infoblox

Threat Intel

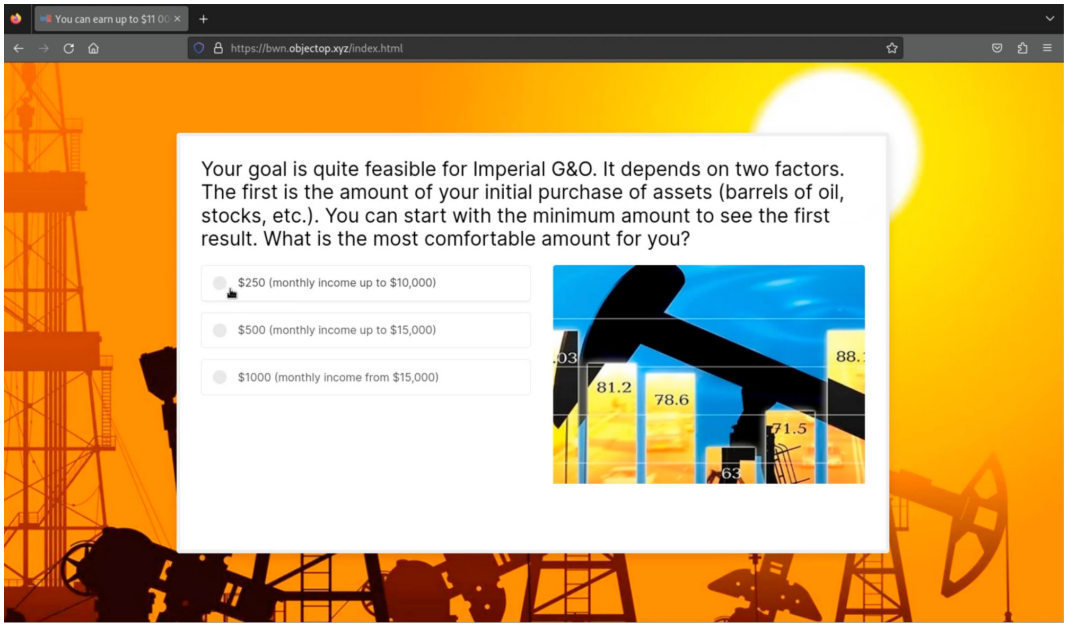
CUIDADO CON LAS AGUAS POCO PROFUNDAS: SAVVY SEAHORSE ATRAE A SUS VÍCTIMAS A PLATAFORMAS DE INVERSIÓN FALSAS A TRAVÉS DE ANUNCIOS DE FACEBOOK

Autores:
Stelios Chatzistogias
Laura da Rocha
Darby Wise

ÍNDICE

RESUMEN EJECUTIVO

Los actores de amenazas del DNS nunca dejan de sorprendernos. Todos los días, nos enteramos de nuevas y creativas campañas que han ideado para explotar a las víctimas. Las estafas de inversión son una de ellas. La Comisión Federal de Comercio de Estados Unidos informó de que en ese país se perdió más dinero por estafas de inversión durante 2023 que por cualquier otro tipo de estafa, con un total de más de 4.600 millones de dólares robados a las víctimas.[1] Savvy Seahorse es un actor de amenazas del DNS que convence a las víctimas para que creen cuentas en plataformas de inversión falsas y hagan depósitos en una cuenta personal, para, a continuación, transferir esos depósitos a un banco en Rusia. Este actor utiliza anuncios de Facebook para atraer usuarios a sus sitios web y, en última instancia, hacer que se registren en plataformas de inversión falsas. Los temas de la campaña suelen implicar la suplantación de empresas conocidas como Tesla, Facebook/Meta e Imperial Oil, entre otras.



Las campañas de Savvy Seahorse son sofisticadas. Utilizan técnicas avanzadas, como la incorporación de falsos bots de ChatGPT y WhatsApp que proporcionan respuestas automatizadas a los usuarios y los instan a introducir información personal a cambio de supuestas oportunidades de inversión de alto rendimiento. Se sabe que estas campañas se dirigen a hablantes de ruso, polaco, italiano, alemán, checo, turco, francés e inglés, al tiempo que protegen específicamente a las posibles víctimas de Ucrania y varios otros países.

Savvy Seahorse abusa del Domain Name System (DNS) de manera oscura: aprovecha los registros de nombres canónicos (CNAME) del DNS para crear un sistema de distribución de tráfico (TDS) destinado a sofisticadas campañas de estafas financieras. Como consecuencia, Savvy Seahorse puede controlar quién tiene acceso al contenido y actualizar dinámicamente las direcciones IP de las campañas maliciosas. Esta técnica de uso de CNAME ha permitido al actor de amenazas evadir la detección por parte del sector de la seguridad; hasta donde sabemos, este es el primer informe que se centra en el uso de CNAME como un TDS diseñado para fines maliciosos.

En este documento, presentamos el concepto de un TDS de CNAME y analizamos cómo Savvy Seahorse utiliza registros CNAME para llevar a cabo campañas de estafa a gran escala, que habían "pasado desapercibidas" en el sector de la seguridad hasta ahora. Las principales conclusiones son:

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

- Savvy Seahorse lleva a cabo campañas a través de anuncios de Facebook.
- Lleva operando al menos desde agosto de 2021.
- Utiliza alojamiento dedicado y cambia de direcciones IP con regularidad.
- Las campañas individuales son de corta duración (cada subdominio se anuncia durante un plazo de 5 a 10 días).
- Al parecer, utiliza un sistema de despliegue gradual en el que el registro CNAME del dominio de una campaña cambia según si está activo en ese momento o no.
- Utiliza entradas de DNS comodín, lo que le permite crear un gran número de campañas independientes con rapidez, pero puede añadir confusión al análisis del DNS pasivo (pDNS).
- Los datos personales de la víctima se envían a un servidor TDS secundario basado en HTTP para validar la información y aplicar el geovallado a fin de excluir a Ucrania y algunos otros países.
- El segundo TDS basado en HTTP también efectúa un seguimiento de las direcciones IP y de correo electrónico de los usuarios a lo largo del tiempo.

UN POCO DE JERGA

Dados los centenares de documentos de solicitud de comentarios (RFC) relacionados con el DNS, el vocabulario puede resultar confuso y conflictivo, especialmente si se combina con la forma en que el sector de la seguridad utiliza la terminología del DNS más allá del ámbito de las redes. Estos son los términos sobre el DNS que usamos en el documento:

- **Nombre de dominio** hace referencia a un nombre de dominio completo (FQDN) que tiene registros DNS asignados. Tanto`www[.]infoblox[.]com` como `infoblox[.]com` son nombres de dominio. Usamos FQDN, nombre de dominio y dominio indistintamente.
- **Dominio base** será el dominio de segundo nivel (SLD) asociado con un nombre de dominio o subdominio; por ejemplo, el dominio base de `www[.]infoblox[.]com` y `blogs[.]infoblox[.]com` es `infoblox[.]com`. Un dominio base puede entenderse como el dominio registrado.
- **Subdominio** hace referencia a un dominio anidado correctamente dentro de otro. Por ejemplo, `www[.]infoblox[.]com` y `blogs[.]infoblox[.]com` son subdominios de `infoblox[.]com`. Los administradores de DNS tal vez discrepen, pero esta explicación es más comprensible para los lectores de threat intelligence.
- **Nombre de host** hace referencia a la parte situada más a la izquierda de un dominio, por ejemplo: `www`.
- **Dominio CNAME** es el valor del nombre de dominio contenido en un registro de nombre de dominio canónico (CNAME).
- **Dominio de campaña** es, en este caso, el que se utiliza para atraer a una víctima con un anuncio de Facebook.

Registros CNAME en DNS

Un registro CNAME en el DNS proporciona un mecanismo para crear alias de nombres de dominio. Estos registros se utilizan para una amplia gama de fines con el objetivo de facilitar y reforzar la gestión la configuración del DNS. Reducen el número total de registros en el DNS y facilitan la sustitución de direcciones IP. El caso de uso clásico de los registros CNAME es asignar al dominio base subdominios utilizados en sitios web.

Por ejemplo, la mayoría de los sitios web utilizan como nombre de host `www`. El FQDN `www.infoblox.com` puede tener un registro CNAME con el valor `infoblox.com`. En este caso, cuando un cliente consulte la dirección IP de `www.infoblox.com`, recibirá la dirección IP de `infoblox.com`. La presencia de un CNAME es en gran medida invisible para el usuario, ya que un servicio recursivo gestiona las resoluciones en su nombre.[2] Decimos que `www.infoblox.com` es un alias de `infoblox.com`.

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

La sucesión de eventos hasta la resolución, como se ilustra en la Figura 1, es más o menos como sigue:

- El cliente, un sistema de resolución, envía una consulta sobre `www.infoblox.com` a su servicio recursivo.
- El servicio recursivo consulta el DNS de la dirección IP (registro A) correspondiente a `www.infoblox.com` y en respuesta recibe un registro CNAME que contiene `infoblox.com`.
- El servicio recursivo consulta el DNS para obtener la dirección IP de `infoblox.com`.[3]
- El servicio recursivo envía la dirección IP al cliente junto con el registro CNAME.
- Por último, el servicio cliente (por ejemplo, el navegador) se conecta a la dirección IP proporcionada.

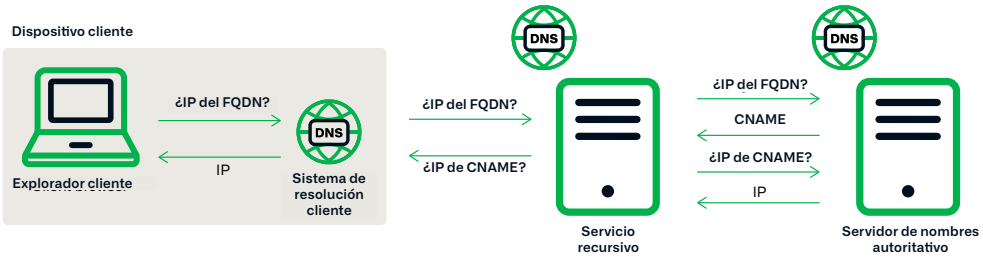


Figura 1: Vista simplificada de la resolución de direcciones IP cuando hay un registro CNAME del DNS para un nombre de dominio totalmente cualificado.

El registro de archivo de zona DNS en este caso podría incluir:

FQDN	Tipo de registro	Valor
`www.infoblox.com.`	CNAME	`infoblox.com`
`infoblox.com`	A	127.0.0.1

Se considera que la porción izquierda del registro es un **alias** del nombre de dominio canónico. De este modo, `www.infoblox[.]com` es un alias de `infoblox[.]com`. Las consultas del registro A tanto para `www[.]infoblox[.]com` como para `infoblox[.]com` devolverían 127.0.0.1. Un nombre de dominio canónico, es decir, el valor del registro CNAME, debe ser un FQDN.

Sistemas de distribución de tráfico CNAME

Aunque el ejemplo clásico de los registros CNAME es mapear el nombre de host `www` al dominio base, en la práctica se utilizan de muchas maneras. Los registros CNAME se usan en muchas redes de distribución de contenidos (CDN). En el ejemplo anterior, sugeríamos que `www[.]infoblox[.]com` podría ser un alias de `infoblox[.]com`, pero en la práctica no lo es. Infoblox, como la mayoría de las grandes empresas actuales, utiliza un proveedor de CDN comercial. En realidad , `www[.]infoblox[.]com` tiene un dominio CNAME en un proveedor de CDN. El objetivo principal de una CDN es proporcionar a los usuarios de todo el mundo un acceso rápido al contenido de un sitio web, independientemente de dónde se encuentren. Para lograrlo, los proveedores de CDN suelen utilizar entornos de alojamiento sofisticados que incluyen dispositivos de caché y proxies; sin embargo, todos estos mecanismos son independientes de las configuraciones de DNS.

Un **TDS** conecta las fuentes de tráfico de internet con los destinos. El término surgió del marketing en Internet, donde un TDS conecta a los visitantes de un sitio web con anuncios. Los hackers maliciosos han hecho suya esta técnica: han tomado el concepto de un TDS utilizado con fines legítimos de marketing y lo han modificado para emplearlo en operaciones

3 En ocasiones, la labor de resolver el valor CNAME recae en el sistema de resolución, pero la mayoría de los servicios recursivos completan automáticamente el proceso de resolución y envían una respuesta combinada.

de ciberdelincuencia. En Infoblox, hemos observado una serie de técnicas utilizadas para crear TDS, incluidos sistemas íntegramente basados en DNS, que toman decisiones en función de la dirección IP del solicitante como criterio único. En nuestras publicaciones anteriores sobre VexTrio[4] y Prolific Puma,[5] describimos varios ejemplos de TDS maliciosos. VexTrio opera tanto un TDS de DNS como un TDS basado en HTTP, mientras que Prolific Puma gestiona un servicio de acortamiento de enlaces. Si bien un TDS de marketing legítimo tiene como objetivo conducir a cualquier usuario hacia contenido publicitario relevante, un TDS malicioso también puede incorporar control del tráfico e impedir que ciertos usuarios visualicen el contenido verídico. Algunas campañas maliciosas encadenan varios TDS sucesivos.

Savvy Seahorse es el primer actor de amenazas del que se ha informado públicamente que abusa de los CNAME de DNS como parte de un TDS malicioso. Aunque requiere una mayor sofisticación en DNS por parte del actor de amenazas, no es infrecuente, si bien hasta la fecha no estaba reconocido en las publicaciones sobre seguridad. Utilizamos el término **TDS de CNAME** para describir la técnica de utilizar registros CNAME de DNS para crear un TDS. A primera vista, este uso de un TDS puede confundirse con una CDN; sin embargo, a diferencia de una CDN, un TDS no está diseñado para proporcionar acceso equitativo y de alto rendimiento al mismo contenido a todos los usuarios.

Usar registros CNAME de DNS para crear un TDS dedicado a actividades maliciosas posiblemente no sea un concepto nuevo para los actores de amenazas, pero al parecer sí lo es en el sector de la seguridad. Desde al menos 2021, Savvy Seahorse aplica esta técnica no divulgada anteriormente para construir infraestructuras y ejecutar campañas fraudulentas dirigidas a usuarios de Facebook/Meta que desean invertir. También llevamos un seguimiento de otros actores que utilizan variantes de la técnica de CNAME.

DE CNAME A SeaNAME

Savvy Seahorse se suma al mecanismo de sustitución de dominios de CNAME y crea subdominios específicos asociados con el dominio principal de la campaña. En particular, todos los dominios de campaña maliciosos son alias de un subdominio de:

`b36cname[.]site`

Por ejemplo, Savvy Seahorse usó anteriormente el dominio `mom[.]multi-info[.]site` en una campaña que suplantaba un programa de inversión de Mastercard. Este dominio tenía un registro CNAME con el valor `prx16[.]b36cname[.]site`. Al mismo tiempo, el actor utilizaba muchos otros subdominios de `multi-info[.]site` en sus campañas. Todos ellos compartían la misma dirección IP, porque Savvy Seahorse usa configuraciones de DNS con comodines. En la Figura 2 se muestra esta configuración.

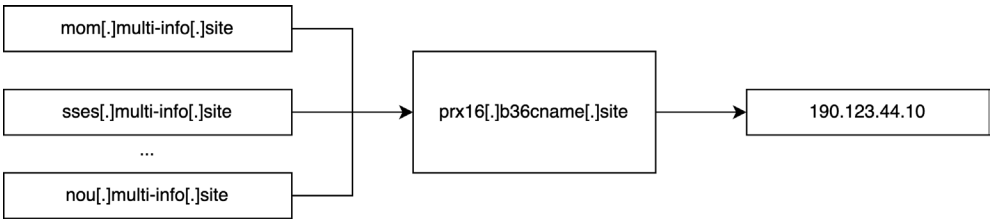


Figura 2: Savvy Seahorse utiliza muchos dominios de campaña a la vez, todos ellos subdominios de un mismo dominio base. Estos subdominios comparten un registro CNAME y, por lo tanto, una dirección IP.

Savvy Seahorse utiliza direcciones IP dedicadas para alojar contenido. El actor alterna periódicamente estas direcciones IP , facilitado por el uso de registros CNAME, que le ayudan a no ser detectado y a camuflarse en los entresijos del DNS.

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/

Los dominios de campaña de Savvy Seahorse no comparten un patrón fácil de distinguir y pueden variar considerablemente en cuanto a su infraestructura de alojamiento, que examinaremos en mayor detalle en secciones posteriores. Estas variaciones pueden dificultar que los investigadores de amenazas identifiquen la actividad como procedente de un mismo actor de amenazas del DNS. A fin de cuentas, la única información que nos permitió vincular los componentes de esta red fue el uso de un CNAME común.

OPERACIONES DE SAVVY SEAHORSE

Savvy Seahorse opera desde agosto de 2021, cuando se creó inicialmente el dominio `b36cname[.]site`. Aunque las herramientas de seguridad a veces señalan los dominios participantes, la infraestructura y el actor responsable han pasado desapercibidos para la industria de la seguridad. Hemos observado unos 4.200 dominios base con un registro CNAME que contiene un subdominio de `b36cname[.]site`. Para alojar campañas, Savvy Seahorse crea varios subdominios para cada SLD mediante un algoritmo de generación de dominios (DGA), en los que el nombre del host es pseudoaleatorio y, en la mayoría de los casos, contiene tres caracteres. Veremos con más detalles este patrón de nombres de host en la siguiente sección.

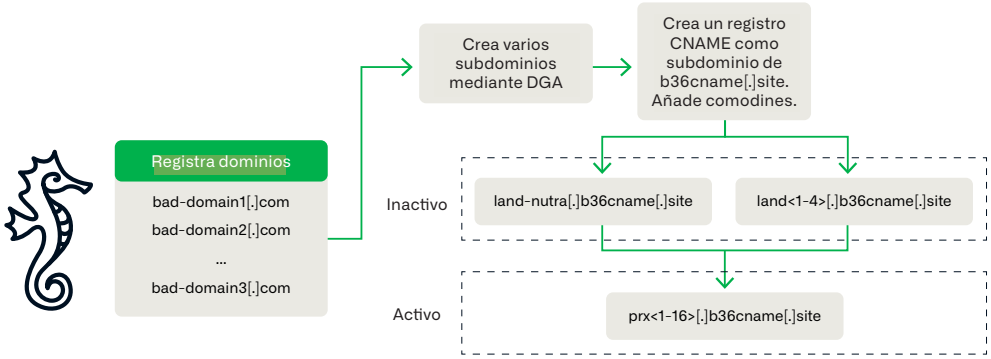


Figura 3: Visión general de las operaciones de Savvy Seahorse

Patrones y comodines de SeaNAME

Cada uno de los registros CNAME de Savvy Seahorse sigue uno de estos tres patrones, como muestra la Tabla 1.

Patrones de CNAME	Propósito
`land-nutra[.]b36cname[.]site`	Subdominio utilizado temporalmente como CNAME antes de que las campañas se activen, para dominios aparcados
`land<1-4>[.]b36cname[.]site`	Subdominios utilizados temporalmente como CNAME antes de que las campañas se activaran, posiblemente con fines de prueba
`prx<1-16>[.]b36cname[.]site`	Subdominios utilizados para campañas activas

Tabla 1: Patrones y propósitos de los registros CNAME

Los siguientes son comportamientos observados en Savvy Seahorse respecto al uso de cada tipo de CNAME:

Los dominios que tenían `land-nutra[.]b36cname[.]site` como registro CNAME estaban en parking en ese tiempo. Cuando se activaron las campañas, los actores cambiaron el registro CNAME a `prx<1-16>[.]b36cname[.]site`.

Del mismo modo, los dominios que en algún momento tuvieron land<1-4>[.]b36cname[.]site como registro CNAME se utilizaron en campañas que estaban inactivas. Estos dominios también cambiaron al registro prx<1-16>[.]b36cname[.]site cuando se activaron las campañas.

Los CNAME land<1-4> podrían usarse para probar algunas campañas antes de activarlas.[6]

Savvy Seahorse ha configurado respuestas de CNAME con comodines para gestionar fácilmente su uso del DNS. En este caso, una consulta a cualquier subdominio (p. ej., comodin[.]xsdelx[.]top) del dominio base arrojará una respuesta que mostrará que comparten el mismo registro de recursos. En la Figura 4, vemos el resultado de enviar un comando "dig" para consultar comodin[.]xsdelx[.]top del dominio base xsdelx[.]top de Savvy Seahorse. La respuesta muestra que, como resultado del comodín, la consulta devolvió el registro CNAME prx2[.]b36cname[.]site. El comodín permite al actor configurar automáticamente los registros para todo nuevo subdominio que cree, lo que permite gestionar con mayor eficacia una infraestructura extensa.

```
; <<>> 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/UYfBWG38E5mslTS/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

xdelx.top.              3600    IN      NS      ns1.dns.com.
xdelx.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
```

Figura 4: Comportamiento de la respuesta con comodines a un subdominio aleatorio de un dominio base existente de Savvy Seahorse. Los servidores responden al subdominio para indicar que su valor de registro CNAME es prx2[.]b36cname[.]site*, el dominio CNAME del actor.*

Dominios

Los actores de amenazas a menudo usan DGA como herramientas para generar grandes cifras de nombres de dominio pseudoaleatorios, que pueden usar para ejecutar campañas y realizar otras actividades maliciosas. Los dominios utilizados en estos DGA suelen seguir patrones visibles similares, que los algoritmos al efecto pueden detectar fácilmente y, por lo tanto, facilitan que se les asocie con un actor de amenazas. Si bien Savvy Seahorse parece usar DGA para crear muchos de sus subdominios y SLD, dichos DGA no parecen seguir un patrón distintivo. Más bien, hemos observado que el actor utiliza diversos patrones de DGA para los SLD, como indica la Tabla 2.

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

Descripción del patrón	Variaciones de la misma palabra clave completa	Palabra clave completa anexada, con caracteres aleatorios de una misma longitud	Variaciones ortográficas en la segunda mitad de una palabra clave	Variaciones de una palabra clave en todo el dominio
Dominios de ejemplo	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

Tabla 2: Patrones de SLD de Savvy Seahorse y dominios de ejemplo

Una técnica común para identificar estos tipos de DGA es utilizar algoritmos de aprendizaje automático. Se podrían utilizar N-gramas[7] para detectar correctamente algunos de los clústeres incluidos en cada una de las columnas de la Tabla 2, pero ese método no detectaría que todos estos clústeres pertenecen a un mismo actor de amenazas del DNS si se limitara a analizar las características de los nombres de dominio. Los cuatro clústeres anteriores tienen patrones muy diferenciados —al igual que otros de los clústeres de dominio que crea Savvy Seahorse— que un modelo basado en N-gramas no podría identificar como parte de un mismo grupo.

Los ejemplos anteriores también muestran que los actores no se limitan a un solo dominio de nivel superior (TLD), ni siquiera con patrones de DGA diferenciados. Savvy Seahorse utiliza varios TLD, a menudo los más abusados. Los cinco primeros por número de dominios son site, `xyz`, `com`, `top` y `life`.

7 https://es.wikipedia.org/wiki/N-grama

TLD	site	xyz	com	top	life
Dominios	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

Tabla 3: Ejemplos de dominios para los TLD más utilizados en campañas maliciosas de Savvy Seahorse

Anteriormente, mencionamos que los nombres de host parecían ser pseudoaleatorios y tenían tres caracteres en la mayoría de los casos, pero hemos visto algunos ejemplos con denominaciones más largas (ver Tabla 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

Tabla 4: Ejemplos de patrones de subdominios

Información de registro de dominios

Savvy Seahorse no sigue un enfoque convencional a la hora de manejar los registros, lo que le ayuda a no ser detectado. Una técnica común que utilizan los actores de amenazas del DNS es registrar dominios en lotes a través de un mismo registrador, así como utilizar el mismo proveedor de servicios de internet (ISP) para alojarlos a fin de gestionar su infraestructura de forma más fácil y rápida. Muchos registradores ofrecen distintas API para facilitar el registro de dominios en lotes. Si bien la mayoría de los registradores proporcionan las API para que se usen con fines legítimos, es sabido que los ciberdelincuentes abusan de esta función con el fin de crear más fácilmente miles de dominios que usar en sus campañas. En nuestro artículo sobre RDGA de octubre de 2023 en el blog se describe el proceso con más detalle.[8]

Cuando los actores recurren al mismo registrador y la misma infraestructura para crear y alojar sus dominios, a menudo resulta sencillo hallar dominios pertenecientes a un mismo actor a través de los metadatos de registro comunes. Savvy Seahorse parece ser paciente y disponer de una infraestructura repartida entre varios registradores y proveedores de alojamiento diferentes. Hemos observado 30 entidades registradoras distintas y 21 ISP para todos los dominios que tienen un subdominio de `b36cname[.]site` como registro CNAME. Esta técnica dificulta a los investigadores de seguridad relacionar los dominios y acotar la infraestructura de un actor.

Las variaciones en los metadatos de registro de los dominios con `b36cname` como CNAME nos hicieron sospechar en un principio que este actor podía ser un proveedor de servicios para otros ciberdelincuentes que ejecutaban campañas de estafas. Sin embargo, nuestro análisis mostró que las campañas de estafas financieras ejecutadas a través de su red compartían unos mismos elementos y un comportamiento general idéntico, lo que nos llevó a concluir que lo más probable es que las campañas estén bajo el control de un único actor: Savvy Seahorse. Hablamos de estas campañas y de su contenido con más detalle en la sección Análisis de las campañas.

Direcciones IP

Savvy Seahorse parece usar aproximadamente 50 direcciones IP dedicadas, que cambia periódicamente, como se muestra en la Figura 5. Los espacios finos en blanco en cada barra temporal representan momentos en que Savvy Seahorse cambió la IP asociada a un registro CNAME.

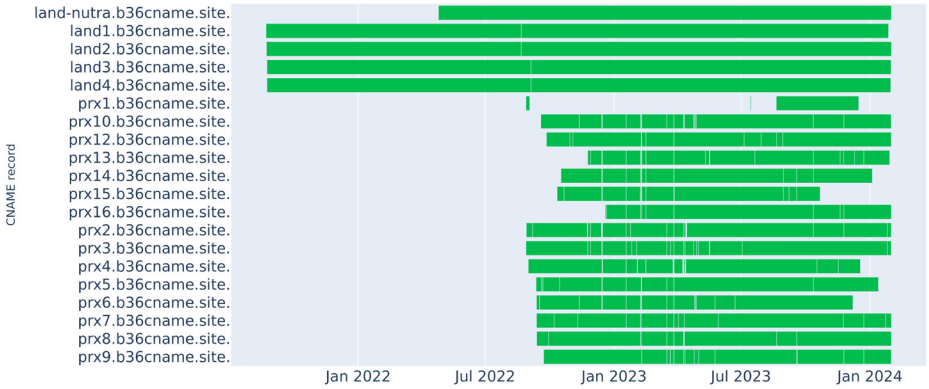


Figura 5: Cronología de los cambios de direcciones IP, por CNAME. Cada barra muestra el tiempo que pasa cada registro CNAME en una dirección IP específica, y los espacios finos indican cuándo cambiaron estos valores. Los actores rotan a menudo las direcciones IP para evitar ser detectados.

Según el análisis de cambios en las IP, observamos lo siguiente:

- `land-nutra[.]b36cname[.]site` es el único CNAME con una sola dirección IP, lo que concuerda con el comportamiento que hemos visto que indica que los dominios asociados con este CNAME están en parking. Esta dirección IP tiene un número total de dominios asociados considerablemente alto, característica que concuerda con las direcciones IP utilizadas para parking.

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

- Los cuatro CNAME que utilizan el patrón `land<1-4>[.]b36cname[.]site` han cambiado de dirección IP una sola vez.
- Los CNAME de `prx<1-16>[.]b36cname[.]site` cambian con frecuencia de dirección IP. Este patrón indica que lo más probable es que estas IP se utilicen exclusivamente para campañas de estafas activas, puesto que los cambios periódicos de IP son una táctica que emplean los actores de amenazas para evitar que los servicios de seguridad los detecten y bloqueen.
- En algunos casos, el actor de amenazas cambia las IP de varios CNAME al mismo tiempo con el mismo valor.
- Parece que el actor de amenazas no utiliza actualmente algunos CNAME, incluidos `prx6[.]b36cname[.]site` y `prx15[.]b36cname[.]site`.

ANÁLISIS DE LAS CAMPAÑAS

Savvy Seahorse utiliza una infraestructura singular para llevar a cabo una serie de campañas de estafas diferentes sobre temas financieros y de inversión. Las campañas incluyen diversas técnicas de señuelo avanzadas, pero todas siguen un patrón similar con el objetivo final de robar la información personal y financiera de la víctima para obtener una ganancia monetaria. Los idiomas utilizados en estas campañas incluyen inglés, ruso, polaco, italiano, alemán, francés, español, checo y turco.

- Las campañas activas operan en el nivel de los subdominios, donde cada subdominio cuenta con un registro CNAME de `prx<1-16>[.]b36cname[.]site`.

Detalles de las campañas

Savvy Seahorse utiliza formularios de registro incrustados en páginas web para recopilar el nombre y los apellidos, la dirección de correo electrónico y el número de teléfono de la víctima. En la Figura 6 aparecen dos ejemplos de este formulario de registro, uno en polaco y otro en inglés.

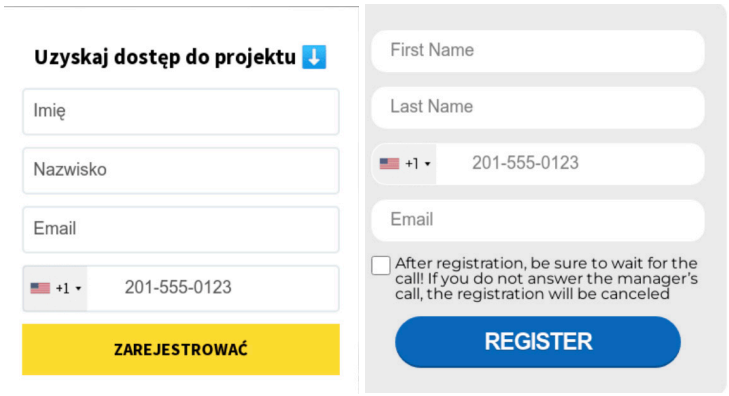


Figura 6: Formularios de registro utilizados en las campañas de Savvy Seahorse

Validación y redirección

Una vez que el usuario introduce sus datos en uno de estos formularios, el dominio contacta con el dominio de TDS secundario que utiliza Savvy Seahorse para sus campañas, `getyourapi[.]site`, para validar la información, incluidas la dirección IP del usuario, la geolocalización y la validez del número de teléfono y el correo electrónico facilitados. En función de las comprobaciones superadas, hemos observado tres situaciones diferentes:

1. Si los datos del formulario son válidos, pero el usuario ya se había registrado previamente con el mismo correo electrónico/número de teléfono, la web indica que el usuario ya está registrado.
2. Si los datos del formulario son válidos, pero el usuario ya ha visitado previamente este dominio a través de la misma dirección IP, la página muestra un mensaje de confirmación del registro e indica al usuario que un representante le llamará para darle información adicional. No se produce ninguna redirección.
3. Si los datos del formulario son válidos y el usuario visita el dominio desde una dirección IP desconocida, se le redirige a una página web de trading falsa, similar a la de la Figura 7.

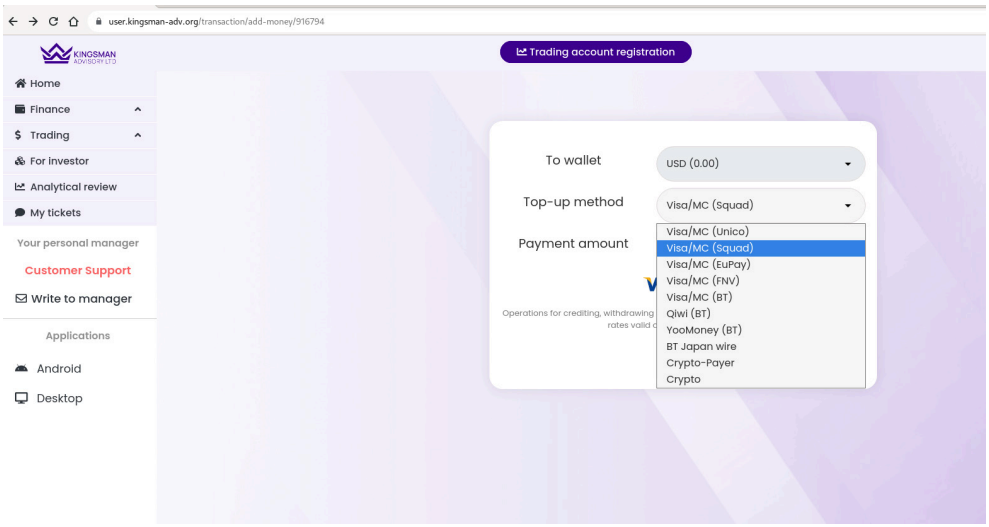


Figura 7: Una plataforma de trading falsa de Savvy Seahorse

Un dato importante que hay que tener en cuenta es que el actor valida la información del usuario para excluir el tráfico de una lista predefinida de países, que incluye Ucrania, India, Fiji, Tonga, Zambia, Afganistán y Moldavia, aunque el razonamiento que le lleva a elegir estos países específicos no está claro. La primera validación verifica el número de teléfono introducido en el formulario de registro; si corresponde a alguno de los países de la lista bloqueada, la web mostrará un mensaje que indica: **"El programa no está disponible en su región".** Si el usuario introduce un número de teléfono aceptable junto con información válida en los demás campos, como hemos mencionado antes, el actor enviará la información a su dominio del TDS secundario para contrastar la geolocalización de la dirección IP del usuario con los países excluidos y determinar si se produce la redirección o no.

Plataforma de trading

Al redirigir al usuario, la plataforma de trading falsa le ofrecerá automáticamente una cuenta creada para él con los datos del formulario de registro. Esta plataforma parece ser muy sofisticada y ofrece la opción de descargar una aplicación de escritorio, así como enlaces a una aplicación de Android en Google Play Store llamada App4World.

A continuación, se anima al usuario a ingresar dinero a su "cartera" a través de varias fuentes, como Visa/Mastercard, una cartera de criptomonedas o proveedores de pagos rusos como Qiwi y YooMoney. Se requiere un importe mínimo de "prepago" de 50 USD para añadir dinero a una cartera. La redirección final a uno de los ocho posibles dominios de procesamiento de pagos (ver Tabla 5) se produce una vez que el usuario especifica una fuente de pago y el importe del depósito. El dominio que utilice la campaña para recopilar información financiera de la víctima dependerá del origen de los fondos.

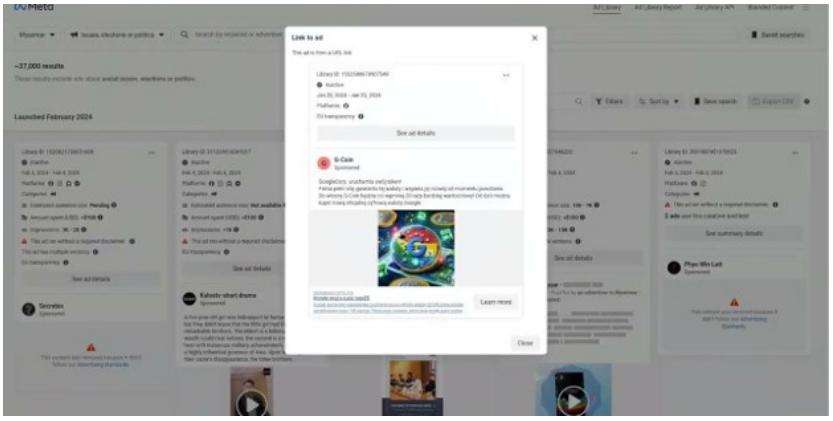
Origen del pago	Dominio de pago	Descripción del dominio de pago
Visa/MC (Unico)	makeyourpay[.]com	Dominio recién registrado que aloja una web de procesamiento de pagos; subdominios en ruso
Visa/MC (Squad)	checkout[.]flutterwave[.]com	Alberga una empresa de infraestructura financiera legítima con sede en Nigeria
Visa/MC (EuPay)	ap-gateway[.]mastercard[.]com	Pasarela de pago legítima para Mastercard
Visa/MC (BT)	sci[.]pointpayment[.]net	Alojado en la misma IP dedicada que varios otros dominios de pago sospechosos
Qiwi (BT)	qiwi[.]bppsa[.]com	El dominio base aloja una página web de procesamiento de pagos en ruso
YooMoney (BT)	ymoney[.]bppsa[.]com	El dominio base aloja una página web de procesamiento de pagos en ruso
BT Japan (transferencia)	processing[.]betatransfer[.]io	API para Betatransfer Kassa, servicio de procesamiento de pagos de alto riesgo (utilizado principalmente para juegos de azar en internet)
Crypto-Payer Crypto	crypto-payer[.]co	Registrado en diciembre de 2023

Tabla 5: Dominios de procesamiento de pagos para recopilar información financiera de la víctima

La investigación indica que el actor parece remitir fondos a SberBank, un banco de propiedad estatal mayoritariamente rusa, al menos desde uno de los dominios de procesamiento de pagos (sci[.]pointpayment[.]net), como muestra la Figura 8.

Figura 8: Datos financieros de sci[.]pointpayment[.]net

El siguiente vídeo ofrece un recorrido por la plataforma de trading falsa.



Ver vídeo del Tutorial sobre campañas de Savvy Seahorse.

Píxel de Meta

Dado que Savvy Seahorse comercializa y distribuye estas campañas a través de anuncios de Facebook/Meta (ver Figura 9), todos los dominios utilizados en campañas activas efectúan múltiples conexiones con `connect[.]facebook[.]net` y `www[.]facebook[.]com`. El actor también utiliza el píxel de Meta, una herramienta legítima, para monitorizar y optimizar el rendimiento de los anuncios.[9]

El píxel de Meta es un fragmento de código JavaScript que consta de dos partes:

- un "script", que se ejecuta al cargar la página, inicializa el píxel de Meta y registra un evento "PageView".
- un "noscript" que se ejecuta si el usuario tiene JavaScript desactivado en su navegador. Esta sección mostrará una imagen de 1x1 píxeles para registrar el evento.

Cada píxel de Meta cuenta con un número de identificación único, que podemos ver en las conexiones HTTP a Facebook. Hemos observado algunas campañas alojadas en el mismo SLD con diferentes subdominios, pero que comparten un mismo ID; otras parecen ser aleatorias.

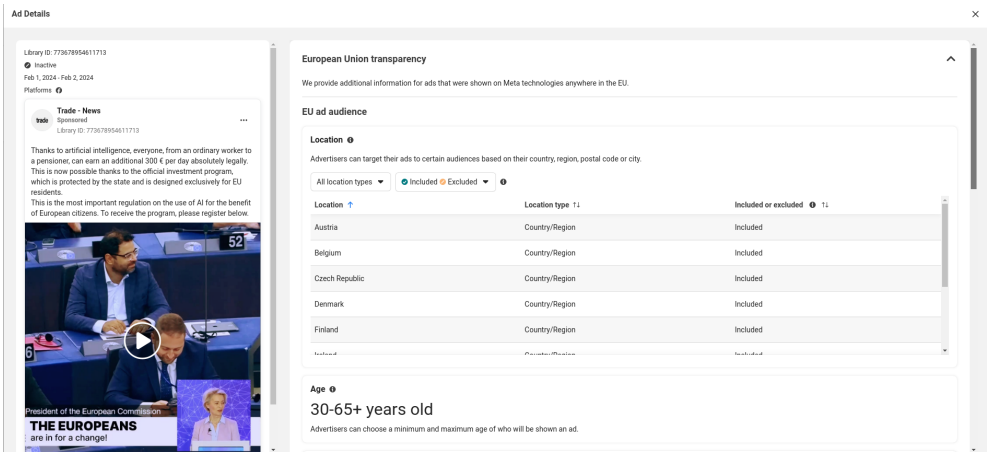


Figura 9: Detalles de un anuncio de Facebook para una campaña de Savvy Seahorse, que muestra los países objetivo y el grupo demográfico de edad

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

Temas

Los temas específicos de las campañas de Savvy Seahorse pueden variar ampliamente, incluidos señuelos que se hacen pasar por empresas legítimas como Apple con oportunidades de inversión y la incorporación de bots que suplantan a WhatsApp, ChatGPT y Tesla.

Proyectos de ganancias que suplantan empresas

Uno de los temas más recurrentes de Savvy Seahorse a lo largo de su trayectoria tiene que ver con "proyectos de ganancias" o programas de inversión, que afirman que el usuario tiene la oportunidad de ganar una cantidad específica de dinero si se registra con su información personal. Los actores de amenazas a menudo emplean una popular técnica de campañas de phishing en la que se hacen pasar por marcas y empresas fácilmente reconocibles para generar confianza en el usuario. La Tabla 6 contiene algunos de los ejemplos que hemos visto.

Subdominio de campaña	CNAME asociado	Descripción de la campaña
new[.]xsdelx[.]top	prx2[.]b36cname[.]site	Campaña en ruso que suplanta a Tesla y a X, y anima a los usuarios a "unirse al proyecto de Elon Musk" para ganar 12.000 € al mes
bwn[.]objectop[.]xyz	prx7[.]b36cname[.]site	Campaña en inglés que suplanta a Imperial Oil, compañía petrolera canadiense legítima. La página de destino muestra una "encuesta" interactiva y anima a los usuarios a invertir entre 250 y 1.000 USD
sej[.]progmedisd[.]site	prx9[.]b36cname[.]site	Campaña de febrero de 2023 en polaco para el "proyecto de ganancias automáticas de Libra", que afirma estar creado por Mark Zuckerberg y promete a los usuarios ganancias de hasta 300.000 złoty polacos (PLN)

Tabla 6: Ejemplos de campañas financieras de Savvy Seahorse

Las Figuras 10 y 11 muestran capturas de pantalla de algunas de las campañas de la Tabla 6. Otros ejemplos de empresas suplantadas por Savvy Seahorse son Apple, Meta, Mastercard, Visa y Google, entre otras.

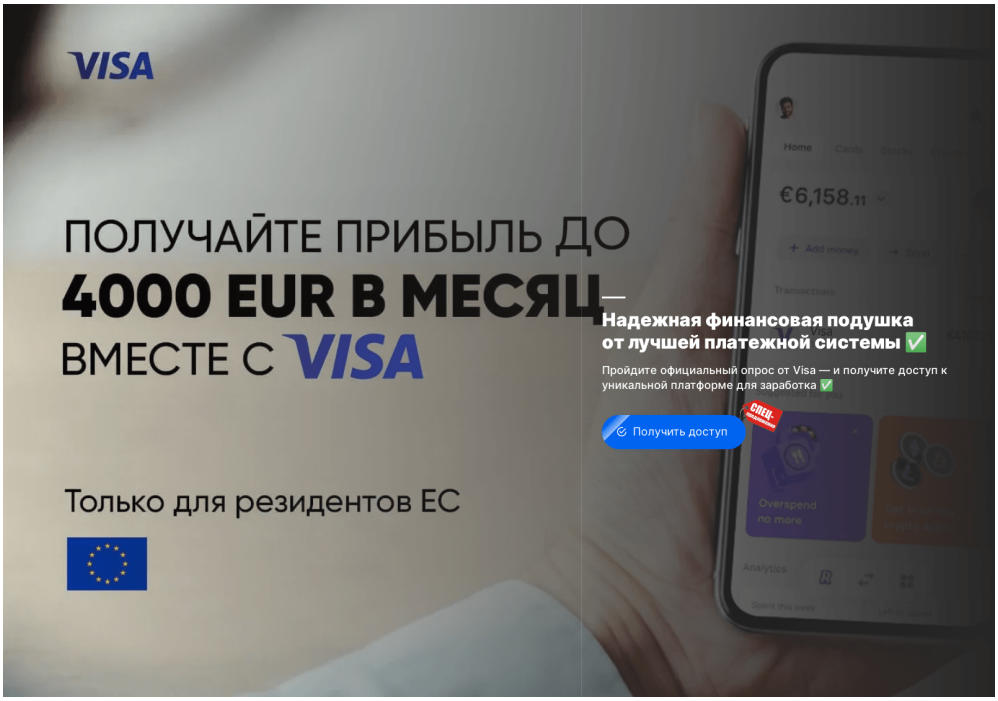


Figura 10: Página de destino de `visa[.]lukzev[.]xyz`*, campaña en ruso que suplanta a Visa*

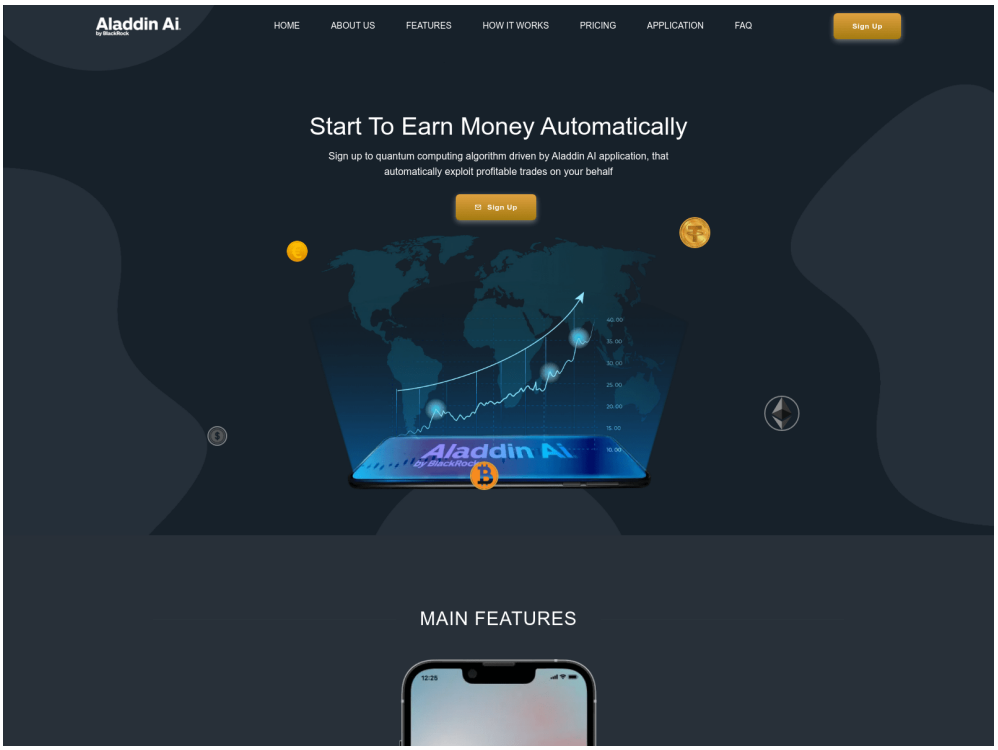


Figura 11: Página de inicio de `adin[.]czproftes[.]xyz` *que suplanta a la plataforma de gestión de carteras de BlackRock*

Bots falsos

Hemos visto algunas campañas con técnicas avanzadas de señuelo con chatbots que suplantan a ChatGPT, WhatsApp y Tesla, entre otros. Recientemente, las estafas con este tipo de bots se han convertido en una tendencia habitual entre los actores de amenazas que tratan de ganarse la confianza de los usuarios para robarles información personal.[10] La captura de pantalla de la Figura 12 muestra nuestras interacciones con uno de estos chatbots en una campaña que suplantaba a Tesla.

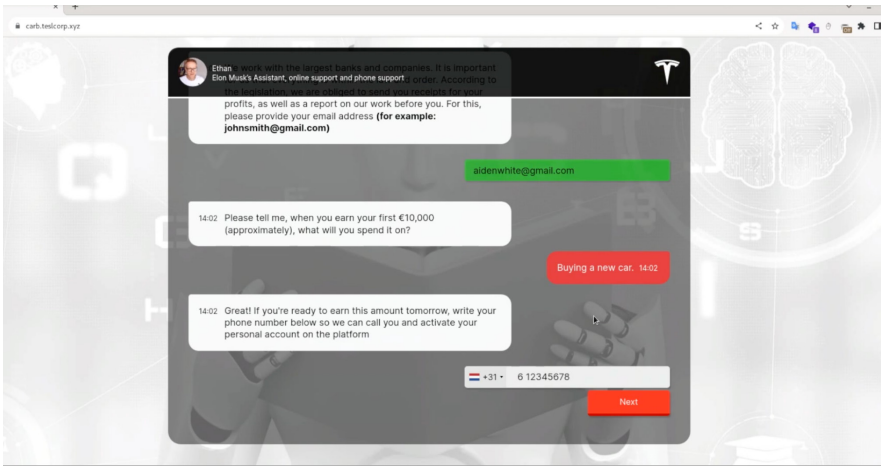


Figura 12: Bot falso con temática de Tesla utilizado en una campaña de Savvy Seahorse

Los bots harán preguntas al usuario sobre su interés en posibles oportunidades de ganancias e inversión, pero en última instancia seguirán el mismo patrón que otras campañas, lo que hace que el usuario se registre con su información personal para luego redirigirlo a la plataforma de trading falsa.

CONCLUSIÓN

En Infoblox, nos centramos en encontrar nuevas formas utilizadas por los actores de amenazas para abusar del DNS y ocultar operaciones delictivas. La técnica de Savvy Seahorse de utilizar los CNAME del DNS como TDS para gestionar operaciones maliciosas demuestra que el DNS es la forma más eficaz de rastrear y detener las actividades de los ciberdelincuentes. Nuestro análisis de los patrones de CNAME fue, en última instancia, lo que nos permitió descubrir a este actor y las tácticas, técnicas y procedimientos (TTP) únicos que utiliza para operar su extensa red de campañas de estafas.

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

INDICADORES DE ACTIVIDAD

A continuación figura una muestra de los indicadores utilizados en las campañas de Savvy Seahorse. Puede verse una lista más completa de indicadores en nuestro repositorio de GitHub aquí.

Indicador	Tipo de indicador
getyourapi[.]site	Dominio TDS secundario de Savvy Seahorse
land-nutra[.]b36cname[.]site	Subdominio utilizado como registro CNAME para dominios en parking
land<1-4>[.]b36cname[.]site	Subdominios utilizados como registros CNAME para campañas inactivas
prx<1-16>[.]b36cname[.]site	Subdominios utilizados como registros CNAME para campañas activas
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	Subdominios para campañas activas de Savvy Seahorse
ultra-vest[.]one kingsman-adv[.]org abyss-world-asset[.]net	Sitios web de trading falsos a los que se redirige a los usuarios en algunas campañas
sci[.]pointpayment[.]net makeyourpay[.]com qiwi[.]bppsa[.]com ymoney[.]bppsa[.]com processing[.]betatransfer[.]io crypto-payer[.]co	Dominios de procesamiento de pagos para recopilar información financiera de la víctima

Indicador	Tipo de indicador
ap-gateway[.]mastercard[.]com	Dominio legítimo de Mastercard, utilizado para recopilar información financiera de la víctima
checkout[.]flutterwave[.]com	Dominio legítimo de Flutterwave, servicio de pago nigeriano, utilizado para recopilar información financiera de la víctima
auproject[.]xyz badanie-pl[.]site blog-vcnews[.]site capital-inwest[.]site dasms[.]xyz duums[.]xyz esbopehan[.]xyz	Dominios base de Savvy Seahorse

THREAT INTEL DE INFOBLOX

Threat Intel de Infoblox es la principal iniciativa de inteligencia sobre amenazas del DNS, cuya originalidad la distingue entre un mar de agregadores. ¿Qué nos diferencia? Dos cosas: increíbles habilidades en DNS y una visibilidad incomparable. El DNS es muy difícil de interpretar y detectar, pero nuestros profundos conocimientos y nuestro acceso exclusivo nos proporcionan una potente herramienta para detectar las ciberamenazas. Somos proactivos más que defensivos y utilizamos nuestros conocimientos para erradicar la ciberdelincuencia de raíz. Además, creemos en la puesta en común de los conocimientos para ayudar a la comunidad de seguridad en general, por lo que damos a conocer investigaciones detalladas y publicamos indicadores en GitHub. Por otra parte, nuestra información se integra a la perfección en las soluciones de detección y respuesta del DNS de Infoblox, por lo que nuestros clientes se benefician de ella automáticamente, además de contar con tasas de falsos positivos despreciables.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com

Versión: 20240216v1