-scale scam campaigns that have "swum" under the radar of the security industry, until now. The major findings are:

1 https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

- Savvy Seahorse delivers campaigns through Facebook advertisements.
- They have been operating since at least August 2021.
- They use dedicated hosting and change IP addresses regularly.
- Individual campaigns are short-lived (each subdomain is advertised for 5 to 10 days).
- They appear to use a phased deployment system in which the CNAME record for a campaign domain will change based on whether it is currently active or not.
- They utilize wildcard DNS entries, which allows them to create a large number of independent campaigns quickly but can add confusion to passive DNS (pDNS) analysis.
- Personal data of the victim is sent to a secondary HTTP-based TDS server to validate the information and apply geofencing to exclude Ukraine and a handful of other countries.
- The second HTTP-based TDS also tracks user IP and email addresses over time.

A LITTLE LINGO

With hundreds of request for comment (RFC) documents related to DNS, the language can be both confusing and conflicting, especially when combined with how the security industry outside of the networking field uses DNS terminology. Here is the DNS lingo we use in this paper:

- **Domain name** refers to a fully qualified domain name (FQDN) that has assigned DNS records. Both `www[.]infoblox[.]com` and `infoblox[.]com` are domain names. We use FQDN, domain name, and domain interchangeably.
- **Base domain** will be the second-level domain (SLD) associated with a domain name or subdomain; for example, the base domain of `www[.]infoblox[.]com` and `blogs[.]infoblox[.]com` is `infoblox[.]com`. A base domain can be thought of as the registered domain.
- **Subdomain** refers to a domain that is properly within another domain, thus `www[.]infoblox[.]com` and `blogs[.]infoblox[.]com` are subdomains of `infoblox[.]com`. DNS administrators will cringe, but this language is more accessible to threat intelligence readers.
- **Hostname** will refer to the left-most label of a domain, for example: `www`.
- **CNAME domain** is the domain name value in a canonical domain name (CNAME) record.
- **Campaign domain** in this case is one used to lure a victim from a Facebook ad.

CNAME Records in DNS

A CNAME record in DNS provides a mechanism to create an alias to a domain name. These records are used for a wide range of purposes and are intended to make DNS configuration management easier and more robust. They reduce the overall number of DNS records and make it easy to switch IP addresses. The classic use case for CNAME records is to map subdomains used for webpages to the base domain.

For example, most websites use a hostname of `www`. The FQDN `www.infoblox.com` may have a CNAME record with the value `infoblox.com`. In this case, when a client queries for the IP address of `www.infoblox.com`, the IP address for `infoblox.com` will be returned to them. The presence of a CNAME is largely invisible to the user, as a recursive resolver handles the resolutions on their behalf.[2] We say that `www.infoblox.com` is an alias for `infoblox.com`.

2 https://datatracker.ietf.org/doc/html/rfc1034#section-4.3.2

The chain of events to resolution, as Figure 1 illustrates, is roughly:

- The client, a stub resolver, makes a query for `www.infoblox.com` to its recursive resolver.
- The recursive resolver queries the DNS for the IP address (A record) of `www.infoblox.com` and receives a CNAME record in response containing `infoblox.com`.
- The recursive resolver queries the DNS for the IP address of `infoblox.com`.[3]
- The recursive resolver returns the IP address to the client along with the CNAME record.
- Finally, the client service (e.g., the browser) connects to the IP address provided.

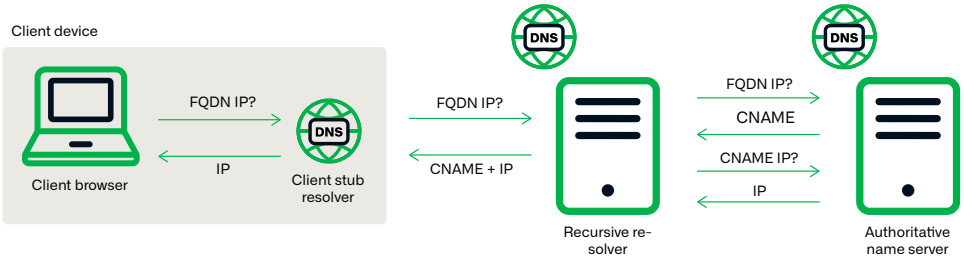


Figure 1: A simplified view of IP address resolution when there is a DNS CNAME record for a fully qualified domain name.

The DNS zone file record in this case might include:

FQDN	Record Type	Value
`www.infoblox.com.`	CNAME	`infoblox.com`
`infoblox.com.`	A	127.0.0.1

The left side of the record is said to be an **alias** for the canonical domain name. So `www.infoblox[.]com` is an alias for `infoblox[.]com`. Queries for the A record of both `www[.]infoblox[.]com` and `infoblox[.]com` would return 127.0.0.1. A canonical domain name, that is, the value of the CNAME record, must be an FQDN.

CNAME Traffic Distribution Systems

While the classic use case for CNAME records is mapping the `www` hostname to the base domain, in practice they are used in many ways. CNAME records are used in many content delivery networks (CDNs). In the example above, we suggested that `www[.]infoblox[.]com` might be an alias for `infoblox[.]com`, but in practice, it is not. Infoblox, like most major companies today, uses a commercial CDN provider. In reality, `www[.]infoblox[.]com` has a CNAME domain within our CDN provider. The primary purpose of a CDN is to provide global users with fast access to website content regardless of where they are located. To achieve this access, CDN providers often use sophisticated hosting environments including caching and proxy appliances; however, those mechanisms are all independent of the DNS configurations.

A **TDS** connects sources of internet traffic to destinations. The term arose from internet marketing where a TDS connects website visitors to advertising. Malicious hackers have capitalized on this technique, taking the concept of a TDS used for legitimate marketing purposes and modifying it for use in cybercrime operations. At Infoblox, we have observed a

3 There is some language that the burden of resolving the CNAME value lies with the stub resolver, but most recursive resolvers will automatically complete the resolution process and return a combined response.

number of techniques used to create TDSs, including systems that are entirely based in DNS and make decisions solely based on the requester's IP address. In our previous publications on VexTrio[4] and Prolific Puma,[5] we described multiple examples of malicious TDSs. VexTrio operates both a DNS TDS and an HTTP-based TDS, while Prolific Puma operates a link-shortening service. Where a legitimate marketing TDS aims to deliver any user to relevant advertising content, a malicious TDS may also incorporate traffic control, restricting certain users from the true content. Some malicious campaigns chain multiple TDSs together.

Savvy Seahorse is the first publicly reported threat actor abusing DNS CNAMEs as part of a malicious TDS. While it requires more sophistication in DNS on the part of the threat actor, it is not uncommon—just unrecognized up to this point in the security literature. We use the term **CNAME TDS** to describe the technique of using DNS CNAME records to create a TDS. At face value, this use of a TDS may be mistaken for a CDN; however, unlike a CDN, a TDS is not designed to provide equal, performant access to all users to the same content.

Using DNS CNAME records to create a TDS for nefarious activities may not be a new concept for threat actors, but it appears to be new to the security industry. Since at least 2021, Savvy Seahorse has relied on this previously unreported technique to build infrastructure and conduct scam campaigns targeting Facebook/Meta users looking to invest. We also track a number of other actors using variations of the CNAME technique.

FROM CNAME TO SeaNAME

Savvy Seahorse co-opts the domain-substitution mechanism of CNAME and creates specific subdomains associated with the primary campaign domain. In particular, all of the malicious campaign domains are aliases for a subdomain of:

`b36cname[.]site`

For example, Savvy Seahorse previously used the domain `mom[.]multi-info[.]site` in a campaign spoofing a Mastercard investment program. This domain had a CNAME record containing the value `prx16[.]b36cname[.]site`. At the same time, the actor used many other subdomains of `multi-info[.]site` in their campaigns. All of these shared the same IP address because Savvy Seahorse uses wildcard DNS configurations. Figure 2 shows this configuration.

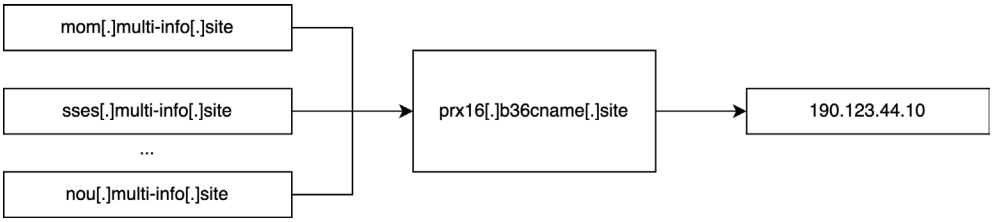


Figure 2: Savvy Seahorse uses many campaign domains simultaneously that are subdomains of the same base domain. These subdomains share a CNAME record and thus an IP address.

Savvy Seahorse uses dedicated IP addresses to host content. The actor regularly rotates these IP addresses and leverages the use of CNAMEs to easily do so, helping them to evade detection and camouflage in the DNS waters.

4 https://blogs.infoblox.com/cyber-threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program

5 https://blogs.infoblox.com/cyber-threat-intelligence/prolific-puma-shadowy-link-shortening-service-enables-cybercrime/

Savvy Seahorse's campaign domains don't share an easily distinguishable pattern and can vary considerably in their hosting infrastructure, which we will examine more in later sections. These variations can make it more difficult for threat researchers to identify the activity as coming from a single DNS threat actor. Ultimately, the only information that enabled us to tie this network together was the use of a common CNAME.

SAVVY SEAHORSE OPERATIONS

Savvy Seahorse has been operating since August 2021, when the `b36cname[.]site` domain was first created. Although participating domains are sometimes flagged by security tools, the greater infrastructure and actor behind them have gone undetected by the security industry. We have observed approximately 4.2k base domains with a CNAME record listing a subdomain of `b36cname[.]site`. To host campaigns, Savvy Seahorse creates several subdomains for each SLD using a domain generation algorithm (DGA), where the hostname is pseudo-random and in most cases, three characters long. We will go into more details of this hostname pattern in the next section.

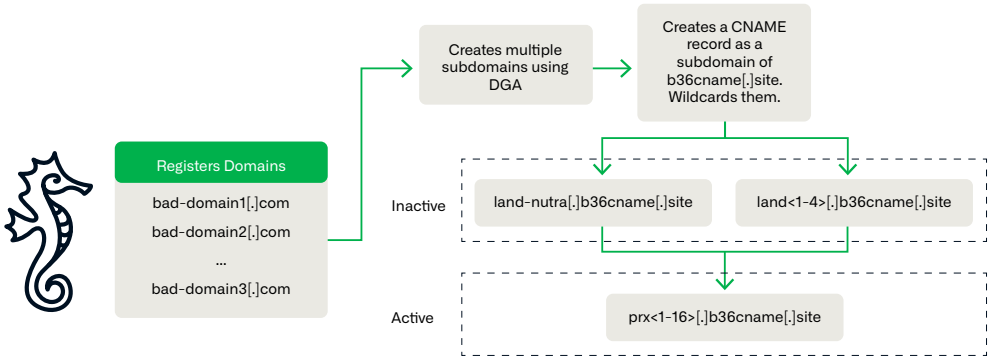


Figure 3: An overview of Savvy Seahorse's operations

SeaNAME Patterns and Wildcarding

Each of the Savvy Seahorse's CNAME records falls under one of the three patterns, as Table 1 shows.

CNAME Patterne	Purpose
`land-nutra[.]b36cname[.]site`	Subdomain used temporarily as CNAME before campaigns become active, for parked domains
`land<1-4>[.]b36cname[.]site`	Subdomains used temporarily as CNAMEs before campaigns became active, possibly for testing purposes
`prx<1-16>[.]b36cname[.]site`	Subdomains used for active campaigns

Table 1: CNAME record patterns and purposes

The following are behaviors we observed on Savvy Seahorse's usage of each type of CNAME:

Domains that had `land-nutra[.]b36cname[.]site` as a CNAME record were parked during that time. When the campaigns became active, the actors changed the CNAME record to `prx<1-16>[.]b36cname[.]site`.

Similarly, domains that at some point had land<1-4>[.]b36cname[.]site as a CNAME record were used for campaigns that were inactive. These domains were also then changed to the prx<1-16>[.]b36cname[.]site record when campaigns were activated.

The land<1-4> CNAMEs may be used for testing some campaigns before they are activated.[6]

Savvy Seahorse has configured wildcard CNAME responses to easily manage their use of DNS. In this case, a query to any subdomain (e.g., wildcard[.]xsdelx[.]top) of the base domain will return a response showing they share the same resource record. In Figure 4, we show the result of performing a dig command to query wildcard[.]xsdelx[.]top of the xsdelx[.]top Savvy Seahorse base domain. The response shows that as a result of the wildcarding, the query returned the CNAME record prx2[.]b36cname[.]site. Wildcarding allows the actor to automatically set the records for any new subdomains they create, which facilitates more efficient management of a large infrastructure.

```
; <<>> DiG 9.10.6 <<>> +trace wildcard.xsdelx.top
;; global options: +cmd
.                       3328    IN      NS      b.root-servers.net.
.                       3328    IN      NS      g.root-servers.net.
.                       3328    IN      NS      d.root-servers.net.
.                       3328    IN      NS      f.root-servers.net.
.                       3328    IN      NS      e.root-servers.net.
.                       3328    IN      NS      i.root-servers.net.
.                       3328    IN      NS      m.root-servers.net.
.                       3328    IN      NS      a.root-servers.net.
.                       3328    IN      NS      h.root-servers.net.
.                       3328    IN      NS      c.root-servers.net.
.                       3328    IN      NS      j.root-servers.net.
.                       3328    IN      NS      k.root-servers.net.
.                       3328    IN      NS      l.root-servers.net.
.                       3328    IN      RRSIG   NS 8 0 518400 20240124220000 20240111210000 30903 . KAZZGJQ19L65se3m2Evl4S/ucf
SV7rPzcTEXZvIiTa96qIyXNdw5+L5R Ece44fVVTc7Kpr2UK844Zb9qnGcjiB22XHqWoeYjyRZgQ2kuEHkVVTC+ jLNeRqQQ84cleKWPebpiSo73paJE3iLqpug8fR
9DUzbW4+XmNFW11Nak ahTafUnmBDbe7fJ/AkI9lH2PdqSTrB882vGZI/UYfBWG38E5msl TS/aa NAL2yIsGYCuargdZDGkp9yOa6q2khrjBBNUeqhlrOQU63yh+qF
rzJ851 O7iyiQmXwl2j22vEzncv23ue16CgHIUu2yaJLGmxI5m9N2lBHAPvgzlC zpdGZg==
;; Received 717 bytes from 127.0.0.2#53(127.0.0.2) in 57 ms

top.                    172800  IN      NS      a.zdnscloud.com.
top.                    172800  IN      NS      b.zdnscloud.com.
top.                    172800  IN      NS      c.zdnscloud.com.
top.                    172800  IN      NS      d.zdnscloud.com.
top.                    172800  IN      NS      f.zdnscloud.com.
top.                    172800  IN      NS      g.zdnscloud.com.
top.                    172800  IN      NS      i.zdnscloud.com.
top.                    172800  IN      NS      j.zdnscloud.com.
top.                    86400   IN      DS      56384 8 2 BA378C5913404EC654DF544F519B0FB287E140D64DAC5D59E3499623 93C17945
top.                    86400   IN      RRSIG   DS 8 1 86400 20240124220000 20240111210000 30903 . z+m6M/ORJDt+eyaQ/jjqUr9G5b+
fosBjAsw5MKrYyGbIjNaYQoBDBtvi bZsVI7YD3vAlRf7HfleOavQJ0nC57B3dsED4jKJ32ulMsHNxJ/+7Nbf/ XZMc20086b6FQC/LxUxYFFw4+fTrfJX1ydp4Ze2
gJi2amF3hWEQJO6aW bP+NiAiT4UTW74AMZH31BLhtYDHkVKzHjXGSGcgBn9Zp4mesaf/fjxQK o3QCgmD8Kb7sqmULt4RMirZUxEYrbHC/LO+GsPb9aAcKA5qC2/8
/if3s j/q4wh5NlD5Asdai2cGhd2oYlJMGBmLVBgEWMIAONBiPSWTR2JimteSe 42BWyQ==
;; Received 676 bytes from 2001:500:2d::d#53(d.root-servers.net) in 24 ms

xsdelx.top.             3600    IN      NS      ns1.dns.com.
xsdelx.top.             3600    IN      NS      ns2.dns.com.
nmb1kc8kpr7nahib8f3qbcm0q3q4s6l1.top. 3600 IN NSEC3 1 0 0 - NMB1KT4CELS35EVJ7GVFSKCJB2HGKQGA  NS
nmb1kc8kpr7nahib8f3qbcm0q3q4s6l1.top. 3600 IN RRSIG NSEC3 8 2 3600 20240119124502 20240105021522 9610 top. b8QG+wOZ+V9gRsl8/ty
UoISU9cTbU3Ha6mh7O/SyeInAtGX9KG2Kl+nU g3RoIofAm6A2GoQmOiQ5hzLPWYPjelSjLXE1PJBUAIYknGxToHz55RE8 JRLb/e4FqZphjgB6EicSKazMW1HA2co
v49hq/lWLzTtg/LduzXQmOAWZ 9SE=
;; Received 331 bytes from 2401:8d00:2::1#53(j.zdnscloud.com) in 166 ms

wildcard.xsdelx.top.    600     IN      CNAME   prx2.b36cname.site.
xsdelx.top.             86400   IN      NS      ns1.dns.com.
xsdelx.top.             86400   IN      NS      ns2.dns.com.
;; Received 130 bytes from 183.253.57.193#53(ns2.dns.com) in 256 ms
```

Figure 4: Wildcard response behavior to a random subdomain of an existent Savvy Seahorse base domain. The servers responded to the subdomain showing it has a CNAME record value of prx2[.]b36cname[.]site*, the actor's CNAME domain.*

Domains

Threat actors often use DGAs as tools to generate large numbers of pseudo-random domain names that they can use to operate campaigns and conduct other malicious activities. Domains used in these DGAs often follow similar visible patterns that dedicated algorithms can easily detect and thereby facilitate correlation to a threat actor. While Savvy Seahorse appears to use DGAs to create many of their SLDs and subdomains, these DGAs don't appear to follow one distinct pattern. Rather, we have observed the actor using several DGA patterns for SLDs, as Table 2 indicates.

6 https://urlscan.io/result/f6521352-dc51-4352-9d5f-691268e17c8c/

Pattern Description	Variations on the same full keyword	Full keyword appended with random characters of the same length	Spelling variations on the second half of a keyword	Variations of a keyword across the domain
Sample Domains	program-delo[.]site program-lid[.]site program-lids[.]site program-life[.]xyz program-plus[.]site program-plus[.]xyz program-pro2[.]xyz program-world[.]site programbndr[.]site programerstr[.]xyz programfuture[.]site programinject07[.]site programir[.]xyz programm-one[.]site programs-pl[.]site	formaa[.]top formew[.]top formhh[.]top formpr[.]top	anticriss-es[.]xyz anticrisses[.]xyz anticriz[.]site anticrsss-ep[.]xyz anticrsss1-ep[.]xyz anticrys[.]xyz anticrysz[.]site antikrys[.]xyz	zol0to-rus[.]xyz zolotoru[.]site xoloto-ru[.]xyz zolotoros[.]site

Table 2: Savvy Seahorse SLD patterns and example domains

A common technique for identifying these types of DGAs is to use machine learning algorithms. One could use N-grams[7] to successfully detect some of the clusters in each column in Table 2, but that method would fail to detect that all these clusters belong to a single DNS threat actor if simply looking at domain label features. All four clusters above have very distinct patterns—as do other domain clusters that Savvy Seahorse creates—that an N-gram-based model wouldn't be able to detect as belonging to the same group.

The examples above also show the actors don't stick to just one top-level domain (TLD), even within distinct DGA naming patterns. Savvy Seahorse uses several TLDs, often ones that are known to be highly abused. The top five by domain count are site, `xyz`, `com`, `top`, and `life`.

7 https://en.wikipedia.org/wiki/N-gram

TLD	site	xyz	com	top	life
Domains	imsol[.]site lareg[.]site mstpr[.]site tayki[.]site teraw[.]site	newtrds[.]xyz newtrdin[.]xyz newstrdinfo[.]xyz newstrdinfos[.]xyz	gelopro[.]com welerpro[.]com glowtrad[.]com strprogram[.]com	newlvlpro[.]top newplatf[.]top newplattf[.]top newplf[.]top newprogf[.]top gelopro[.]com welerpro[.]com glowtrad[.]com strprogram[.]com	maxhongtrade[.]life firehongtrade[.]life librahongtrade[.]life

Table 3: Sample domains for the most commonly used TLDs in Savvy Seahorse's malicious campaigns

Previously, we mentioned that the hostnames appear to be pseudo-random and three characters long in most cases, but we have seen some examples with longer labels (see Table 4).

byseniscon[.]top	worldtrades[.]top	tesxprofit[.]top
per[.]byseniscon[.]top	bln[.]worldtrades[.]top	bkz[.]tesxprofit[.]top
bzmm[.]byseniscon[.]top	bts[.]worldtrades[.]top	gfk[.]tesxprofit[.]top
i9us[.]byseniscon[.]top	cai[.]worldtrades[.]top	krx[.]tesxprofit[.]top
ijks[.]byseniscon[.]top	cpq[.]worldtrades[.]top	kvn[.]tesxprofit[.]top
ji8s[.]byseniscon[.]top	da2[.]worldtrades[.]top	mcr[.]tesxprofit[.]top
q89k[.]byseniscon[.]top	dab[.]worldtrades[.]top	mld[.]tesxprofit[.]top
u76a[.]byseniscon[.]top	dha[.]worldtrades[.]top	ndx[.]tesxprofit[.]top
jskks[.]byseniscon[.]top	dl5[.]worldtrades[.]top	nfk[.]tesxprofit[.]top
nbxnz[.]byseniscon[.]top	ewt[.]worldtrades[.]top	nqs[.]tesxprofit[.]top
nuuvi[.]byseniscon[.]top	fe0[.]worldtrades[.]top	nzb[.]tesxprofit[.]top

Table 4: Subdomain pattern examples

Registration Information

Savvy Seahorse does not follow a conventional approach in the way they handle registrations, which helps them evade detection. A common technique that DNS threat actors use is to register domains in bulk through the same registrar, as well as use the same internet service provider (ISP) to host them for easier and faster management of their infrastructure. Many registrars offer APIs to facilitate bulk registration of domains. While most registrars intend for the APIs to be used for legitimate purposes, cybercriminals have been known to abuse this feature to more easily create thousands of domains to use for their campaigns. Our October 2023 blog on RDGAs describes the process in more detail.[8]

When actors leverage the same registrar and infrastructure to create and host their domains, it can often be straightforward to find domains belonging to the same actor through common registration metadata. Savvy Seahorse appears to be more of a patient creature with infrastructure spread across a number of different registrars and hosting providers. We observed 30 unique registrant organizations and 21 ISPs for all domains with a subdomain of `b36cname[.]site` as a CNAME record. This technique makes it more difficult for security researchers to correlate domains and distinguish an actor's infrastructure.

The variations in registration metadata for domains with a `b36cname` record originally caused us to suspect that this actor may be a service provider for other cybercriminals running scam campaigns. However, our analysis showed that the financial scam campaigns run via their network all share the same elements and overall behavior, leading us to conclude that the campaigns are most likely controlled by a single actor: Savvy Seahorse. We discuss these campaigns and their content in more detail in the Campaign Analysis section.

IP Addresses

Savvy Seahorse appears to use approximately 50 dedicated IP addresses, and regularly changes them, as Figure 5 illustrates. The small gaps in each timeline bar represent when Savvy Seahorse changed the IP associated with a CNAME record.

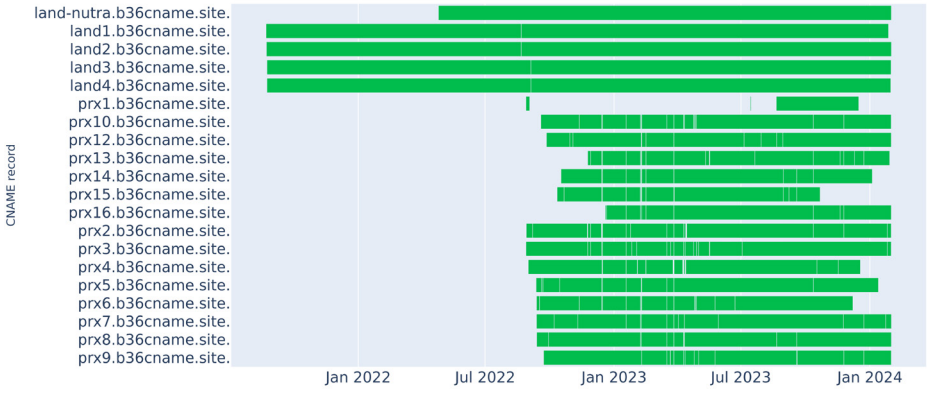


Figure 5: Timeline of IP address changes by CNAME. Each bar shows the time that each CNAME record spends on a specific IP address, and narrow gaps indicate when these values changed. Actors often rotate IP addresses to evade detection.

Based on analysis of the changes in IPs, we've observed the following:

- `land-nutra[.]b36cname[.]site` is the only CNAME with a single IP address, which aligns with the behavior we've seen indicating domains associated with this CNAME are parked. This IP address has a significantly large overall number of domains associated with it, a characteristic that aligns with IP addresses used for parking.

8 https://blogs.infoblox.com/cyber-threat-intelligence/rdgas-the-new-face-of-dgas/

- All four of the CNAMEs using the land<1-4>[.]b36cname[.]site pattern have changed IP addresses only once.
- prx<1-16>[.]b36cname[.]site CNAMEs frequently change IP addresses. This pattern indicates these IPs are most likely used exclusively for active scam campaigns because periodic changes to the IPs are a tactic threat actors employ to evade detection and blocking by security vendors.
- There are some occurrences of the threat actor changing the IPs for multiple CNAMEs at the same time for the same value.
- A few CNAMEs, including prx6[.]b36cname[.]site and prx15[.]b36cname[.]site, don't seem to currently be in use by the threat actor.

CAMPAIGN ANALYSIS

Savvy Seahorse uses a unique infrastructure to conduct a number of different scam campaigns that follow financial and investment themes. The campaigns feature a variety of advanced lure techniques, but they all follow a similar pattern with the end goal of stealing the victim's personal and financial information for monetary gain. The languages used for these campaigns include English, Russian, Polish, Italian, German, French, Spanish, Czech, and Turkish.

- Active campaigns operate at the subdomain level, where each subdomain has a prx<1-16>[.]b36cname[.]site CNAME record.

Campaign Details

Savvy Seahorse uses registration forms embedded in each web page to gather the victim's first and last name, email address, and phone number. Two examples of this registration form, one in Polish and the other in English, appear in Figure 6.

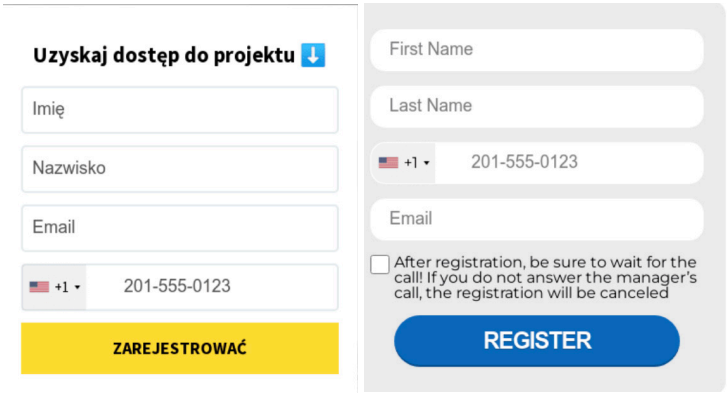


Figure 6: Registration forms used in Savvy Seahorse's campaigns

Validation and Redirection

After the user enters their information in these forms, the domain will reach out to the secondary TDS domain that Savvy Seahorse uses in their campaigns, getyourapi[.]site, to perform validation checks on the information, including the user's IP address, geolocation, and the validity of the phone number and email provided. Depending on which checks pass, we have observed three different scenarios:

1. If the form data is valid but the user has previously registered using the same email/phone number, the web page states the user has already registered.
2. If the form data is valid but the user has previously visited this domain via the same IP address, the page displays a message confirming registration and states a representative will call them for additional information. No redirection occurs.
3. If the form data is valid and the user visits the domain with an unfamiliar IP address, they are redirected to a fake trading web page similar to the one in Figure 7.

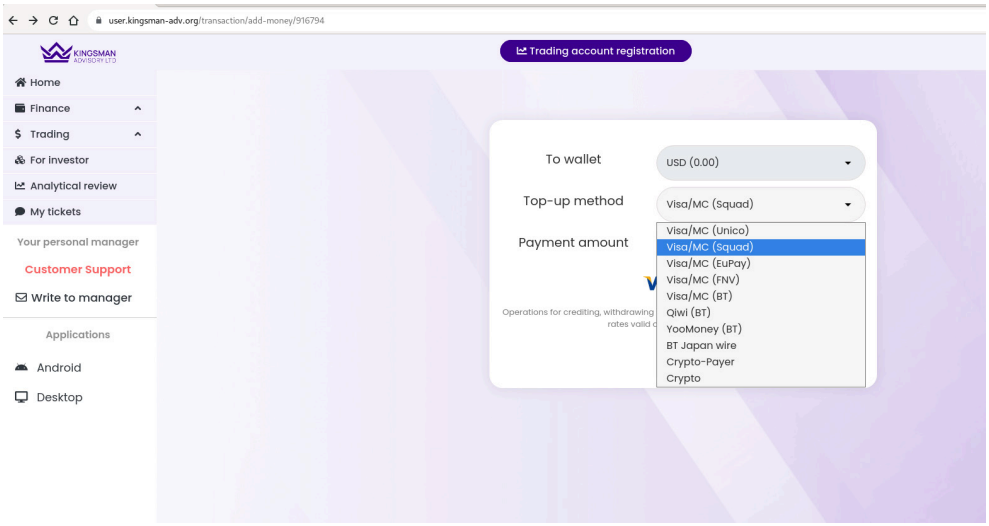


Figure 7: A Savvy Seahorse fake trading platform

An important detail to note is the actor validates the user's information to exclude traffic from a predefined list of countries, including Ukraine, India, Fiji, Tonga, Zambia, Afghanistan, and Moldova, although their reasoning for choosing these specific countries is unclear. The first validation check is on the phone number entered into the registration form; if it originates from one of the block-listed countries, the web page will display a message stating, "**The program is not support [sic] in your region.**" If the user enters an acceptable phone number along with all other valid information as mentioned above, the actor will send the information to its secondary TDS domain to validate the geolocation of the user's IP address against the excluded countries to decide whether or not redirection will occur.

Trading Platform

Once the user is redirected, the fake trading platform will automatically have an account set up for them with the details from the registration form. This platform appears to be highly sophisticated and offers the option to download a desktop application, as well as links to an Android app in the Google Play Store called App4World.

The user is then encouraged to add money to their "wallet" from a number of different sources including Visa/Mastercard, a crypto wallet, or Russian payment providers such as Qiwi and YooMoney. A minimum "top-up" amount of $50 USD is required to add money to a wallet. Final redirection to one of eight possible payment processing domains (see Table 5) occurs once the user specifies a payment source and deposit amount. Which domain the campaign uses to collect financial information from the victim depends on which source they choose to transfer money from.

Payment Source	Payment Domain	Payment Domain Description
Visa/MC (Unico)	makeyourpay[.]com	Newly registered domain hosting payment processing web page; Russian-language subdomains
Visa/MC (Squad)	checkout[.]flutterwave[.]com	Hosts a legitimate financial infrastructure company based in Nigeria
Visa/MC (EuPay)	ap-gateway[.]mastercard[.]com	Legitimate payment gateway for Mastercard
Visa/MC (BT)	sci[.]pointpayment[.]net	Hosted on same dedicated IP as a number of other suspicious payment domains
Qiwi (BT)	qiwi[.]bppsa[.]com	Base domain hosts a Russian-language payment processing web page
YooMoney (BT)	ymoney[.]bppsa[.]com	Base domain hosts a Russian-language payment processing web page
BT Japan (wire)	processing[.]betatransfer[.]io	API for Betatransfer Kassa, a high-risk payment processing service (primarily used for online gambling)
Crypto-Payer Crypto	crypto-payer[.]co	Registered December 2023

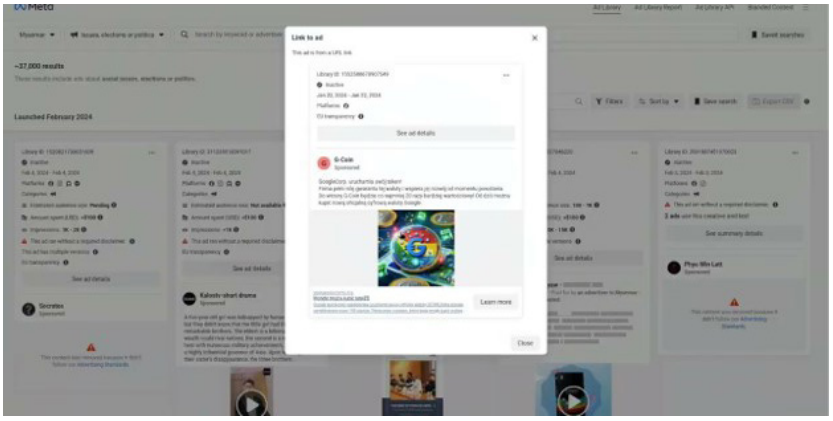
Table 5: Payment processing domains to collect victim's financial information

Upon investigation, the actor appears to be routing money to SberBank, a majority Russian-state-owned bank, for at least one of the payment processing domains (`sci[.]pointpayment[.]net`) as Figure 8 shows.

URL: https://sci.pointpayment.net/
BIN of the acquiring bank: 546901
NAME of the acquiring bank: SBERBANK of Russia Merchant
ID in the bank: 000000010006546
Merchant name: MYTIPS_CARD2CARD
Merchant URL: http://www.sberbank.ru

Figure 8: Financial details for `sci[.]pointpayment[.]net`

The video below provides a walkthrough of the fake trading platform.



View the video, Savvy Seahorse Campaign Walkthrough.

Meta Pixel

Because Savvy Seahorse markets and distributes these campaigns via Facebook/Meta ads (see Figure 9), all domains used in active campaigns make multiple connections to `connect[.]facebook[.]net` and `www[.]facebook[.]com`. The actor also uses Meta Pixel, a legitimate tool, to track and optimize the performance of the ads.[9]

A Meta Pixel is a piece of JavaScript code consisting of two parts:

- A "script" that is executed when the page is loaded, initializes the Facebook pixel, and tracks a "PageView" event.
- A "noscript" that is executed when the user has JavaScript disabled in their browser. This section will display a 1x1 pixel image to track the event.

Each Meta Pixel features a unique ID number that we can see in the HTTP connections to Facebook. We have observed some campaigns that are hosted on the same SLD with different subdomains sharing the same ID, but others appear to be randomized.

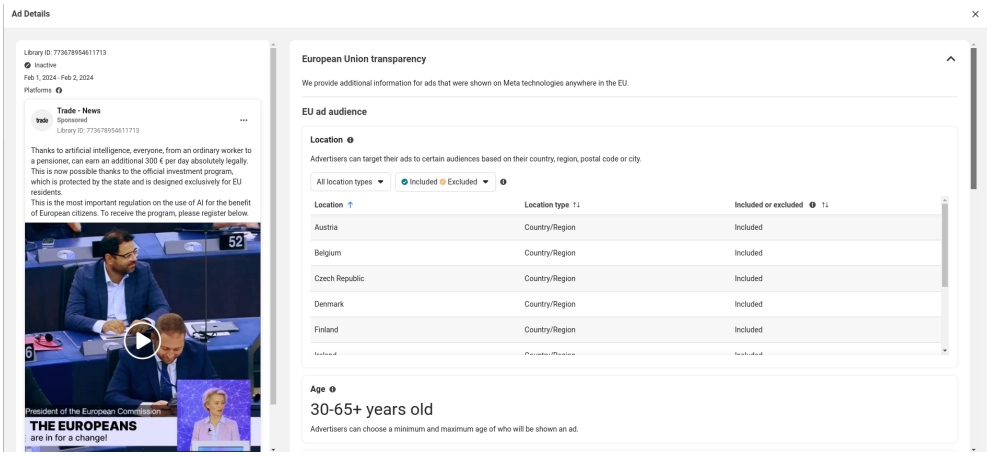


Figure 9: Facebook ad details for Savvy Seahorse's campaign showing targeted countries and age demographic

9 https://www.facebook.com/business/tools/meta-pixel

Themes

Specific themes for Savvy Seahorse's campaigns can vary widely, including lures spoofing legitimate companies such as Apple for investment opportunities and incorporating bots that impersonate WhatsApp, ChatGPT, and Tesla.

Earning Projects Impersonating Companies

One of the most common themes Savvy Seahorse has used throughout its time of operations involves "earning projects" or investment programs that claim the user has an opportunity to earn a specific amount of money if they register with their personal information. Threat actors often employ a popular phishing campaign technique where they attempt to impersonate easily recognizable brands and companies to build trust with the user. Table 6 gives a few examples we have seen.

Campaign Subdomain	Associated CNAME	Campaign Description
new[.]xsdelx[.]top	prx2[.]b36cname[.]site	Russian-language campaign spoofing Tesla and X, encouraging users to "join Elon Musk's project" to receive 12,000 euros per month
bwn[.]objectop[.]xyz	prx7[.]b36cname[.]site	English-language campaign spoofing Imperial Oil, a legitimate Canadian petroleum company. Landing page features an interactive "survey" and encourages users to invest $250 to $1,000 USD
sej[.]progmedisd[.]site	prx9[.]b36cname[.]site	Polish-language campaign from February 2023 for the "Libra automatic earning project," which claims to have been created by Mark Zuckerberg and promises users earnings of up to 300,000 Polish złoty (PLN)

Table 6: Examples of Savvy Seahorse financial campaigns

Figures 10 and 11 show screenshots from some of the campaigns in Table 6. Other examples of companies Savvy Seahorse has spoofed include, but are not limited to, Apple, Meta, Mastercard, Visa, and Google.

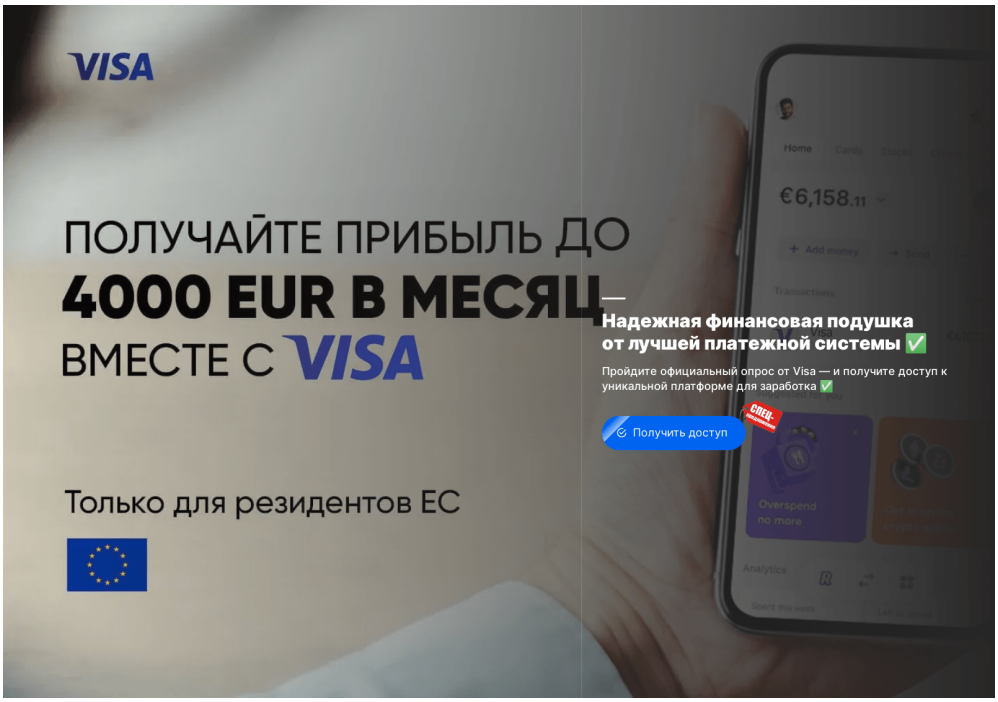


Figure 10: Landing page for `visa[.]lukzev[.]xyz`*, a Russian-language campaign spoofing Visa*

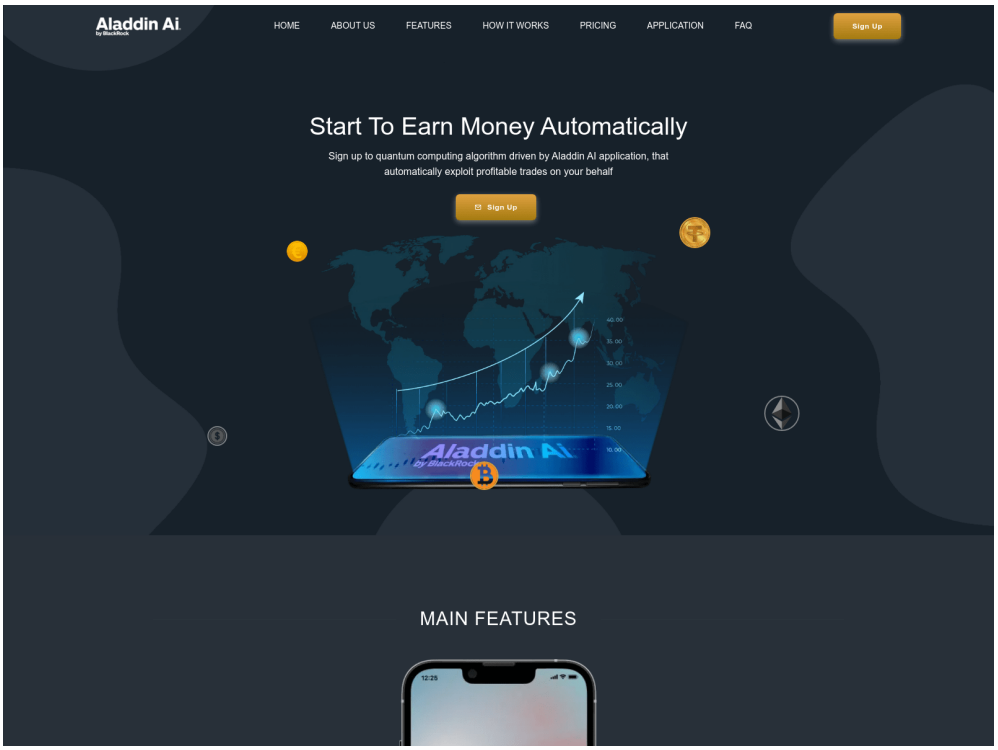


Figure 11: Landing page for `adin[.]czproftes[.]xyz` *impersonating BlackRock's portfolio management platform*

Fake Bots

We have seen a few campaigns featuring advanced lure techniques with chatbots impersonating ChatGPT, WhatsApp, and Tesla, among others. Recently, scams with these types of bots have become a common trend among threat actors looking to gain the trust of users to steal their personal information.[10] The screenshot in Figure 12 shows our interactions with one of these chatbots from a campaign spoofing Tesla.

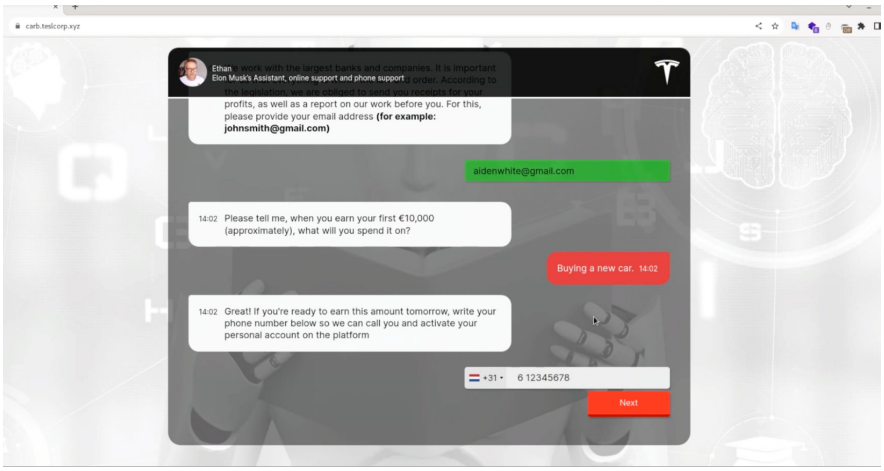


Figure 12: Fake Tesla-themed bot used in Savvy Seahorse campaign

The bots will ask the user questions about their interest in potential opportunities for earning and investing but ultimately follow the same pattern as other campaigns—prompting the user to register with their personal information before redirecting them to the fake trading platform.

CONCLUSION

At Infoblox, we remain focused on finding new ways that threat actors are abusing DNS to conceal their criminal operations. Savvy Seahorse's technique of using DNS CNAMEs as a TDS to manage their malicious operations demonstrates how DNS is the most effective way of tracking and disrupting the activities of cybercriminals. Our analysis into CNAME patterns was ultimately what enabled us to discover this actor and the unique tactics, techniques, and procedures (TTPs) it employs to operate its large network of scam campaigns.

10 https://www.security.org/digital-security/guide-to-chatbot-scams/

INDICATORS OF ACTIVITY

Below is a sample of indicators used in Savvy Seahorse's campaigns. A more comprehensive list of indicators appears in our GitHub repository here.

Indicator	Type of Indicator
getyourapi[.]site	Savvy Seahorse secondary TDS domain
land-nutra[.]b36cname[.]site	Subdomain used as CNAME record for parked domains
land<1-4>[.]b36cname[.]site	Subdomains used as CNAME records for inactive campaigns
prx<1-16>[.]b36cname[.]site	Subdomains used as CNAME records for active campaigns
new[.]xsdelx[.]top bwn[.]objectop[.]xyz sej[.]progmedisd[.]site adin[.]czproftes[.]xyz visa[.]lukzev[.]xyz sun[.]autotrdes[.]top hmz[.]coivalop[.]xyz news[.]beneffit[.]top goiin[.]baltez-offic[.]xyz	Subdomains for active Savvy Seahorse campaigns
ultra-vest[.]one kingsman-adv[.]org abyss-world-asset[.]net	Fake trading websites the user is redirected to in some campaigns
sci[.]pointpayment[.]net makeyourpay[.]com qiwi[.]bppsa[.]com ymoney[.]bppsa[.]com processing[.]betatransfer[.]io crypto-payer[.]co	Payment processing domains to collect victim's financial information

Indicator	Type of Indicator
ap-gateway[.]mastercard[.]com	Legitimate domain for Mastercard used collect victim's financial information
checkout[.]flutterwave[.]com	Legitimate domain for Flutterwave, a Nigerian payment service used to collect victim's financial information
auproject[.]xyz badanie-pl[.]site blog-vcnews[.]site capital-inwest[.]site dasms[.]xyz duums[.]xyz esbopehan[.]xyz	Savvy Seahorse base domains

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: 20240216v1