infoblox

Threat Intel

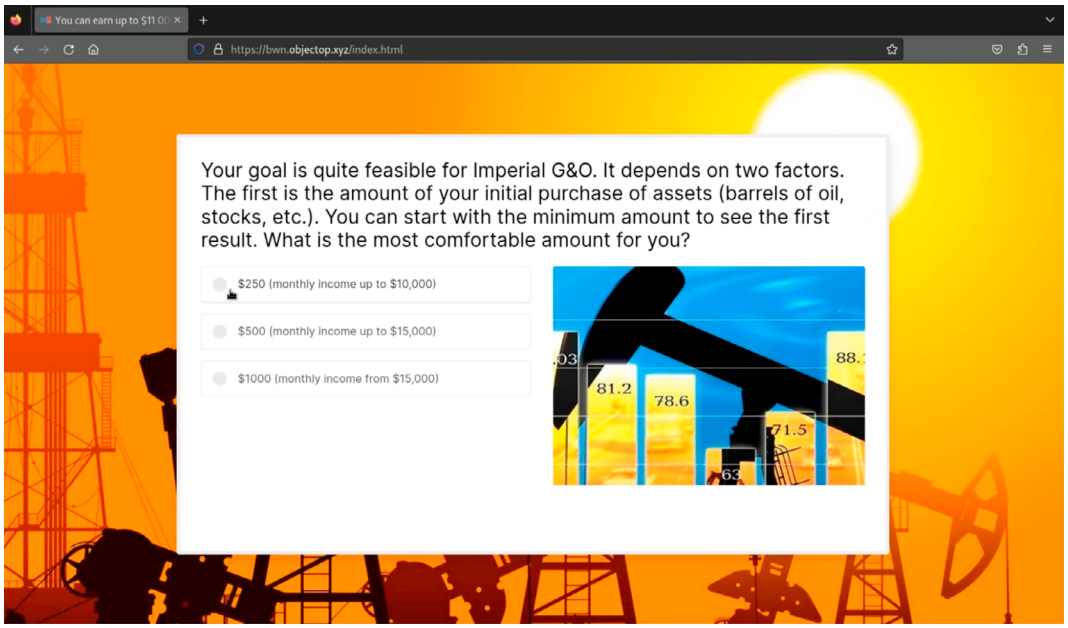
VORSICHT VOR SEICHTEN GEWÄSSERN: SAVVY SEAHORSE LOCKT OPFER ÜBER FACEBOOK-WERBUNG AUF GEFÄLSCHTE ANLAGEPLATTFORMEN

Autoren:
Stelios Chatzistogias
Laura da Rocha
Darby Wise

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

DNS-Bedrohungsakteure überraschen uns immer wieder. Jeden Tag erfahren wir von kreativen neuen Kampagnen, die sie sich ausgedacht haben, um ihre Opfer auszubeuten. Anlagebetrug ist eine davon. Die US-amerikanische Federal Trade Commission berichtete, dass im Jahr 2023 in den USA durch Anlagebetrug mehr Geld verloren ging als durch jede andere Art von Betrug. Insgesamt wurden den Opfern über 4,6 Milliarden US-Dollar gestohlen.[1] Savvy Seahorse ist ein DNS-Bedrohungsakteur, der Opfer dazu bringt, Konten auf gefälschten Anlageplattformen zu eröffnen und Einzahlungen auf ein persönliches Konto vorzunehmen. Diese Einzahlungen werden dann an eine Bank in Russland überwiesen. Dieser Akteur nutzt Facebook-Werbung, um Benutzer auf seine Websites zu locken und sie letztlich dazu zu bewegen, sich bei gefälschten Anlageplattformen anzumelden. Zu den Kampagnenthemen gehört oft, dass sich der Akteur als ein bekanntes Unternehmen wie Tesla, Facebook/Meta und Imperial Oil ausgibt, um nur einige zu nennen.



Die Kampagnen von Savvy Seahorse sind ausgefeilt. Sie bringen ausgeklügelte Techniken zum Einsatz, beispielsweise die Einbindung gefälschter ChatGPT- und WhatsApp-Bots, die den Benutzern automatisierte Antworten liefern und sie dazu drängen, persönliche Daten einzugeben, um im Gegenzug angebliche Anlagemöglichkeiten mit hoher Rendite zu erhalten. Es ist bekannt, dass diese Kampagnen auf Russisch, Polnisch, Italienisch, Deutsch, Tschechisch, Türkisch, Französisch, Spanisch und Englisch sprechende Menschen abzielen, wobei potenzielle Opfer in der Ukraine und einer Handvoll anderer Länder besonders geschützt werden.

Savvy Seahorse missbraucht das Domain Name System (DNS) auf obskure Weise: Der Akteur nutzt kanonische DNS-Namenseinträge (CNAME-Einträge), um ein Traffic Distribution System (TDS) für ausgeklügelte Finanzbetrugskampagnen zu erstellen. Dadurch kann Savvy Seahorse kontrollieren, wer Zugriff auf Inhalte hat, und die IP-Adressen bösartiger Kampagnen dynamisch aktualisieren. Diese Technik der Verwendung von CNAMEs hat es dem Bedrohungsakteur ermöglicht, sich der Entdeckung durch die Sicherheitsbranche zu entziehen. Unseres Wissens nach ist dies der erste Bericht, der sich auf die Verwendung von CNAMEs als TDS für böswillige Zwecke konzentriert.

In diesem Dokument stellen wir das Konzept eines CNAME-TDS vor und erläutern, wie Savvy Seahorse CNAME-Einträge verwendet, um großangelegte Betrugskampagnen durchzuführen, die bislang unter dem Radar der Sicherheitsbranche „geschwommen“ sind. Die wichtigsten Ergebnisse sind:

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

- Savvy Seahorse stellt seine Kampagnen über Facebook-Werbung bereit.
- Diese laufen seit mindestens August 2021.
- Der Akteur nutzt dediziertes Hosting und wechselt regelmäßig die IP-Adressen.
- Einzelne Kampagnen sind kurzlebig (jede Subdomain wird 5 bis 10 Tage lang beworben).
- Der Akteur scheint ein stufenweises Bereitstellungssystem zu nutzen, bei dem sich der CNAME-Eintrag für eine Kampagnendomain abhängig davon ändert, ob sie derzeit aktiv ist oder nicht.
- Er nutzt Wildcard-DNS-Einträge, mit denen er schnell eine große Anzahl unabhängiger Kampagnen erstellen kann, die aber bei passiver DNS-Analyse (pDNS) für Verwirrung sorgen können.
- Persönliche Daten des Opfers werden an einen sekundären HTTP-basierten TDS-Server gesendet, um die Informationen zu validieren und Geofencing anzuwenden, um die Ukraine und eine Handvoll anderer Länder auszuschließen.
- Das zweite HTTP-basierte TDS verfolgt auch die IP- und E-Mail-Adressen der Benutzer im Laufe der Zeit.

EIN BISSCHEN JARGON

Bei Hunderten von Request-for-Comment-Dokumenten (RFC) mit Bezug zu DNS kann der sprachliche Aspekt sowohl verwirrend als auch widersprüchlich sein, insbesondere, wenn man bedenkt, wie die Sicherheitsbranche außerhalb des Netzwerkbereichs DNS-Terminologie verwendet. Deshalb folgt hier die DNS-Terminologie, die wir in diesem Dokument verwenden:

- **Domainname** bezieht sich auf einen vollqualifizierten Domainnamen (FQDN), dem DNS-Einträge zugewiesen sind. Sowohl `www[.]infoblox[.]com` als auch `infoblox[.]com` sind Domainnnamen. Wir verwenden FQDN, Domainname und Domain synonym.
- Die **Basisdomain** ist die Second-Level-Domain (SLD), die einem Domainnamen oder einer Subdomain zugewiesen ist; zum Beispiel ist die Basisdomain von `www[.]infoblox[.]com` und `blogs[.]infoblox[.]com` die Domain `infoblox[.]com`. Eine Basisdomain kann als die registrierte Domain betrachtet werden.
- Der Begriff **Subdomain** bezieht sich auf eine Domain, die sich eigentlich innerhalb einer anderen Domain befindet. Daher sind `www[.]infoblox[.]com` und `blogs[.]infoblox[.]com` Subdomains von `infoblox[.]com`. DNS-Administratoren werden jetzt das Gesicht verziehen, aber diese Ausdrucksweise ist für Leser aus dem Threat-Intelligence-Bereich verständlicher.
- **Hostname** bezieht sich auf das Label ganz links einer Domain, beispielsweise `www`.
- Die **CNAME-Domain** ist der Wert des Domainnamens in einem kanonischen Domainnamen-Eintrag (CNAME-Eintrag).
- Die **Kampagnen-Domain** ist in diesem Fall eine Domain, die verwendet wird, um ein Opfer über eine Facebook-Anzeige anzulocken.

CNAME-Einträge im DNS

Ein CNAME-Eintrag im DNS bietet einen Mechanismus zum Erstellen eines Alias für einen Domainnamen. Diese Einträge werden für eine Vielzahl von Zwecken verwendet und sollen die DNS-Konfigurationsverwaltung einfacher und robuster machen. Sie reduzieren die Gesamtzahl der DNS-Einträge und erleichtern den Wechsel der IP-Adresse. Der klassische Anwendungsfall für CNAME-Einträge besteht darin, für Webseiten verwendete Subdomains der Basisdomain zuzuordnen.

Die meisten Websites verwenden zum Beispiel den Hostnamen `www`. Der FQDN `www.infoblox.com` könnte einen CNAME-Eintrag mit dem Wert `infoblox.com` haben. Wenn in diesem Fall ein Client die IP-Adresse von `www.infoblox.com` abfragt, wird ihm die IP-Adresse von `infoblox.com` ausgegeben. Das Vorhandensein eines CNAME ist für den Benutzer weitgehend unsichtbar, da ein rekursiver Resolver die Auflösungen in seinem Namen vornimmt.[2] Wir sagen, dass `www.infoblox.com` ein Alias für `infoblox.com` ist.

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

Die grobe Kette der Ereignisse bis zur Auflösung ist, wie Abbildung 1 zeigt, folgendermaßen:

- Der Client, ein Stub-Resolver, sendet eine Abfrage für `www.infoblox.com` an seinen rekursiven Resolver.
- Der rekursive Resolver fragt beim DNS die IP-Adresse (A-Eintrag) von `www.infoblox.com` ab und erhält als Antwort einen CNAME-Eintrag, der `infoblox.com` enthält.
- Der rekursive Resolver fragt beim DNS die IP-Adresse von `infoblox.com` ab.[3]
- Der rekursive Resolver gibt die IP-Adresse zusammen mit dem CNAME-Eintrag an den Client aus.
- Schließlich verbindet sich der Client-Dienst (z. B. der Browser) mit der angegebenen IP-Adresse.

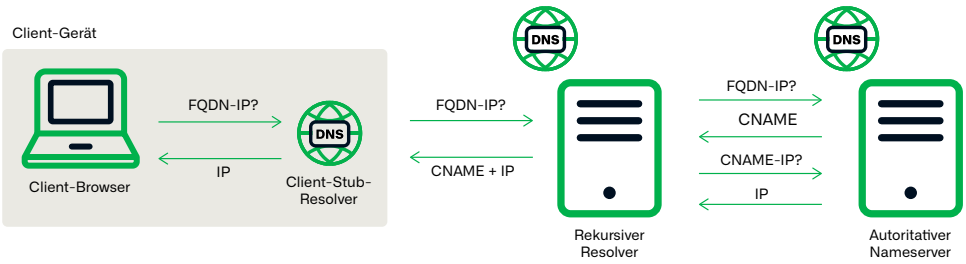


Abbildung 1: Eine vereinfachte Ansicht der IP-Adressauflösung, wenn es einen DNS-CNAME-Eintrag für einen vollqualifizierten Domainnamen gibt.

Der DNS-Zonendateieintrag könnte in diesem Fall Folgendes enthalten:

FQDN	Eintragstyp	Wert
`www.infoblox.com.`	CNAME	`infoblox.com`
`infoblox.com.`	A	127.0.0.1

Der linke Teil des Eintrags wird als **Alias** für den kanonischen Domainnamen bezeichnet, also gilt: `www.infoblox[.]com` ist ein Alias für `infoblox[.]com`. Für Abfragen für den A-Eintrag von sowohl `www[.]infoblox[.]com` als auch `infoblox[.]com` würde 127.0.0.1 ausgegeben. Ein kanonischer Domainname, also der Wert des CNAME-Eintrags, muss ein FQDN sein.

CNAME Traffic Distribution Systems

Der klassische Anwendungsfall für CNAME-Einträge ist die Zuordnung des `www`-Hostnamens zur Basisdomain, aber in der Praxis werden sie auf verschiedenste Arten verwendet. CNAME-Einträge werden in vielen Content Delivery Networks (CDNs) genutzt. Im obigen Beispiel haben wir angedeutet, dass `www[.]infoblox[.]com` ein Alias für `infoblox[.]com` sein könnte, aber in der Praxis ist das nicht der Fall. Infoblox nutzt, wie die meisten großen Unternehmen heutzutage, einen kommerziellen CDN-Anbieter. In Wirklichkeit hat `www[.]infoblox[.]com` eine CNAME-Domain bei unserem CDN-Anbieter. Der Hauptzweck eines CDN besteht darin, Nutzern auf der ganzen Welt einen schnellen Zugriff auf Website-Inhalte zu ermöglichen, unabhängig davon, wo sie sich befinden. Um diesen Zugriff zu ermöglichen, verwenden CDN-Anbieter oft ausgeklügelte Hosting-Umgebungen, einschließlich Caching- und Proxy-Appliances; diese Mechanismen sind jedoch alle unabhängig von den DNS-Konfigurationen.

Ein **TDS** verbindet Internet-Traffic-Quellen mit Zielen. Der Begriff stammt aus dem Internetmarketing, wo ein TDS Website-Besucher mit Werbung verbindet. Böswillige Hacker haben sich diese Technik zunutze gemacht, indem sie das Konzept eines TDS, das für legitime Marketingzwecke verwendet wird, für den Einsatz im Rahmen von Cyberkriminalität modifiziert haben. Bei Infoblox haben wir schon eine ganze Reihe von Techniken zur Erstellung von TDS beobachtet, darunter Systeme, die vollständig auf DNS basieren und Entscheidungen

3 Es gibt einige Formulierungen, die implizieren, dass die Last der Auflösung des CNAME-Werts beim Stub-Resolver liegt, aber die meisten rekursiven Resolver schließen den Auflösungsprozess automatisch ab und geben eine kombinierte Antwort aus.

ausschließlich auf der Grundlage der IP-Adresse des Abfragenden treffen. In unseren früheren Veröffentlichungen zu VexTrio[4] und Prolific Puma[5] haben wir mehrere Beispiele für bösartige TDS beschrieben. VexTrio betreibt sowohl ein DNS-TDS als auch ein HTTP-basiertes TDS, während Prolific Puma einen Link-Shortener-Service betreibt. Während ein legitimes Marketing-TDS darauf abzielt, jedem Benutzer relevante Werbeinhalte bereitzustellen, kann ein bösartiges TDS auch Traffic Control beinhalten, die bestimmten Benutzern die eigentlichen Inhalte verwehrt. Einige bösartige Kampagnen verketten mehrere TDS miteinander.

Savvy Seahorse ist der erste öffentlich gemeldete Bedrohungsakteur, der DNS-CNAMEs als Teil eines bösartigen TDS missbraucht. Obwohl dies seitens des Bedrohungsakteurs mehr DNS-Kompetenz erfordert, ist das nicht ungewöhnlich, wurde bisher in der Sicherheitsliteratur jedoch nicht erkannt. Wir verwenden den Begriff **CNAME-TDS**, um die Technik zu beschreiben, bei der DNS-CNAME-Einträge zum Erstellen eines TDS verwendet werden. Auf den ersten Blick kann diese Verwendung eines TDS mit einem CDN verwechselt werden; im Gegensatz zu einem CDN ist ein TDS jedoch nicht darauf ausgelegt, allen Benutzern den gleichen leistungsfähigen Zugriff auf dieselben Inhalte zu bieten.

Die Verwendung von DNS-CNAME-Einträgen zur Erstellung eines TDS für schändliche Aktivitäten ist vielleicht kein neues Konzept für Bedrohungsakteure, aber für die Sicherheitsbranche scheint es neu zu sein. Seit mindestens 2021 verlässt sich Savvy Seahorse auf diese bisher unbekannte Methode, um Infrastruktur aufzubauen und Betrugskampagnen durchzuführen, die auf Facebook-/Meta-Benutzer abzielen, die investieren möchten. Wir verfolgen auch eine Reihe anderer Akteure mit Variationen der CNAME-Vorgehensweise.

VON CNAME ZU SeaNAME

Savvy Seahorse übernimmt den Domain-Substitutionsmechanismus von CNAME und erstellt spezifische Subdomains, die mit der primären Kampagnen-Domain verknüpft sind. Insbesondere sind alle böswilligen Kampagnen-Domains Aliase für eine Subdomain von:

`b36cname[.]site`

Beispielsweise hat Savvy Seahorse zuvor die Domain `mom[.]multi-info[.]site` in einer Kampagne verwendet, die ein Mastercard-Investmentprogramm vortäuschte. Diese Domain hatte einen CNAME-Eintrag mit dem Wert `prx16[.]b36cname[.]site`. Gleichzeitig verwendete der Akteur in seinen Kampagnen viele andere Subdomains von `multi-info[.]site`. Alle davon hatten dieselbe IP-Adresse, da Savvy Seahorse Wildcard-DNS-Konfigurationen nutzt. Abbildung 2 zeigt diese Konfiguration.

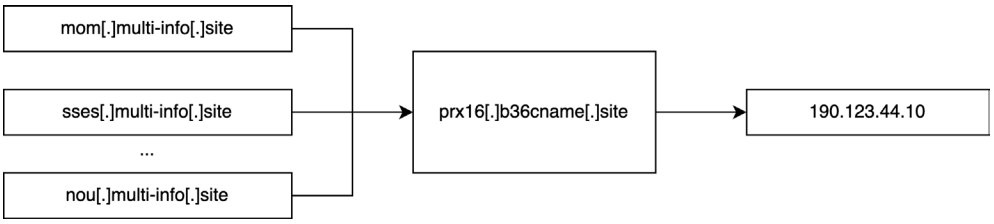


Abbildung 2: Savvy Seahorse verwendet viele Kampagnendomains gleichzeitig, die Subdomains der gleichen Basisdomain sind. Diese Subdomains teilen sich einen CNAME-Eintrag und damit eine IP-Adresse.

Savvy Seahorse verwendet dedizierte IP-Adressen zum Hosten von Inhalten. Der Akteur wechselt diese IP-Adressen regelmäßig und auf einfache Weise mittels CNAMEs, die ihm dabei helfen, einer Erkennung zu entgehen und sich erfolgreich in den DNS-Gewässern zu tarnen.

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/

Die Kampagnendomains von Savvy Seahorse weisen kein leicht erkennbares Muster auf und können sich in ihrer Hosting-Infrastruktur erheblich unterscheiden, worauf wir in späteren Abschnitten näher eingehen werden. Diese Variationen können es für Bedrohungsforscher schwieriger machen, die Aktivitäten als von einem einzigen DNS-Bedrohungsakteur stammend zu identifizieren. Letztendlich war die einzige Information, die es uns ermöglichte, dieses Netzwerk zu enttarnen, die Verwendung eines gemeinsamen CNAME.

SAVVY SEAHORSE-AKTIVITÄTEN

Savvy Seahorse ist seit August 2021 aktiv, als die Domain `b36cname[.]site` zum ersten Mal erstellt wurde. Obwohl teilnehmende Domains manchmal von Sicherheitstools erkannt werden, sind die größere Infrastruktur und die Akteure dahinter von der Sicherheitsbranche unentdeckt geblieben. Wir haben etwa 42.000 Basisdomains mit einem CNAME-Eintrag beobachtet, der eine Subdomain von `b36cname[.]site` aufführt. Um Kampagnen zu hosten, erstellt Savvy Seahorse mehrere Subdomains für jede SLD mit Hilfe eines Algorithmus zur Generierung von Domains (DGA), wobei der Hostname pseudo-zufällig und in den meisten Fällen drei Zeichen lang ist. Im nächsten Abschnitt gehen wir näher auf dieses Hostnamen-Muster ein.

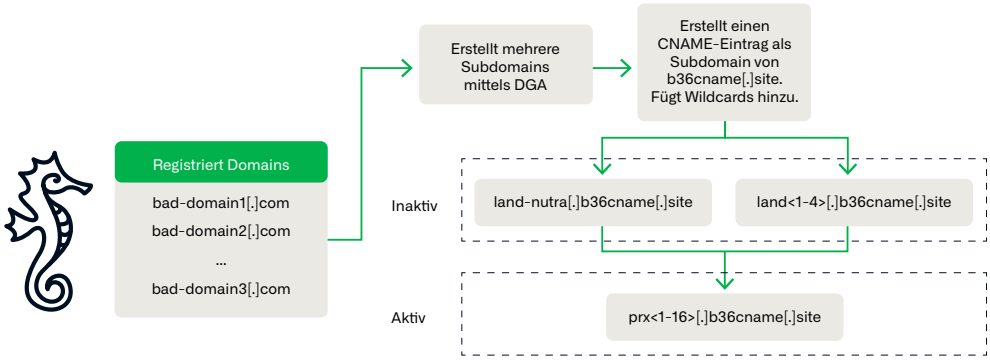


Abbildung 3: Ein Überblick über die Aktivitäten von Savvy Seahorse

SeaNAME-Muster und Wildcarding

Jeder der CNAME-Einträge von Savvy Seahorse fällt unter eines der drei Muster, wie von Tabelle 1 gezeigt.

CNAME-Muster	Zweck
`land-nutra[.]b36cname[.]site`	Subdomain, die vorübergehend als CNAME verwendet wird, bevor Kampagnen aktiv werden, für geparkte Domains
`land<1-4>[.]b36cname[.]site`	Subdomains, die vorübergehend als CNAMEs verwendet wurden, bevor Kampagnen aktiv wurden, möglicherweise zu Testzwecken
`prx<1-16>[.]b36cname[.]site`	Subdomains, die für aktive Kampagnen verwendet werden

Tabelle 1: Muster und Zwecke von CNAME-Einträgen

Im Folgenden sind die Verhaltensweisen aufgeführt, die wir bei der Verwendung der einzelnen CNAME-Typen durch Savvy Seahorse beobachtet haben:

Domains, die `land-nutra[.]b36cname[.]site` als CNAME-Eintrag hatten, wurden während dieser Zeit geparkt. Als die Kampagnen aktiv wurden, änderten die Akteure den CNAME-Eintrag in `prx<1-16>[.]b36cname[.]site`.

In ähnlicher Weise wurden Domains, die irgendwann land<1–4>[.]b36cname[.]site als CNAME-Eintrag hatten, für Kampagnen verwendet, die inaktiv waren. Diese Domains wurden dann auch in den Eintrag prx<1–16>[.]b36cname[.]site geändert, als Kampagnen aktiviert wurden.

Die land<1–4>-CNAMEs könnten zum Testen einiger Kampagnen verwendet werden, bevor sie aktiviert werden.[6]

Savvy Seahorse hat Wildcard-CNAME-Antworten konfiguriert, um seine Verwendung von DNS auf einfache Weise zu verwalten. In diesem Fall wird für eine Abfrage an eine beliebige Subdomain (z. B. wildcard[.]xsdelx[.]top) der Basisdomain eine Antwort ausgegeben, die zeigt, dass sie denselben Ressourceneintrag haben. In Abbildung 4 sehen Sie das Ergebnis eines dig-Befehls zur Abfrage von wildcard[.]xsdelx[.]top der Savvy Seahorse-Basisdomain xsdelx[.]top. Die Antwort zeigt, dass die Abfrage als Ergebnis des Wildcardings den CNAME-Eintrag prx2[.]b36cname[.]site ausgegeben hat. Wildcarding ermöglicht es dem Akteur, die Einträge für jede neue Subdomain, die er erstellt, automatisch zu setzen, was eine effizientere Verwaltung einer großen Infrastruktur ermöglicht.

```
; <<>> 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+XmNFW1lNak 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 bZsVI7YD3vA1Rf7HfleOavQJ0nC57B3dsED4jKJ32ulMsHNxJ/+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
```

Abbildung 4: Wildcard-Antwortverhalten auf eine zufällige Subdomain einer existierenden Savvy Seahorse-Basisdomain. Die Server haben auf die Subdomain reagiert und so gezeigt, dass sie einen CNAME-Eintragswert von prx2[.]b36cname[.]site *hat, die CNAME-Domain des Akteurs.*

Domains

Bedrohungsakteure nutzen DGAs häufig als Tools zum Generieren einer großen Anzahl pseudo-zufälliger Domainnamen, mit denen sie Kampagnen und andere böswillige Aktivitäten durchführen können. Die in diesen DGAs verwendeten Domains folgen oft ähnlichen sichtbaren Mustern, die von speziellen Algorithmen leicht erkannt werden können und so die Zuordnung zu einem Bedrohungsakteur erleichtern. Während Savvy Seahorse offenbar DGAs zum Erstellen vieler seiner SLDs und Subdomains verwendet, scheinen diese DGAs keinem bestimmten Muster zu folgen. Vielmehr haben wir beobachtet, dass der Akteur mehrere DGA-Muster für SLDs verwendet, wie Tabelle 2 zeigt.

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

Musterbeschreibung	Variationen desselben vollständigen Keywords	Vollständiges Keyword, an das zufällige Zeichen gleicher Länge angehängt werden	Variationen der Schreibweise der zweiten Hälfte eines Keywords	Variationen eines Keywords innerhalb der Domain
Beispiel-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

Tabelle 2: Savvy Seahorse-SLD-Muster und -Beispieldomänen

Eine gängige Technik zur Identifizierung dieser DGA-Typen ist die Verwendung von Algorithmen für maschinelles Lernen. Man könnte N-Gramm verwenden,[7] um einige der Cluster in jeder Spalte in Tabelle 2 erfolgreich zu erkennen, aber diese Methode würde nicht erkennen, dass alle diese Cluster zu einem einzigen DNS-Bedrohungsakteur gehören, wenn man nur die Merkmale der Domain-Label-Eigenschaften betrachtet. Alle vier der oben genannten Cluster haben sehr unterschiedliche Muster – wie auch einige andere Domain-Cluster, die Savvy Seahorse erstellt –, die ein N-Gramm-basiertes Modell nicht als zur selben Gruppe gehörig erkennen könnte.

Die obigen Beispiele zeigen auch, dass sich die Akteure nicht nur an eine Top-Level-Domain (TLD) halten, selbst innerhalb klarer DGA-Benennungsmuster. Savvy Seahorse verwendet mehrere TLDs, oft solche, von denen bekannt ist, dass sie häufig missbraucht werden. Die Top 5 nach Anzahl der Domains sind site, `xyz`, `com`, `top` und `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

Tabelle 3: Beispieldomains für die am häufigsten verwendeten TLDs in den bösartigen Kampagnen von Savvy Seahorse

Wir haben bereits erwähnt, dass die Hostnamen in den meisten Fällen pseudo-zufällig und drei Zeichen lang zu sein scheinen, aber wir haben einige Beispiele mit längeren Labeln gesehen (siehe Tabelle 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

Tabelle 4: Beispiele für Subdomain-Muster

Registrierungsinformationen

Savvy Seahorse verfolgt keinen konventionellen Ansatz bei der Handhabung von Registrierungen, was dem Akteur hilft, einer Erkennung zu entgehen. Eine gängige Technik, die DNS-Bedrohungsakteure anwenden, ist die Massenregistrierung von Domains über denselben Registrar sowie die Nutzung desselben Internetdienstanbieters (ISP) für das Hosting, um die Verwaltung ihrer Infrastruktur einfacher und zeitsparender zu gestalten. Viele Registrare bieten APIs an, um die Massenregistrierung von Domains zu erleichtern. Während die meisten Registrare beabsichtigen, dass die APIs für legitime Zwecke genutzt werden, ist bekannt, dass Cyberkriminelle diese Funktion missbrauchen, um leichter Tausende von Domains für ihre Kampagnen erstellen zu können. In unserem Blogeintrag zu RDGAs vom Oktober 2023 wird dieser Prozess ausführlicher beschrieben.[8]

Wenn Akteure denselben Registrar und dieselbe Infrastruktur nutzen, um ihre Domains zu erstellen und zu hosten, kann es oftmals unkompliziert sein, Domains, die demselben Akteur gehören, über gemeinsame Registrierungs-Metadaten zu finden. Savvy Seahorse scheint einen geduldigeren Ansatz zu verfolgen, denn seine Infrastruktur ist über eine Reihe verschiedener Registrare und Hosting-Anbieter verteilt. Wir haben für alle Domains mit einer Subdomain von `b36cname[.]site` als CNAME-Eintrag 30 verschiedene Registrierungsorganisationen und 21 ISPs beobachtet. Diese Technik macht es für Sicherheitsforscher schwieriger, Domains zu korrelieren und die Infrastruktur eines Akteurs zu erkennen.

Die Unterschiede in den Registrierungs-Metadaten für Domains mit einem `b36cname`-Eintrag ließen uns ursprünglich vermuten, dass dieser Akteur ein Dienstleister für andere Cyberkriminelle sein könnte, die Betrugskampagnen durchführen. Unsere Analyse hat jedoch gezeigt, dass die Finanzbetrugskampagnen, die über dieses Netzwerk laufen, alle die gleichen Elemente und das gleiche Gesamtverhalten aufweisen, was uns zu dem Schluss führt, dass die Kampagnen höchstwahrscheinlich von einem einzigen Akteur gesteuert werden: Savvy Seahorse. Wir besprechen diese Kampagnen und ihren Inhalt im Abschnitt „Kampagnenanalyse“ ausführlicher.

IP-Adressen

Savvy Seahorse scheint ungefähr 50 dedizierte IP-Adressen zu verwenden und ändert diese regelmäßig, wie Abbildung 5 zeigt. Die kleinen Lücken in jedem Zeitleistenbalken stellen dar, wann Savvy Seahorse die mit einem CNAME-Eintrag verknüpfte IP geändert hat.

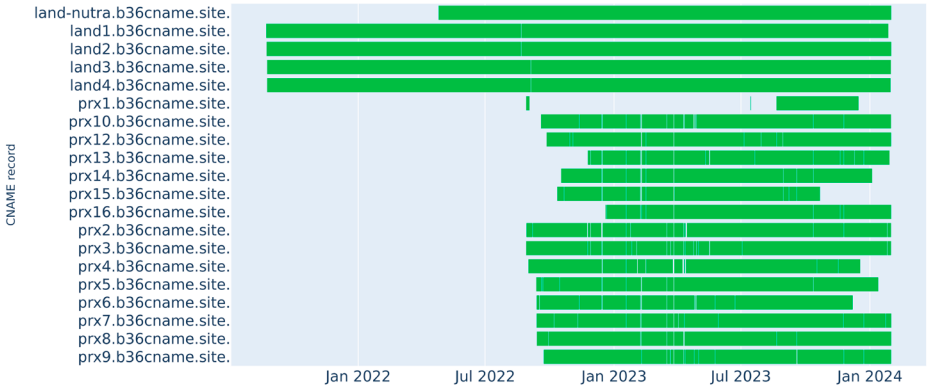


Abbildung 5: Zeitleiste der IP-Adressänderungen nach CNAME. Jede Leiste zeigt die Zeit, die jeder CNAME-Eintrag für eine bestimmte IP-Adresse aufwendet, und enge Lücken zeigen an, wann sich diese Werte geändert haben. Akteure wechseln oft die IP-Adressen, um einer Entdeckung zu entgehen.

Basierend auf einer Analyse der IP-Änderungen haben wir Folgendes beobachtet:

- `land-nutra[.]b36cname[.]site` ist der einzige CNAME mit einer einzigen IP-Adresse, was mit dem Verhalten übereinstimmt, das wir beobachtet haben, und das darauf hindeutet, dass die mit diesem CNAME verbundenen Domains geparkt werden. Diese IP-Adresse weist eine signifikant hohe Gesamtzahl an Domains auf, die mit ihr verbunden sind, ein Merkmal, das mit IP-Adressen übereinstimmt, die zum Parken verwendet werden.

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

- Alle vier CNAMEs, die das `land<1-4>[.]b36cname[.]site`-Muster nutzen, haben die IP-Adressen nur einmal geändert.
- `prx<1-16>[.]b36cname[.]site`-CNAMEs ändern häufig die IP-Adressen. Dieses Muster deutet darauf hin, dass diese IPs höchstwahrscheinlich ausschließlich für aktive Betrugskampagnen verwendet werden, da regelmäßige Änderungen an den IPs eine Taktik sind, die Bedrohungsakteure anwenden, um der Erkennung und Blockierung durch Sicherheitsanbieter zu entgehen.
- Es gibt einige Vorkommnisse, bei denen der Bedrohungsakteur die IPs für mehrere CNAMEs gleichzeitig für den gleichen Wert ändert.
- Einige CNAMEs, darunter `prx6[.]b36cname[.]site` und `prx15[.]b36cname[.]site`, werden vom Bedrohungsakteur derzeit anscheinend nicht verwendet.

KAMPAGNENANALYSE

Savvy Seahorse nutzt eine einzigartige Infrastruktur, um eine Reihe von verschiedenen Betrugskampagnen mit Finanz- und Anlagethemen durchzuführen. Die Kampagnen verwenden eine Vielzahl hochentwickelter Locktechniken, folgen jedoch alle einem ähnlichen Muster und haben letztlich das Ziel, die persönlichen und finanziellen Daten des Opfers zu stehlen, um sich daran zu bereichern. Die für diese Kampagnen verwendeten Sprachen sind unter anderem Englisch, Russisch, Polnisch, Italienisch, Deutsch, Französisch, Spanisch, Tschechisch und Türkisch.

- Aktive Kampagnen finden auf Subdomain-Ebene statt, wobei jede Subdomain einen `prx<1-16>[.]b36cname[.]site`-CNAME-Eintrag hat.

Kampagnendetails

Savvy Seahorse verwendet in jede Webseite eingebettete Registrierungsformulare, um den Vor- und Nachnamen, die E-Mail-Adresse und die Telefonnummer des Opfers zu erfassen. Zwei Beispiele für dieses Registrierungsformular, eines auf Polnisch und das andere auf Englisch, finden Sie in Abbildung 6.

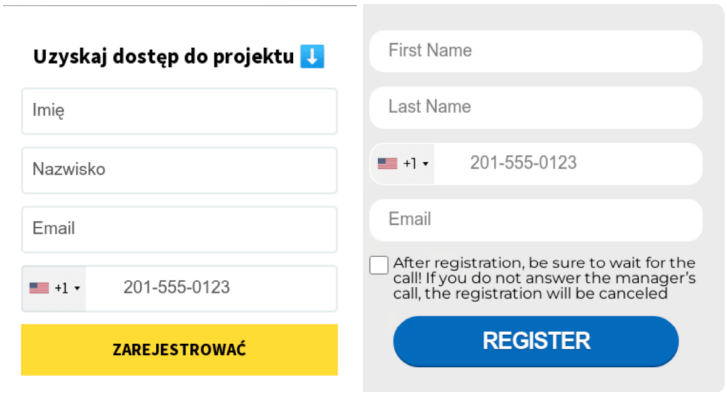


Abbildung 6: In den Kampagnen von Savvy Seahorse verwendete Registrierungsformulare

Validierung und Umleitung

Nachdem der Benutzer seine Informationen in diese Formulare eingegeben hat, wendet sich die Domain an die sekundäre TDS-Domain, die Savvy Seahorse in seinen Kampagnen verwendet, `getyourapi[.]site`, um die Informationen zu überprüfen, einschließlich der IP-Adresse des Benutzers, Geolokalisierung und Gültigkeit der angegebenen Telefonnummer und E-Mail-Adresse. Je nachdem, welche Überprüfungen bestanden werden, haben wir drei verschiedene Szenarien beobachtet:

1. Wenn die Formulardaten gültig sind, sich der Benutzer jedoch zuvor schon einmal mit derselben E-Mail-Adresse/Telefonnummer registriert hat, wird auf der Webseite angezeigt, dass der Benutzer bereits registriert ist.
2. Wenn die Formulardaten gültig sind, der Benutzer diese Domain aber schon einmal über dieselbe IP-Adresse besucht hat, wird auf der Seite eine Meldung angezeigt, die die Registrierung bestätigt und besagt, dass ein Vertreter ihn für weitere Informationen anrufen wird. Es erfolgt keine Umleitung.
3. Wenn die Formulardaten gültig sind und der Benutzer die Domain mit einer bisher unbekannten IP-Adresse besucht, wird er auf eine gefälschte Handelswebseite weitergeleitet, ähnlich wie der in Abbildung 7 gezeigten.

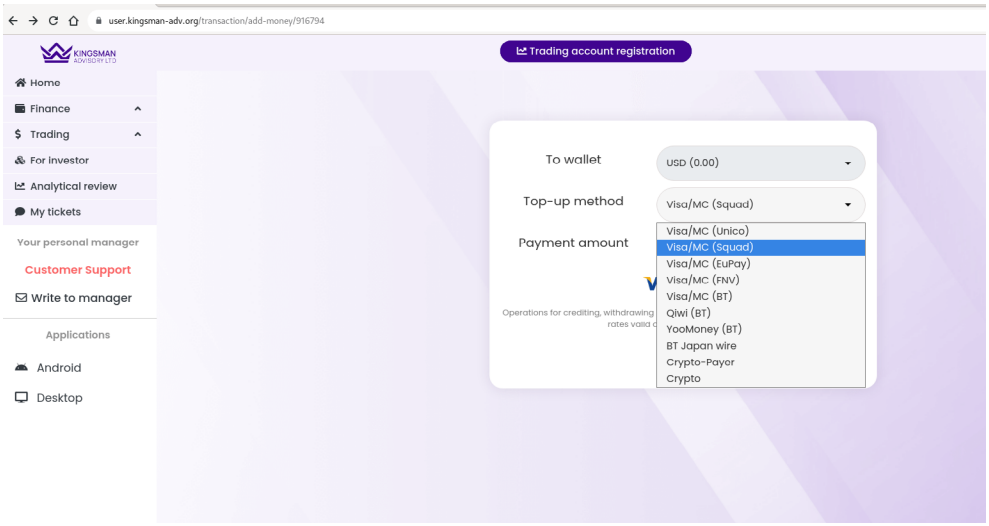


Abbildung 7: Eine gefälschte Handelsplattform von Savvy Seahorse

Ein wichtiges Detail ist, dass der Akteur die Daten des Benutzers validiert, um Datenverkehr aus einer vordefinierten Liste von Ländern auszuschließen, die unter anderem die Ukraine, Indien, Fidschi, Tonga, Sambia, Afghanistan und Moldawien enthält, wobei die Gründe für die Auswahl dieser Länder unklar sind. Die erste Validierung bezieht sich auf die Telefonnummer, die in das Registrierungsformular eingegeben wird. Wenn sie aus einem der Länder stammt, die auf der Blockliste stehen, erscheint auf der Webseite eine Meldung, die in etwa besagt: „**Das Programm wird in Ihrer Region nicht unterstützt.**“ Wenn der Benutzer eine akzeptable Telefonnummer zusammen mit allen anderen gültigen Informationen wie oben aufgeführt eingibt, sendet der Akteur die Informationen an seine sekundäre TDS-Domain, um die Geolokalisierung der IP-Adresse des Benutzers anhand der ausgeschlossenen Länder zu validieren und zu entscheiden, ob eine Weiterleitung erfolgt oder nicht.

Handelsplattform

Sobald der Benutzer weitergeleitet wird, wird auf der gefälschten Handelsplattform automatisch ein Konto mit den Angaben aus dem Registrierungsformular für ihn eingerichtet. Diese Plattform scheint sehr ausgeklügelt zu sein und bietet die Möglichkeit, eine Desktop-Anwendung herunterzuladen, sowie Links zu einer Android-App namens App4World im Google Play Store.

Der Benutzer wird dann aufgefordert, Geld aus verschiedenen Quellen wie Visa/Mastercard, einem Krypto-Wallet oder russischen Zahlungsanbietern wie Qiwi und YooMoney in sein „Wallet“ einzuzahlen. Ein „Aufladungsbetrag“ von mindestens 50 USD ist erforderlich, um Geld auf ein Wallet einzahlen zu können. Die endgültige Umleitung auf eine von acht möglichen Zahlungsabwicklungsdomains (siehe Tabelle 5) erfolgt, sobald der Benutzer eine Zahlungsquelle und einen Einzahlungsbetrag angibt. Welche Domain die Kampagne verwendet, um Finanzinformationen von den Opfern zu sammeln, hängt davon ab, von welcher Quelle diese Geld überweisen wollen.

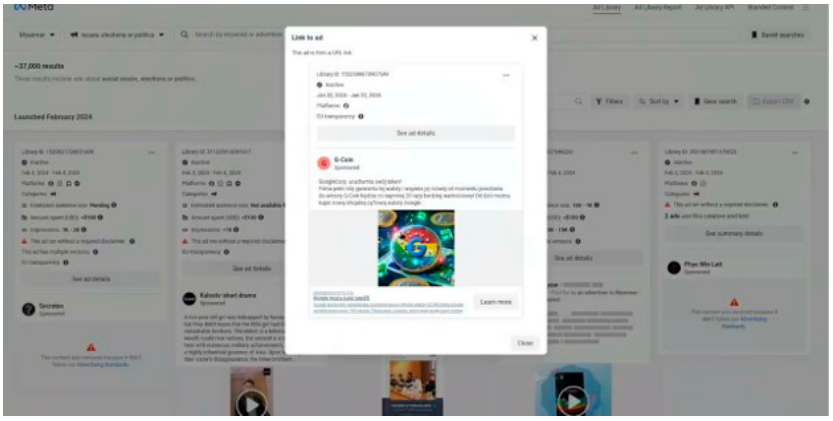
Zahlungsquelle	Zahlungsdomain	Beschreibung der Zahlungsdomain
Visa/MC (Unico)	makeyourpay[.]com	Neu registrierte Domain, die eine Webseite zur Zahlungsabwicklung hostet; russischsprachige Subdomains
Visa/MC (Squad)	checkout[.]flutterwave[.]com	Hostet ein legitimes Finanzinfrastrukturunternehmen mit Sitz in Nigeria
Visa/MC (EuPay)	ap-gateway[.]mastercard[.]com	Legitimes Zahlungsgateway für Mastercard
Visa/MC (BT)	sci[.]pointpayment[.]net	Gehostet auf derselben dedizierten IP wie eine Reihe anderer verdächtiger Zahlungsdomains
Qiwi (BT)	qiwi[.]bppsa[.]com	Die Basisdomain hostet eine russischsprachige Webseite zur Zahlungsabwicklung
YooMoney (BT)	ymoney[.]bppsa[.]com	Die Basisdomain hostet eine russischsprachige Webseite zur Zahlungsabwicklung
BT Japan (wire)	processing[.]betatransfer[.]io	API für Betatransfer Kassa, einen Hochrisiko-Zahlungsabwicklungsdienst (wird hauptsächlich für Online-Glücksspiel verwendet)
Crypto-Payer Crypto	crypto-payer[.]co	Registriert im Dezember 2023

Tabelle 5: Zahlungsabwicklungsdomains zum Erfassen der Finanzdaten des Opfers

Bei näherer Untersuchung stellte sich heraus, dass der Akteur offenbar Geld für mindestens eine der Zahlungsabwicklungsdomains (sci[.]pointpayment[.]net) an die SberBank weiterleitet, eine mehrheitlich in russischem Staatsbesitz befindliche Bank, wie Abbildung 8 zeigt.

Abbildung 8: Finanzielle Details für sci[.]pointpayment[.]net

Im folgenden Video sehen Sie einen Überblick über die gefälschte Handelsplattform.



Hier können Sie das Video ansehen: „Savvy Seahorse Campaign Walkthrough“

Meta-Pixel

Da Savvy Seahorse diese Kampagnen über Facebook/Meta-Anzeigen bewirbt und verbreitet (siehe Abbildung 9), stellen alle in aktiven Kampagnen verwendeten Domains mehrere Verbindungen zu `connect[.]facebook[.]net` und `www[.]facebook[.]com` her. Der Akteur verwendet außerdem Meta-Pixel, ein legitimes Tool, um die Leistung der Anzeigen zu verfolgen und zu optimieren.[9]

Ein Meta-Pixel ist ein JavaScript-Code, der aus zwei Teilen besteht:

- Einem „script“, das beim Laden der Seite ausgeführt wird und das Facebook-Pixel initialisiert sowie ein „PageView“-Ereignis trackt.
- Einem „noscript“, das ausgeführt wird, wenn der Benutzer JavaScript in seinem Browser deaktiviert hat. In diesem Abschnitt wird ein 1x1-Pixel-Bild angezeigt, um das Ereignis zu tracken.

Jedes Meta-Pixel verfügt über eine eindeutige ID-Nummer, die wir in den HTTP-Verbindungen zu Facebook sehen können. Wir haben einige Kampagnen beobachtet, die auf demselben SLD gehostet werden, wobei sich verschiedene Subdomains die gleiche ID teilen, andere jedoch zufällig ausgewählt zu sein scheinen.

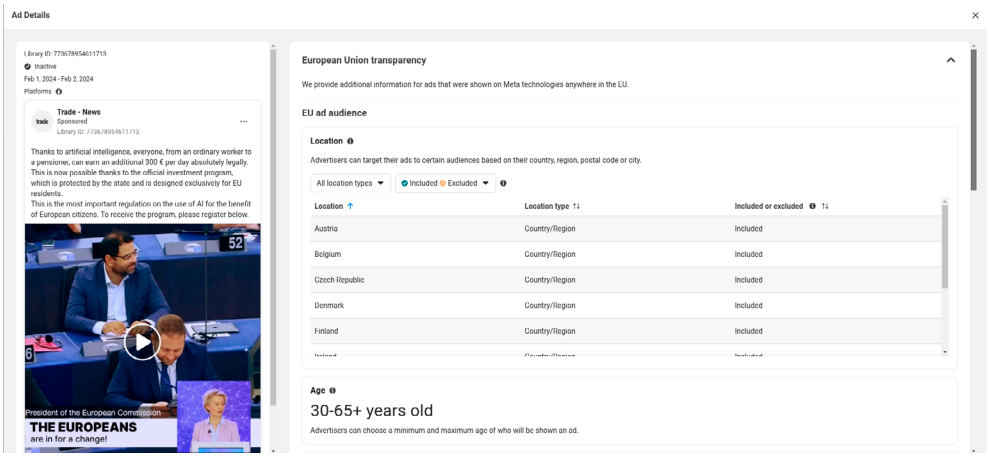


Abbildung 9: Facebook-Anzeigendetails für die Kampagne von Savvy Seahorse mit Angabe der Zielländer und Altersdemografie

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

Themen

Die spezifischen Themen der Kampagnen von Savvy Seahorse können sehr unterschiedlich sein und umfassen Köder, die seriöse Unternehmen wie Apple als Investitionsmöglichkeiten vortäuschen, und die Einbindung von Bots, die sich als WhatsApp, ChatGPT und Tesla ausgeben.

Investitionsprogramme, die Unternehmen imitieren

Eines der häufigsten Themen, die Savvy Seahorse während seiner gesamten Geschäftszeit verwendet hat, betrifft sogenannte „Earning Projects“ oder Investitionsprogramme, für die behauptet wird, dass der Benutzer die Möglichkeit hat, einen bestimmten Geldbetrag zu verdienen, wenn er sich mit seinen persönlichen Daten registriert. Bedrohungsakteure wenden häufig eine beliebte Phishing-Kampagnentechnik an, bei der sie versuchen, sich als leicht erkennbare Marken und Unternehmen auszugeben, um das Vertrauen des Benutzers zu gewinnen. Tabelle 6 enthält einige Beispiele, die wir gesehen haben.

Kampagnen-Subdomain	Zugehöriger CNAME	Kampagnenbeschreibung
new[.]xsdelx[.]top	prx2[.]b36cname[.]site	Russischsprachige Kampagne, die Tesla und X vortäuscht und Benutzer dazu auffordert, „am Projekt von Elon Musk teilzunehmen“, um 12.000 EUR pro Monat zu erhalten
bwn[.]objectop[.]xyz	prx7[.]b36cname[.]site	Englischsprachige Kampagne, die Imperial Oil vortäuscht, ein legitimes kanadisches Erdölunternehmen. Die Landingpage enthält eine interaktive „Umfrage“ und ermutigt die Benutzer, 250 bis 1.000 USD zu investieren
sej[.]progmedisd[.]site	prx9[.]b36cname[.]site	Polnischsprachige Kampagne ab Februar 2023 für das „Libra automatic earning project“, das behauptet, von Mark Zuckerberg geschaffen worden zu sein, und den Benutzern einen Verdienst von bis zu 300.000 polnischen Złoty (PLN) verspricht

Tabelle 6: Beispiele für Finanzkampagnen von Savvy Seahorse

Die Abbildungen 10 und 11 zeigen Screenshots von einigen der Kampagnen in Tabelle 6. Andere Beispiele für Unternehmen, die Savvy Seahorse bereits vorgetäuscht hat, sind unter anderem Apple, Meta, Mastercard, Visa und Google.

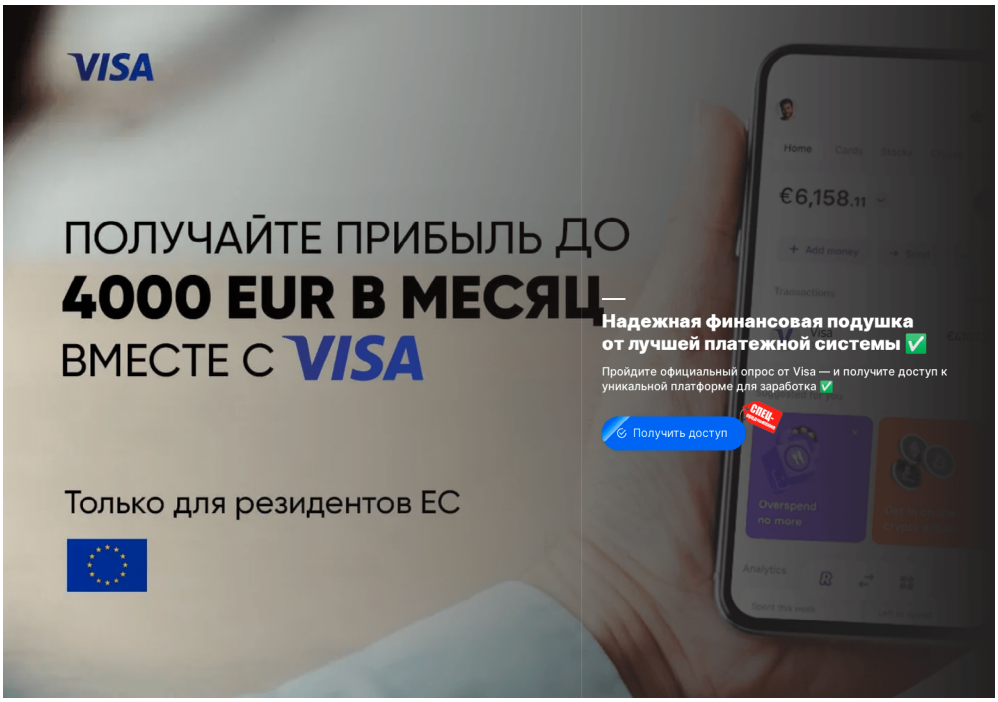


Abbildung 10: Landingpage für `visa[.]lukzev[.]xyz`*, eine russischsprachige Kampagne, die Visa vortäuscht*

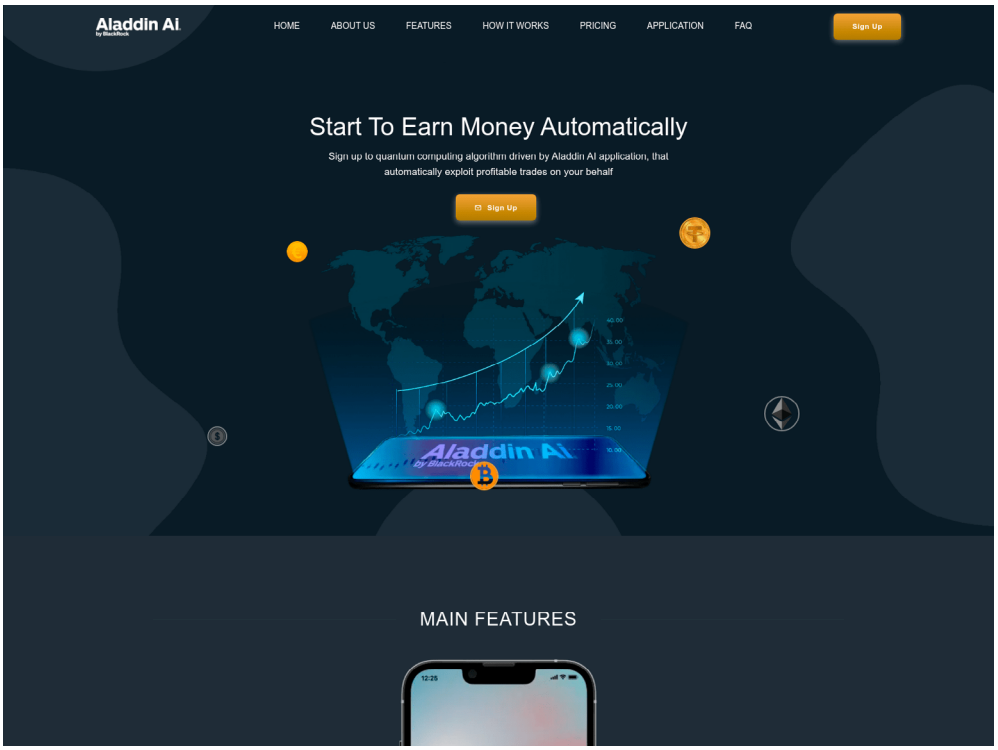


Abbildung 11: Landingpage für `adin[.]czproftes[.]xyz`*, das sich als die Portfolio-Management-Plattform von BlackRocks ausgibt*

Gefälschte Bots

Wir haben einige Kampagnen gesehen, bei denen fortschrittliche Ködertechniken mit Chatbots eingesetzt wurden, die sich unter anderem als ChatGPT, WhatsApp und Tesla ausgaben. In letzter Zeit sind Betrügereien mit dieser Art von Bots zu einem häufigen Trend bei Bedrohungsakteuren geworden, die das Vertrauen der Benutzer gewinnen wollen, um deren persönliche Daten zu stehlen.[10] Der Screenshot in Abbildung 12 zeigt unsere Interaktionen mit einem dieser Chatbots aus einer Kampagne, die Tesla vortäuscht.

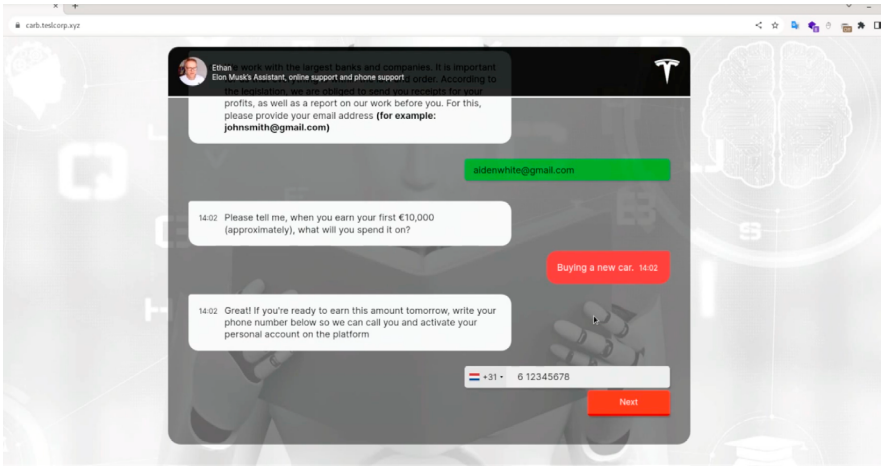


Abbildung 12: Gefälschter Bot mit Tesla-Thema, der in einer Savvy Seahorse-Kampagne verwendet wird

Die Bots stellen dem Benutzer Fragen zu seinem Interesse an potenziellen Verdienst- und Investitionsmöglichkeiten, folgen letztlich aber dem gleichen Muster wie andere Kampagnen: Sie fordern den Benutzer auf, sich mit seinen persönlichen Daten zu registrieren, bevor er auf die gefälschte Handelsplattform umgeleitet wird.

ZUSAMMENFASSUNG

Bei Infoblox konzentrieren wir uns weiterhin darauf, neue Arten aufzudecken, auf die Bedrohungsakteure DNS missbrauchen, um ihre kriminellen Aktivitäten zu verbergen. Die Technik von Savvy Seahorse, DNS-CNAMEs als TDS zur Verwaltung seiner böswilligen Aktivitäten zu verwenden, zeigt, dass DNS die effektivste Methode ist, um die Aktivitäten von Cyberkriminellen zu verfolgen und zu unterbrechen. Letztendlich war es unsere Analyse der CNAME-Muster, die es uns ermöglicht hat, diesen Akteur und die einzigartigen Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTP) zu entdecken, die er einsetzt, um sein großes Netzwerk von Betrugskampagnen zu betreiben.

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

AKTIVITÄTSINDIKATOREN

Nachfolgend finden Sie ein Beispiel für Indikatoren, die in den Kampagnen von Savvy Seahorse verwendet werden. Eine umfassendere Liste von Indikatoren gibt es in unserem GitHub-Repository, das Sie hier finden.

Indikator	Art des Indikators
getyourapi[.]site	Sekundäre TDS-Domäne von Savvy Seahorse
land-nutra[.]b36cname[.]site	Subdomain, die als CNAME-Eintrag für geparkte Domains verwendet wird
land<1-4>[.]b36cname[.]site	Subdomains, die als CNAME-Einträge für inaktive Kampagnen verwendet werden
prx<1-16>[.]b36cname[.]site	Subdomains, die als CNAME-Einträge für aktive Kampagnen verwendet werden
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 für aktive Savvy Seahorse-Kampagnen
ultra-vest[.]one kingsman-adv[.]org abyss-world-asset[.]net	Gefälschte Handelswebsites, auf die der Benutzer bei einigen Kampagnen weitergeleitet wird
sci[.]pointpayment[.]net makeyourpay[.]com qiwi[.]bppsa[.]com ymoney[.]bppsa[.]com processing[.]betatransfer[.]io crypto-payer[.]co	Domains zur Zahlungsabwicklung zur Erfassung der Finanzdaten des Opfers

Indikator	Art des Indikators
ap-gateway[.]mastercard[.]com	Legitime Domain für Mastercard zur Erfassung der Finanzdaten des Opfers
checkout[.]flutterwave[.]com	Legitime Domain für Flutterwave, einen nigerianischen Zahlungsdienst, der zur Erfassung der Finanzdaten des Opfers benutzt wird
auproject[.]xyz badanie-pl[.]site blog-vcnews[.]site capital-inwest[.]site dasms[.]xyz duums[.]xyz esbopehan[.]xyz	Basisdomänen von Savvy Seahorse

INFOBLOX THREAT INTEL

Infoblox Threat Intel ist der führende Anbieter von Original-DNS-Bedrohungsdaten und hebt sich von der Masse der Aggregatoren ab. Was zeichnet uns aus? Zwei Dinge: extrem umfassende DNS-Kenntnisse und beispiellose Sichtbarkeit. DNS ist bekanntermaßen schwierig zu interpretieren und zur „Jagd“ einzusetzen, aber unser tiefes Verständnis und unser einzigartiger Zugang ermöglichen es uns, Cyberbedrohungen aufzuspüren. Wir sind proaktiv, nicht nur defensiv, und nutzen unsere Erkenntnisse, um Cyberkriminalität dort zu unterbinden, wo sie entsteht. Wir glauben auch an den Wissensaustausch, um die breitere Sicherheits-Community zu unterstützen, indem wir detaillierte Forschungsergebnisse und Indikatoren auf GitHub veröffentlichen. Darüber hinaus sind unsere Informationen nahtlos in unsere Infoblox DNS Detection and Response-Lösungen integriert, sodass Kunden automatisch von ihren Vorteilen und extrem niedrigen Falsch-Positiv-Raten profitieren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com

Version: 20240216v1