infoblox

Threat Intel

LOS DEPREDADORES DEL DNS ATACAN: LOS VIPERS Y LOS HAWKS TOMAN EL CONTROL DE LOS DOMINIOS VULNERABLES

Autores:
Infoblox Threat Intel

TABLA DE CONTENIDO

INTRODUCCIÓN

Todo comenzó con un dominio similar. El dominio se eligió por su semejanza a un recurso de hosting de Slack, pero estaba alojado en Rusia. ¿Un simple phishing? Tal vez. Excepto que también había una curiosa cadena de redireccionamiento. Se estaba utilizando un dominio de CBS Interactive registrado desde hace mucho tiempo para redirigir a las posibles víctimas a un portal falso de Slack.[1] ¿Realmente podría la cadena de televisión haber dejado el dominio? No, seguía registrada en Mark Monitor. Sin embargo, al revisar el historial de resoluciones del DNS, quedó claro que, tras permanecer inactivo durante un tiempo, el dominio empezó a resolverse en Rusia. Es muy probable que hayan tomado el control. En enero de 2024, secuestrar un dominio de alto valor como `clickermediacorp[.]com` se consideraba una señal de robo de credenciales. Informamos del secuestro tanto al registrador como al proveedor de DNS y seguimos adelante.

Unos meses más tarde, volvió a surgir el tema del secuestro misterioso de dominios. Los investigadores de Proofpoint estaban rastreando un sistema de distribución de tráfico criminal (TDS) llamado 404TDS, que estaba relacionado con la distribución de malware y otro contenido malicioso. Nos especializamos en la detección de amenazas DNS, y mientras otros ven malware para realizar ingeniería inversa o páginas web que analizar, nosotros identificamos huellas de los actores en la configuración de los registros de DNS y en el rastro de consultas que dejan tras sus operaciones. Nos encantan los actores de TDS porque un TDS está intrínsecamente integrado en las configuraciones de DNS y, a menudo, somos capaces de ver patrones que nos permiten supervisar el TDS a medida que evoluciona, en lugar de esperar a que lleguen cargas maliciosas. Pensamos que debía haber una firma DNS para 404TDS.

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

Cuando empezamos a buscar un mecanismo para rastrear el 404TDS, enseguida nos dimos cuenta de que todos los dominios habían sido secuestrados, incluido `clickermediacorp[.]com`. Pero el alcance de estos secuestros era inusualmente amplio, y la explicación del robo de credenciales o hackeos de registradores no tenía sentido. Nos asociamos con un investigador de Eclypsium y comenzamos a tratar de encontrar una explicación para el secuestro generalizado de dominios relacionado con el 404TDS.

Descubrimos que los servidores de nombres DNS mal configurados eran el factor común en todos los secuestros y que podíamos tomar control de dominios mal configurados en ciertos proveedores con solo unos clics. A pesar de ser expertos en amenazas de DNS, esto era nuevo para nosotros. Y no solo para nosotros: antes de publicar en julio de 2024, hablamos con un amplio grupo de personas en los sectores gubernamental e industrial, en investigación de amenazas y redes. Ninguno de los contactos con los que hablamos durante los primeros meses estaba al tanto del vector de ataque y, mucho menos, de su explotación masiva. Brian Krebs recordó haber informado sobre una amplia campaña que empleaba esta técnica, aunque en ese momento parecía un problema de un único registrador y no un fallo sistémico.[2] Por fin descubrimos el informe original de Matt Bryant sobre la vulnerabilidad, que nosotros bautizamos como "Sitting Ducks", y nos dimos cuenta de que probablemente los actores habían utilizado este vector de ataque durante al menos ocho años sin ser detectados.[3]

Nuestro primer informe sobre Sitting Ducks tenía como objetivo generar conciencia sobre una técnica de secuestro poco conocida y proporcionar acciones concretas para que los propietarios y solicitantes de registro de dominios protegieran sus dominios. Esperábamos que generara reacciones, y no solo por parte de los delincuentes. En nuestra investigación, descubrimos que estos dominios vulnerables son a menudo el resultado de fusiones, adquisiciones y la pérdida de historial debido a cambios de personal. Mientras que el dominio `clickermediacorp[.]com` fue asegurado tras nuestro informe de julio, desafortunadamente, otros dominios de CBS siguen siendo vulnerables. *Si está leyendo esto, y necesitas ayuda, no dude en contactarnos.* Trabajamos con una organización afectada para solucionar los problemas con sus dominios, debido a que habían perdido tanto el conocimiento de los dominios como las credenciales del registrador. En el caso más grave, colaboramos con los propietarios de dominios .gov para corregir sus configuraciones.

Desde nuestra publicación inicial, hemos identificado casi 800 mil dominios registrados vulnerables. Aproximadamente el nueve por ciento (70 mil) de esos dominios vulnerables fueron posteriormente secuestrados. Sabemos que estas cifras no reflejan con precisión la superficie de ataque, ya que son el resultado de un sistema de monitoreo limitado. El desafío de un ataque Sitting Ducks radica en que es fácil de ejecutar y muy difícil de detectar. Desde al menos 2018, los ciberdelincuentes han utilizado este vector para secuestrar más de 80 mil nombres de dominio, incluidos aquellos pertenecientes a marcas reconocidas, organizaciones sin fines de lucro y entidades gubernamentales.

Sitting Ducks no es el único vector de ataque relacionado con configuraciones que hemos visto este año; también hubo múltiples tipos de secuestros de CNAME e incluso un caso de toma de control de un servidor WHOIS.[4,5] A nivel general, los gobiernos y los organismos de normalización también tienen un papel que desempeñar en la protección de los usuarios contra este tipo de ataques. Las organizaciones nacionales y multinacionales deberían crear conciencia e incentivar la reducción de riesgos para todos los problemas relacionados con configuraciones, incluidos los requisitos de seguridad que incorporan medidas de protección contra ataques como el secuestro de DNS. Desafortunadamente, muchas organizaciones gubernamentales, incluida la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), se centran en las vulnerabilidades de software y, como resultado, las vulnerabilidades de configuración no califican para la designación de UN CVE, a pesar de su potencial impacto criminal. Por ejemplo, incluso los solicitantes de registro de un dominio .gov sólo están obligados a utilizar un proveedor de DNS "competente". Hemos encontrado que la consecuencia de esto es que ciertos registradores crean una delegación

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

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

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

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

lame para los nuevos registros de dominios, obligando a que se configure una configuración de servidor de nombres antes de que se establezcan los registros del proveedor de DNS. Es una carrera contra el reloj, pero la hemos observado una y otra vez. El no prestar atención a estos problemas permite que su explotación siga ocurriendo casi sin control. Esperamos que comience a haber tanto formación en sensibilización como medidas proactivas para abordar no solo el vector de ataque Sitting Ducks, sino también toda la clase de vulnerabilidades de configuración.

Una reacción muy común es culpar al titular del dominio por la responsabilidad de mantener sus configuraciones. Esto puede ser cierto, pero al mismo tiempo, tanto los registradores como los proveedores de DNS pueden desempeñar un papel crítico para reducir la ciberdelincuencia al hacer que estos tipos de secuestros sean más difíciles de realizar o más fáciles de remediar. Durante nuestra investigación, informamos sobre los secuestros de Sitting Ducks tanto a registradores como a proveedores de DNS, pero en gran medida lo desestimaron y no se tomaron medidas, a pesar de que proporcionamos evidencia de los ataques. En muchos casos, no pudimos informar a los titulares de dominios porque habían utilizado información de registro privada. En varios casos, cuando interactuamos con titulares de dominios comprometidos, no sabían que eran propietarios de los dominios, la memoria y la documentación perdida con el tiempo y las fusiones corporativas. La incapacidad de llegar a los titulares de dominios implica que, siendo realistas, para reducir la delincuencia, tanto los registradores como los proveedores de DNS deben asumir un papel más activo al responder a la información de las organizaciones de inteligencia de amenazas y minimizar el abuso de sus plataformas y usuarios.

Durante nuestra investigación del vector de ataque, descubrimos más de una docena de actores independientes que lo estaban explotando. En este documento analizamos varios de ellos, incluido el operador de 404 TDS y VexTrio Viper. También presentamos a dos nuevos actores que rastreamos: Horrid Hawk y Hasty Hawk.

El objetivo de este artículo es demostrar formas específicas en que se utilizan estos dominios secuestrados para que puedan identificarse y cerrarse más fácilmente. Compartiremos:

- Cómo evitar un ataque de Sitting Ducks e identificar un dominio comprometido
- Cómo varios actores de amenazas aprovechan los ataques de Sitting Ducks para crear una infraestructura resistente a la detección de proveedores de seguridad
- Cómo algunos actores de amenazas de Sitting Ducks se afilian entre sí, lo que indica algún tipo de intercambio de información o economía subterránea para los dominios secuestrados
- Cómo algunos dominios vinculados a las principales marcas son secuestrados constantemente, a menudo por diferentes actores de amenazas,
- Y cómo el DNS es fundamental para la detección y el seguimiento de estos actores de amenazas persistentes.

EL VECTOR DE ATAQUE SITTING DUCKS

Primero, hagamos un repaso. En julio, publicamos conjuntamente con Eclypsium un informe sobre un vector de ataque ampliamente explotado e infravalorado al que llamamos Sitting Ducks.[6] Con este ataque, el actor malicioso obtiene el control total del dominio al tomar el control de sus configuraciones de DNS. También puede secuestrar el dominio sin necesidad de robar credenciales ni acceder a la cuenta del registrador del propietario del dominio, lo que lo hace especialmente sigiloso. En la mayoría de los casos, estos dominios, o subdominios, han sido olvidados por su propietario original, por lo que el ataque pasa desapercibido. Hemos visto a más de una docena de actores de amenazas que abusan de estos dominios secuestrados para llevar a cabo una variedad de actividades delictivas, como distribución de malware, comando y control (C2), phishing, operaciones del sistema de distribución de tráfico (TDS) y más.

Un ataque Sitting Ducks se aprovecha de una mala configuración en los ajustes DNS de un dominio, concretamente cuando el DNS apunta al servidor de nombres autoritativo equivocado. Existen algunas condiciones que deben cumplirse para que un atacante pueda secuestrar un dominio de esta manera:

Un dominio registrado o el subdominio de un dominio registrado que utiliza o delega los servicios DNS autoritativos en un proveedor diferente al del registrador del dominio; esto se denomina **delegación**.

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

- La delegación es **lame**, lo que significa que los servidores de nombres autorizados del registro no tienen información sobre el dominio y, por lo tanto, no pueden resolver las consultas.
- El proveedor de DNS autorizado es **explotable**, lo que significa que el atacante puede "reclamar" el dominio en el proveedor y configurar los registros de DNS sin acceder a la cuenta válida del propietario en el registrador de dominios.

La Figura 1 muestra una secuencia de ataque Sitting Ducks común. Existen numerosas variantes de este tipo de ataque, ninguna de las cuales requiere comprometer la infraestructura de DNS legítima, lo que lo hace totalmente diferente de las técnicas de secuestro de DNS más conocidas. "Las variaciones dentro de este ataque incluyen la redelegación a otro proveedor de DNS y la delegación lame parcial, lo que significa que solo algunos de los servidores de nombres autoritativos están mal configurados. La baja barrera técnica de entrada ofrece a muchos grupos cibernéticos la oportunidad de aprovechar la vulnerabilidad. Esto da como resultado más casos de ataque que son difíciles de detectar debido a la buena reputación que muchos de estos dominios secuestrados tienen.

Si bien los ataques Sitting Ducks son fáciles de realizar y difíciles de detectar, también se pueden prevenir por completo con configuraciones correctas en el registrador de dominios y los proveedores de DNS. Sin embargo, no todos los proveedores de DNS son explotables. Después de evaluar alrededor de una docena de ellos, hemos confirmado que todos los días ocurren cientos de secuestros de dominios en proveedores explotables: hemos identificado aproximadamente 800 mil dominios registrados con delegaciones lame desde agosto, pero el número real es mucho mayor; no hemos incluido subdominios vulnerables y limitamos nuestra búsqueda a muestras de ciertos proveedores.

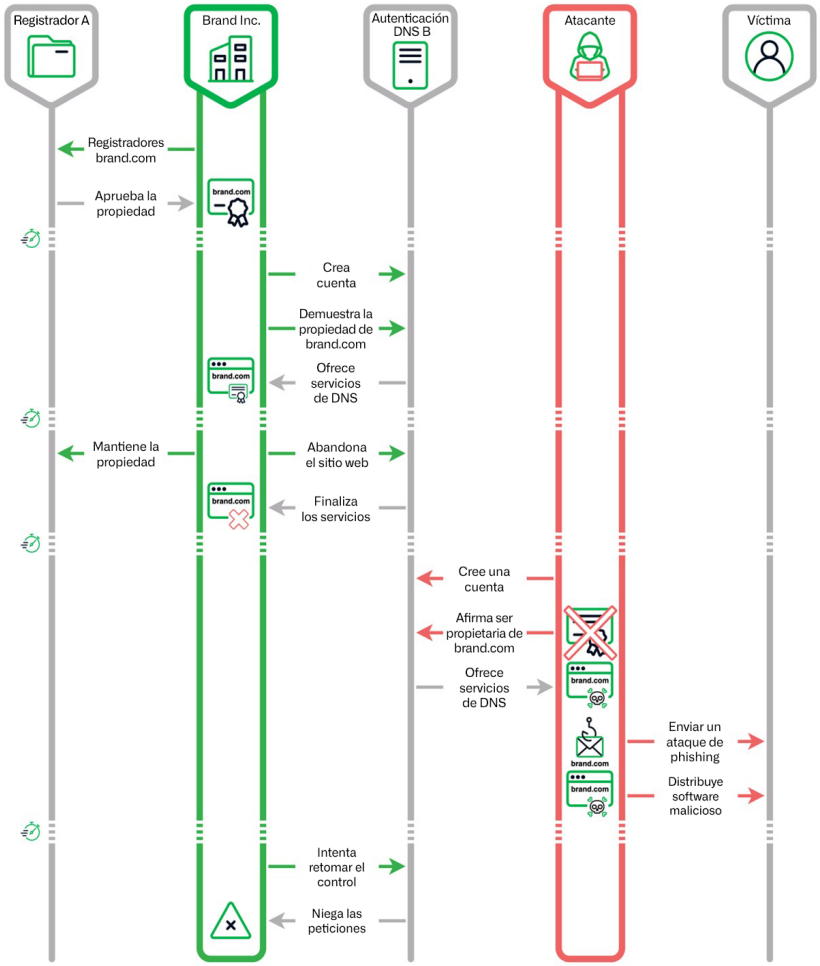

Figura 1. Una secuencia de ataque Sitting Ducks común

Todavía se desconoce cómo los actores de amenazas identifican dominios vulnerables a través de los proveedores. Hemos implementado varios métodos de detección y, a través de ellos, descubrimos que entre el seis y el diez por ciento de los dominios asignados a proveedores de DNS explotables en un día determinado no estaban correctamente configurados. Algunos proveedores explotables tenían un número significativamente mayor de dominios vulnerables y, dado que nuestras pruebas fueron limitadas, el verdadero panorama de explotación probablemente es mucho mayor de lo que sabemos hoy en día. En general, estimamos que más de 1 millón de dominios registrados son vulnerables a un ataque Sitting Ducks en un día determinado. La mayoría de los dominios vulnerables que hemos identificado cuentan con servidores de nombres asignados a uno de los pocos proveedores de DNS disponibles.

Ahora, echemos un vistazo a algunos de los actores que utilizan este vector de ataque.

VACANT VIPER

¿Qué importa un nombre?

Vacant Viper es el nombre que hemos dado al actor de la amenaza que opera el 404TDS, el cual fue reportado inicialmente por Proofpoint.[7] Como práctica, Infoblox no cambia los nombres de actores establecidos ni de los componentes de infraestructura. Cuando nos referimos al 404TDS, estamos hablando del TDS en sí, y cuando hablamos de Vacant Viper, nos referimos al actor que secuestra dominios para el 404TDS y se dedica a otras actividades maliciosas como el spam.

Mientras estudiábamos el 404TDS para encontrar una firma de DNS que pudiera predecir qué dominios se integrarían a la infraestructura del TDS, nos dimos cuenta de que los dominios estaban siendo secuestrados. Además, al observar detenidamente los dominios comprometidos, parecía que el actor estaba tramando algo más que solo operar un TDS criminal. Bautizamos al actor secuestrador como Vacant Viper, usando nuestra categoría "viper" como una referencia al origen del TDS.

Vacant Viper es uno de los primeros actores de amenazas conocidos en explotar el ataque Sitting Ducks y ha secuestrado alrededor de 2500 dominios cada año desde diciembre de 2019. Este actor utiliza los dominios secuestrados para ejecutar operaciones maliciosas de spam, distribuir pornografía, establecer C2 de troyanos de acceso remoto (RAT) y lanzar malware como DarkGate y AsyncRAT, junto con sus operaciones en el 404TDS.[8] Entre sus afiliados reportados se encuentran TA-866 y TA-571.

Vacant Viper abusa de las empresas de DNS de DigiCert, pero prefiere las cuentas gratuitas en DNS Made Easy, que están disponibles durante un período de prueba de treinta días y solo requieren una dirección de correo electrónico para configurarse. Sin embargo, también han secuestrado dominios en Constellix, un servicio de DNS premium que requiere la interacción con los representantes de ventas antes de ofrecer una prueba gratuita. Desde que informamos por primera vez sobre los ataques Sitting Ducks en julio de 2024, el actor ha ajustado sus técnicas, pero sigue operando exclusivamente con este conjunto de proveedores. La cantidad de secuestros que realizan varía con el tiempo, pero, por ejemplo, identificamos aproximadamente 100 dominios secuestrados por Vacant Viper en las dos primeras semanas de octubre de 2024.

Vacant Viper no secuestra dominios para vincularlos a una marca específica, sino para obtener un conjunto de recursos con alta reputación que no sean bloqueados por los proveedores de seguridad. Vacant Viper también toma el control de algunos dominios de manera recurrente con el paso del tiempo. Por ejemplo, en enero de 2024, se observó que `clickermediacorp[.]com` formaba parte del 404TDS y estaba asociado con una campaña de phishing que imitaba a Slack. Sin embargo, este dominio ya había sido utilizado en enero de 2020 para distribuir distintos tipos de contenido, incluyendo pornografía y estafas con bitcoin.

Una característica clave de un TDS es tener afiliados: proveedores que envían tráfico al TDS y clientes que reciben tráfico del TDS. En el mundo de la publicidad, el objetivo de un TDS es maximizar las ganancias, es decir, dirigir a los usuarios al anuncio que es más probable que les guste.

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

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

El objetivo de un TDS criminal es similar: atraer a los usuarios con contenido que probablemente deseen consumir, y luego redirigirlos al contenido malicioso, ya sea una descarga de malware, una página de inicio de sesión falsa o una estafa con tarjetas de regalo.

Los siguientes ejemplos de cadenas de ataque del 404TDS muestran las técnicas de redirección utilizadas tanto por el TDS como por sus afiliados, incluyendo cómo Vacant Viper utiliza dominios secuestrados en el 404TDS.

Un dominio que Vacant Viper secuestró y usó en el 404TDS es `mcpennsylvania[.]com`, un dominio registrado por McDonald's con el registrador corporativo CSC Corporate Domains y asignado a los servidores de nombres en DNS Made Easy, una subsidiaria de DigiCert.[9] Vacant Viper ha secuestrado este dominio repetidamente a lo largo de los últimos años, y actualmente tiene una delegación lame. En una observación reciente, vimos que este dominio de McDonald's redirigía a `ncbtv[.]com` (anteriormente operado por un proveedor de servicios de IPTV), que se registró con GoDaddy en 2011, originalmente con una dirección de correo electrónico china. Irónicamente, este dominio también, ahora cubierto bajo registro privado, parece haber sido secuestrado mediante un ataque Sitting Ducks en varias ocasiones, posiblemente desde 2017. Actualmente, `ncbtv[.]com` está vinculado con VexTrio Viper, un actor de amenazas que usa dominios secuestrados para alojar sitios de citas y otros contenidos. Suponiendo que este actor sea independiente de Vacant Viper, podemos ver que los actores de amenazas que usan ataques Sitting Ducks cooperan entre sí y probablemente comparten conocimientos y/o recursos para los dominios vulnerables.

En junio de 2023, cuando Vacant Viper secuestró `mcpennsylvania[.]com`, lo utilizó para el 404TDS en una cadena de ataque de malware AsyncRAT y aprovechó dos mecanismos diferentes (meta refresh y HTTP refresh) para redirigir al usuario:[10]

- La URL `hXXps://mcpennsylvania[.]com/y0t/gojhuovy` mostraba un error 404 (No encontrado), sin embargo, se ejecutó un meta refresh en segundo plano para redirigir al usuario mediante la etiqueta HTML meta:

  » `<meta http-equiv="refresh" content="0;hXXps://ecole-artcom[.]com/wdown">`

- La segunda URL `hXXps://ecole-artcom[.]com/wdown/` no mostró contenido, salvo un encabezado de HTTP refresh, que efectivamente redirigió al usuario nuevamente a una tercera URL
- La tercera URL `hXXps://www[.]mediasimulasi[.]com/wazxd` ejecutó un archivo JavaScript llamado Information_28_jun_1220107.js, que luego descargó archivos relacionados con AsyncRAT[11]

Aunque se desconoce quién controla los dominios de destino, estos solo se han observado en conexión con 404TDS. Mostramos los encabezados de la cadena de ataque `mcpennsylvania[.]com` en la Figura 2.

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

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

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

Figura 2. Los encabezados de refresh redirigieron a los usuarios a `hXXps://www[.]mediasimulasi[.]com/wazxd`

Vacant Viper también utilizó la técnica HTML meta refresh en las cadenas de ataque que distribuían el malware DarkGate a través de archivos adjuntos de spam maliciosos. La cadena de redirección para la entrega del malware DarkGate[12] es similar a la del anterior para AsyncRAT, pero no incluye el método HTTP refresh:

1. El usuario intenta acceder a `afarm[.]net`, lo que genera un error 404 No encontrado
2. La URL del TDS `hXXps://afarm[.]net/uvz2q` luego redirige a `https://wercosliuhqgheirn[.]com/` a través del método HTML meta refresh `<meta http-equiv="refresh" content="0;hXXps://wercosliuhqgheirn[.]com/">`
3. El usuario es redirigido a `hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php`, donde se descarga el siguiente archivo que contiene el malware DarkGate:

Nombre del archivo	Hash SHA-256
08-May-24-document-53aa77b6.jar	f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a

Los ocho dominios en la Tabla 1 siguen el mismo patrón de redirección para entregar el mismo archivo JAR asociado con DarkGate.[13] Hemos visto seis de estos dominios en archivos adjuntos de spam con nombres similares, como may-document_85138492.pdf, en mayo de 2024. Todos estos archivos se distribuyen como adjuntos en correos electrónicos de spam maliciosos, los cuales contienen un mensaje genérico que hace referencia a una factura o documento de gastos adjunto, alentando al usuario a abrirlo para poder realizar el pago.

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

Tabla 1. Dominios secuestrados utilizados por Vacant Viper para distribuir el malware DarkGate

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

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

Si bien la investigación de Vacant Viper llevó a nuestro (re-)descubrimiento del vector de ataque Sitting Ducks, también nos permitió vincular a otros actores de amenazas con dicho vector. Algunos de estos actores ya estaban siendo rastreados y otros no. En general, hemos encontrado extremadamente difícil descubrir un dominio comprometido por sí solo; hemos utilizado el comportamiento del actor de amenazas para retroceder y encontrar una firma que luego pueda ser rastreada. Para los actores de amenazas que aprovechan el secuestro de DNS, usamos la categoría de nomenclatura "hawk" (halcón).

¿Por qué un halcón?

Estos actores de amenazas se abalanzan sobre los dominios vulnerables y los secuestran, del mismo modo que los halcones se lanzan en picado para atrapar a su presa.

HORRID HAWK

Horrid Hawk es un actor de amenazas de DNS que ha estado secuestrando dominios y utilizándolos para esquemas de fraude de inversión desde al menos febrero de 2023. Son interesantes porque utilizan dominios secuestrados en cada etapa de sus campañas recientes y crean anzuelos convincentes sobre programas de inversión o cumbres gubernamentales inexistentes. Incorporan los dominios secuestrados en anuncios breves de Facebook que apuntan a usuarios en más de 30 idiomas, abarcando varios continentes. Rastreamos a Horrid Hawk a través de DNS y hemos identificado casi 5 mil de sus dominios secuestrados.

Una cadena de ataque de Horrid Hawk involucra dos dominios secuestrados diferentes; la mayoría de las veces, estos han sido secuestrados de algunos proveedores de DNS: Linode, TierraNet y A2 Hosting. Después de secuestrar un dominio, Horrid Hawk reconfigura la dirección IP del registro A a un servidor dedicado diferente. El actor asigna uno de los dominios a un servidor TDS que protege la página de destino de los investigadores de seguridad y filtra a los visitantes no deseados. Horrid Hawk asigna el otro dominio a la página de destino que alberga contenido fraudulento sobre inversiones. Al principio de su historia, Horrid Hawk también registró sus propios dominios similares que encajaban con los temas de inversión gubernamentales, como `oil-poland[.]site` y `balticpipe[.]playroom8[.]site`. El actor utilizó estos dominios para sus páginas de destino que alojaban contenido relacionado con estafas de proyectos de gas. La Figura 3 muestra la línea de tiempo de dos dominios que secuestraron y utilizaron juntos en un ataque.

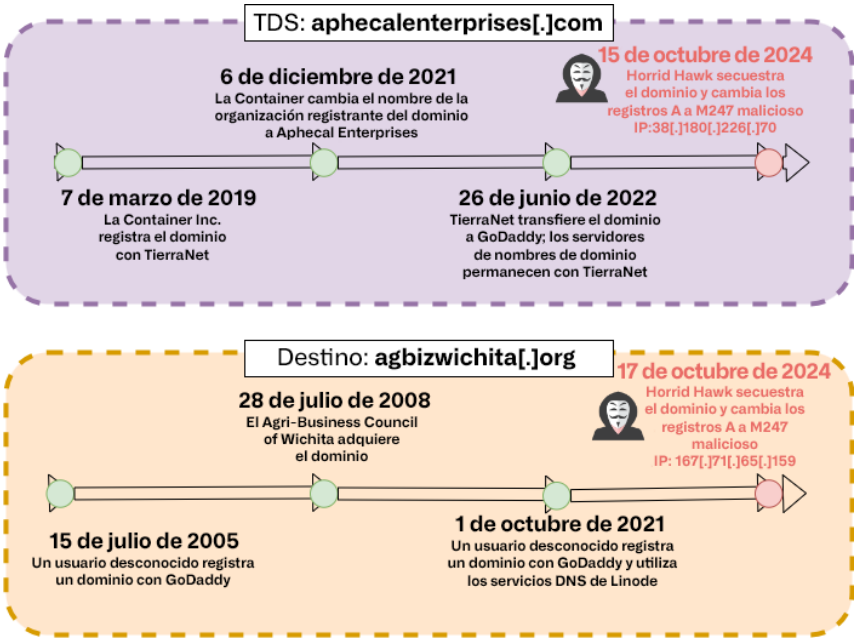

Figura 3. Línea de tiempo del secuestro de dominios de `aphecalenterprises[.]com` *(TDS) y* `agbizwichita[.]org` *(dominio de la página de destino)*

Horrid Hawk se ceba con los consumidores de todo el mundo. Comienzan sus ataques creando numerosos anuncios en Facebook, como el que se muestra en la Figura 4, dirigidos a usuarios en Polonia y que anuncian un falso proyecto de gas financiado por el gobierno, el "Gasoducto del Báltico". La imagen utilizada en el anuncio de Facebook contiene un mensaje que insta a los usuarios mayores de 50 años a hacer clic en el enlace del anuncio y leer el contenido del artículo web. Esta campaña publicitaria en Facebook llegó a más de 13 mil internautas. Aunque el ejemplo que utilizamos en esta sección es una campaña dirigida a usuarios mayores de habla polaca, Horrid Hawk también emplea señuelos de phishing en inglés, italiano, turco, español y muchos otros idiomas.

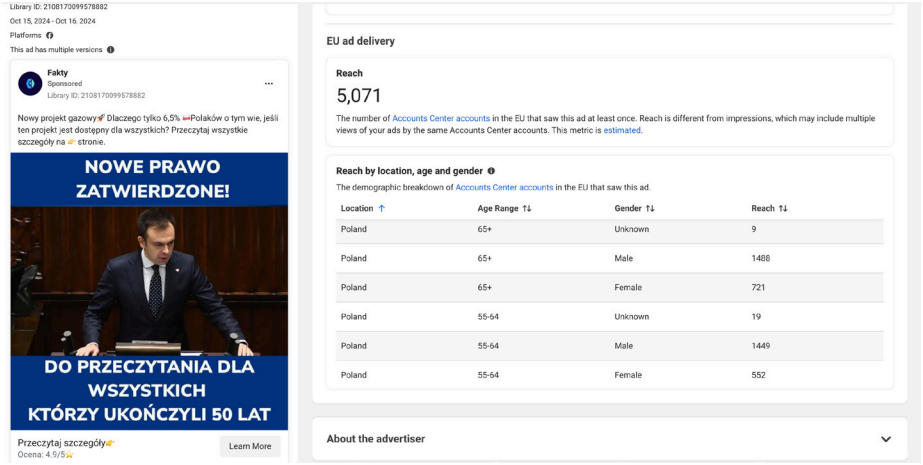

Figura 4. Ejemplo de un anuncio de Facebook de Horrid Hawk dirigido a usuarios de habla polaca que en su mayoría tienen más de 55 años

El enlace publicitario que se muestra en la Figura 4 apunta a `hXXps://aphecalenterprises[.]com/`, una URL utilizada por el servidor TDS de Horrid Hawk. Este sistema es importante para el actor de amenazas porque protege la página de destino de la estafa perfilando a los visitantes web y filtrando a los invitados irrelevantes o no deseados, como los investigadores de seguridad y los robots de rastreo web. El servidor utiliza la información de geolocalización para determinar la siguiente ubicación URL del visitante de la web. Por ejemplo, si un usuario llega a `hXXps://aphecalenterprises[.]com/` desde una dirección IP basada en Polonia, Horrid Hawk lo redirigirá a la página web fraudulenta con temática gubernamental ubicada en: `hXXps://agbizwichita[.]org/9fMS3XSS`. La ruta de URL aleatoria 9fMS3XS es solo temporal y este sitio web cargará un archivo estático (/lander/long-ready-2_0/index.html) al que hace referencia el atributo href HTML base. La Figura 5 es la página web que vimos cuando esta URL aún estaba activa.

Figura 5. Página web de estafa de temática política (`hXXps://agbizwichita[.]org/lander/long-ready-2_0/index.html`) dirigida a usuarios de habla polaca

Si la dirección IP del visitante del sitio web se encuentra en un país que no es relevante para la audiencia objetivo de Horrid Hawk, esos usuarios generalmente serán redirigidos a una página web de engaño que utiliza el mismo dominio del TDS. Por ejemplo, cuando visitamos `aphecalenterprises[.]com` desde una dirección IP fuera de Polonia, el TDS nos mostró una página web inofensiva que imitaba una tienda de ropa en línea. La Figura 6 muestra la estructura de la URL y el contenido de la página de señuelo. Las URL de las páginas web señuelo contienen un nombre de archivo con el prefijo estático `w-{código de país}-`. En este caso, el código de país era "pl", una abreviatura de Polonia, y la "w" posiblemente signifique cubierta blanca o etiqueta blanca.

Figura 6. Una página web señuelo servida por el TDS de Horrid Hawk para visitantes fuera del objetivo

El tema más prevalente que hemos visto en las diversas páginas web ha sido relacionado con el "Proyecto Gasoducto del Báltico", un esquema de inversión que afirma que los ciudadanos polacos que inviertan en nuevos gasoductos pueden ganar grandes sumas de dinero. En el ejemplo anterior que involucra la página de destino `agbizwichita[.]org`, Horrid Hawk utiliza una táctica para asustar que aprovecha el miedo natural de las personas a perderse algo (FOMO). La página web afirma que los ciudadanos que no participen en el proyecto de gas financiado por el gobierno incurrirán en un aumento del 55 % en los gastos relacionados con el gas. Al igual que las campañas de inversión operadas por otro actor de esquemas de inversión que reportamos este año, Savvy Seahorse,[14] las campañas del proyecto del "Gasoducto del Báltico" piden al usuario que introduzca sus datos personales, incluido nombre, correo electrónico y número de teléfono, en un formulario incrustado para registrarse en la oportunidad de inversión. Luego se informa a los usuarios que serán contactados para solicitarles información adicional antes de que puedan acceder a la "plataforma de inversión". Ver Figura 7. Aunque otros actores de amenazas ejecutan estafas del Gasoducto del Báltico, Horrid Hawk se distingue por su uso de ataques Sitting Ducks para secuestrar dominios.[15]

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

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

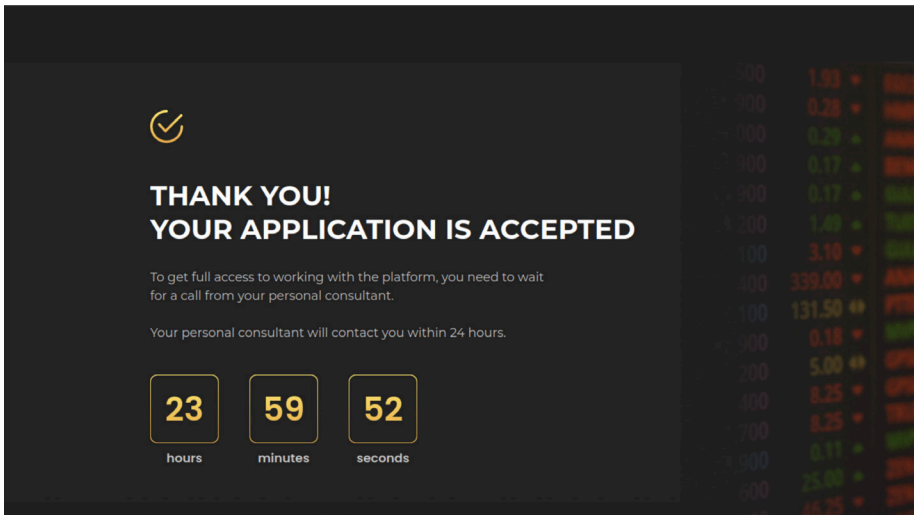

Figura 7. Una página de respuesta típica de Horrid Hawk que se muestra después de que una víctima se registre con éxito en los sitios web fraudulentos

HASTY HAWK

Hasty Hawk es otro actor de amenazas que descubrimos durante nuestra investigación sobre la técnica de secuestro Sitting Ducks. Desde al menos marzo de 2022, Hasty Hawk ha secuestrado más de 200 dominios para operar campañas de phishing generalizadas, que en su mayoría suplantan páginas de envío de DHL y sitios de donaciones falsos para apoyar a Ucrania. El actor explota muchos proveedores, incluidos HawkHost, Maria Hosting y DigitalOcean. Los dominios secuestrados a menudo se reconfiguran a través de DNS para alojar contenido en ASN rusos como PROTON66 o BEGET, aunque también se sabe que el actor utiliza otros proveedores como OVH. Hasty Hawk utiliza anuncios de Google y posiblemente otros medios como mensajes de spam para distribuir contenido malicioso.

Los nombres de dominio completos (FQDN) de Hasty Hawk tienden a seguir algunos patrones, tales como:

- `dhl.<números aleatorios>.<dominio secuestrado>`
- `dhl-id<números aleatorios>.<dominio secuestrado>`
- `<números/letras aleatorios>.dhl.<dominio secuestrado>`

La Figura 8 muestra los cambios en los registros DNS de `thebagshelf[.]com` desde su fecha de creación hasta el día en que fue secuestrado por Hasty Hawk. Al igual que Horrid Hawk, Hasty Hawk también reconfigura la dirección del registro A a un servidor dedicado al actor. Además de los prefijos de subdominio con temática de DHL como `dhl[.]3204[.]thebagshelf[.]com`, hemos observado otros prefijos de nombre de subdominio estáticos en estos servidores, como `id-f<número aleatorio>.<dominio secuestrado>` (por ejemplo, `id-f0596[.]successbusinesspages[.]com`).

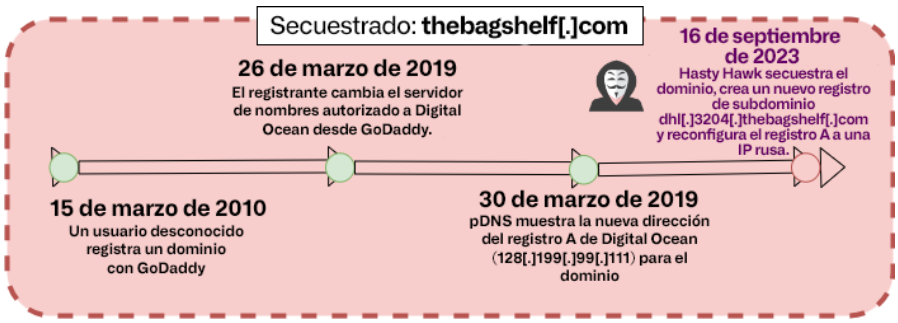

Figura 8. Línea de tiempo del secuestro de dominio de `thebagshelf[.]com`

Recientemente, Hasty Hawk cambió muchas de sus páginas con temática de DHL por sitios falsos de donaciones que son copias espejo del sitio legítimo, supportukrainenow[.]org, dirigido por la organización Global Shapers,[16] para apoyar a Ucrania durante la guerra (véase la Figura 9). El actor también ha creado páginas suplantando a la Unión Europea con otro falso sitio de donación que está dirigido a europeos que desean apoyar a las víctimas de la guerra.

Figura 9. Web de donaciones falsa que suplanta a supportukrainenow[.]org

Hasty Hawk utiliza un TDS para dirigir a los usuarios a diferentes páginas web que varían en contenido e idioma en función de su geolocalización y, posiblemente, de otras características del usuario. Cuando los usuarios ven contenido diferente según el dispositivo que utilizan, su ubicación o en distintos momentos, es una clara indicación de que un TDS está trabajando en segundo plano, asegurando que las víctimas sean redirigidas a la página que más beneficia a los criminales. Hasty Hawk también cambia algunos de sus dominios entre diferentes temas de campaña. Veamos el ejemplo de la Figura 10, sobre las redirecciones basadas en geolocalización y los cambios en el contenido de la página web a lo largo del tiempo para el FQDN dhl[.]3204[.]thebagshelf[.]com.

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

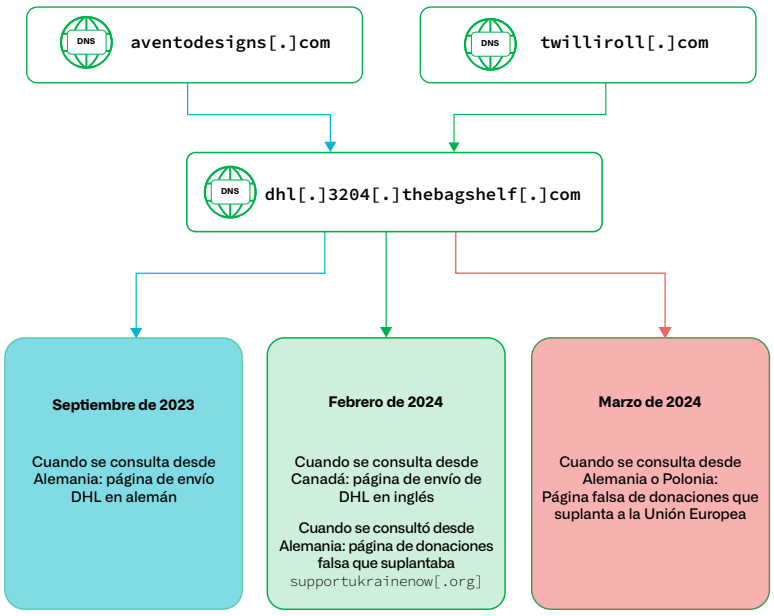

Figura 10: Ejemplo de redirecciones hacia `dhl[.]3204[.]thebagshelf[.]com` *y algunas de las páginas web que el actor ha mostrado a lo largo del tiempo*

1. **Septiembre de 2023** – El FQDN aloja una página de envío DHL en alemán. Los usuarios fueron redirigidos allí desde `aventodesigns[.]com`.[17]
2. **Febrero de 2024** – El FQDN aloja tanto una página de envío DHL en inglés (redirigida desde `twilliroll[.]com`) para los usuarios de Canadá, como la página falsa de donación que suplanta a `supportukrainenow[.]org` para usuarios en Alemania.
3. **Marzo de 2024** – El FQDN cambia de IP de `91[.]212[.]166[.]71` a `91[.]212[.]166[.]14` y aloja la página de soporte de Ucrania que suplanta a la Unión Europea para usuarios en Alemania y Polonia.

Hasty Hawk continuó cambiando los temas de campaña para este único FQDN a lo largo de 2024. En septiembre, el FQDN alojaba la página de envío DHL en inglés que se muestra en la Figura 11 o redirigía a una página CAPTCHA que exigía al usuario "completar la verificación de seguridad para acceder a `dhl[.]com`", redirigiendo al sitio web legítimo de DHL como señuelo.[18]

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

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

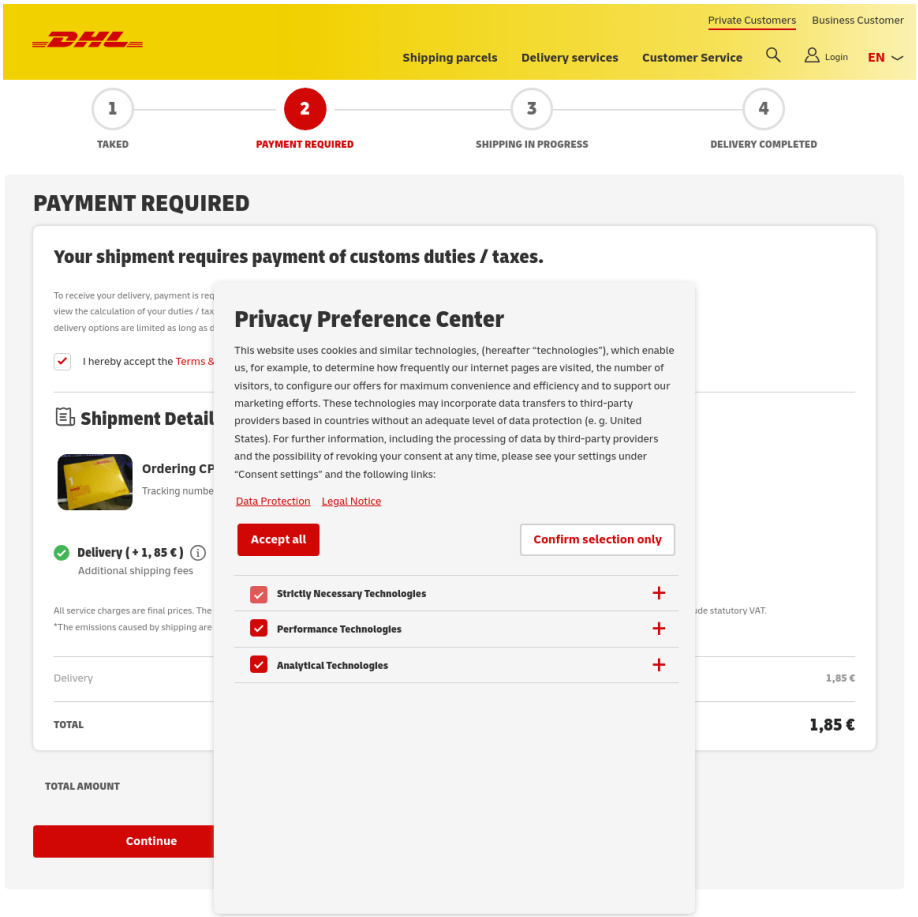

Figura 11. Página de phishing de DHL para `dhl[.]3204[.]thebagshelf[.]com` *en septiembre de 2024*

VEXTRIO VIPER Y AFILIADOS

A medida que nuestra investigación nos llevó a descubrir más y más dominios secuestrados por medio de la técnica Sitting Ducks, reconocimos algunos como parte de la enorme infraestructura TDS de VexTrio Viper desde principios de 2020. Estos dominios inicialmente nos llamaron la atención debido a su antigüedad, pero una vez que descubrimos que fueron secuestrados, la pieza que faltaba encajó. Básicamente, VexTrio Viper usa dominios secuestrados en su TDS de manera similar a Vacant Viper. VexTrio gestiona el programa de afiliados cibernético más grande, redirigiendo el tráfico web comprometido de más de 65 socios afiliados, algunos de los cuales también han robado dominios mediante Sitting Ducks para sus propias actividades maliciosas.

VexTrio ha asumido el control de dominios inactivos que previamente estaban delegados a los servidores de nombres de DigiCert/DNS Made Easy (DME), Constellix y DigitalOcean para gestionar sus servidores TDS. Los dominios secuestrados redirigen el tráfico hacia sus editores de contenido malicioso, o sus propios sitios maliciosos, que albergan estafas de citas falsas y tarjetas de regalo, notificaciones falsas de CAPTCHA de robots, etc.

Uno de los ejemplos más notables es `mpinc[.]com`. Hemos confirmado que VexTrio secuestró el dominio en agosto de 2023, aunque podría haber sido comprometido desde abril de 2022. El propietario original de este dominio es MPR Associates, una organización centrada en la investigación educativa. Este dominio estuvo activo principalmente en los años 90 y 2000 antes de ser adquirido en 2013 por RTI International (`rti[.]org`), un instituto de investigación sin fines de lucro especializado en cuestiones sociales, científicas y de salud. El dominio se cambió a los servidores DNS de DME a finales de 2015. Según pDNS, `mpinc[.]com` estuvo estacionado en una IP de DigitalOcean (`157[.]230[.]67[.]179`) durante tres meses a partir de enero de 2022, antes de ser secuestrado en abril de 2022 por un actor de amenazas,

probablemente VexTrio. Mientras estuvo bajo el control de VexTrio de agosto a octubre de 2023, el dominio redirigió a los usuarios a uno de los sitios de citas falsas comúnmente utilizados por el actor, como se muestra en la Figura 12.[19, 20] Actualmente, `mpinc[.]com` está en estado inactivo y no se ha delegado a un servidor DNS autorizado.

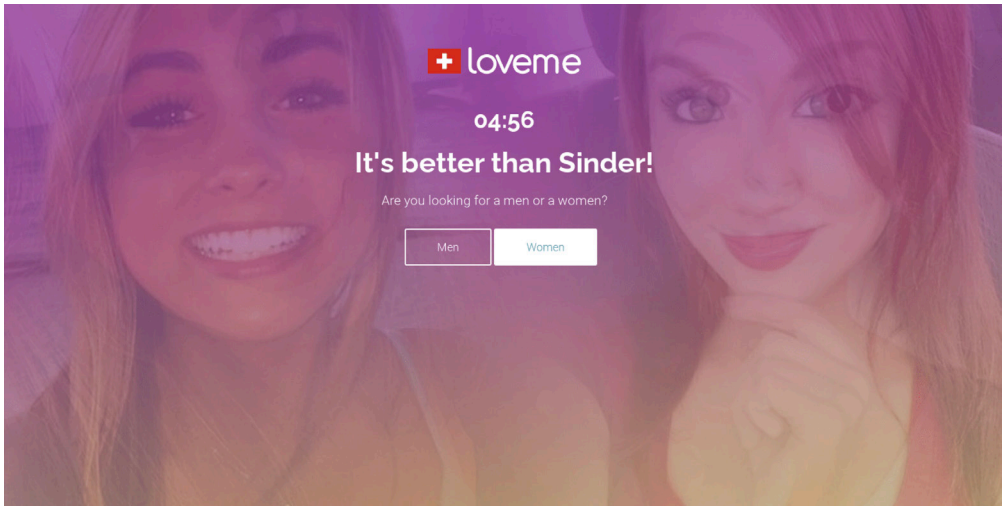

Figura 12. Página de citas falsa para el dominio secuestrado `mpinc[.]com`

VexTrio también secuestró `iccps[.]org`, un dominio que anteriormente se utilizaba para la Conferencia Internacional Anual sobre Sistemas Ciberfísicos de la ACM/IEEE (ICCPS). El dominio fue registrado desde septiembre de 2009 por un profesor de la Universidad Carnegie Mellon. Según la información de WHOIS, evaluamos que este dominio, una vez delegado a los servidores de nombres de DME, pasó a ser explotable a partir de principios de agosto de 2023. VexTrio luego lo usó en su infraestructura TDS, redirigiendo a los usuarios hacia sus campañas desde septiembre hasta octubre de 2023. Después se resolvió en la dirección IP de DigitalOcean utilizada para los dominios caducados, y finalmente se estacionó en una IP de Bodis, donde permanece actualmente. ACM/IEEE utiliza ahora `iccps[.]acm[.]org`[21] para su conferencia.

LOS AFILIADOS DE VEXTRIO VIPER UTILIZAN ANTIBOT CLOUD

También hemos observado que los afiliados de VexTrio Viper explotan Sitting Ducks. Muchos de ellos utilizan AntiBot Cloud, un servicio antibot ruso, como método para filtrar los bots y el tráfico de los investigadores de seguridad. La funcionalidad de AntiBot incluye la capacidad de establecer reglas para bloquear ciertos servicios o usuarios de bots en función de su información, como su IP, geolocalización y agente de usuario. Los usuarios pueden ejecutar este servicio de forma gratuita localmente, con protección limitada contra bots, o actualizar a la versión premium en la nube. A simple vista, AntiBot Cloud no parece ser intrínsecamente malicioso, pero la mayoría de la base de usuarios parecen ser ciberdelincuentes. El servicio, preferido por los ciberdelincuentes rusos y de otros países de Europa del Este, se desarrolló originalmente en ruso, luego se expandió al contenido en inglés y presenta el rublo ruso como una de sus principales opciones de pago (véase la Figura 13). AntiBot parece estar gestionado en su totalidad por una persona que utiliza el alias de MikFoxi, que se autodenomina programador autónomo. También es importante señalar que solo los afiliados, y no VexTrio Viper, usan AntiBot, por lo que bloquear AntiBot no afectará a VexTrio. Los FQDN para el servicio en la nube de AntiBot incluyen:

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

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

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

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

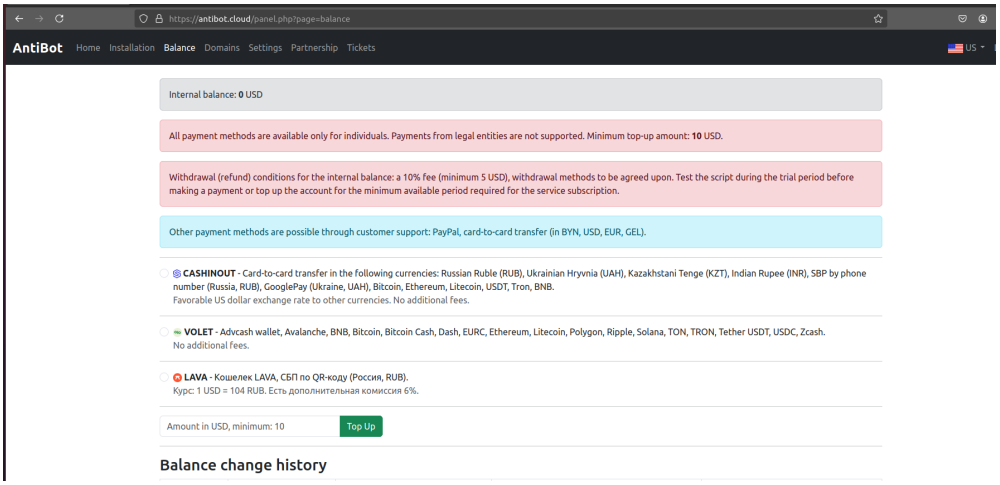

Figura 13. Opciones de pago de AntiBot, incluido el rublo ruso

Un afiliado que usa AntiBot secuestró el dominio missouri[.]com[22] a través de DME en octubre de 2022, aunque este dominio podría haber sido robado previamente por otros actores maliciosos incluso antes. Mientras el dominio estaba bajo el control de este afiliado, los usuarios eran redirigidos a un sitio web falso de citas operado por VexTrio Viper. Antes del primer secuestro, el sitio web que usaba missouri[.]com fue desarrollado por State Ventures, LLC y posiblemente estaba relacionado con el estado de Missouri. Anteriormente, el dominio mostraba un gran número de registros de subdominio dedicados a las ciudades y condados de Missouri. Los datos almacenados en caché muestran que era un sitio rico en contenido relacionado con los negocios y el turismo del estado, como se muestra en la Figura 14 a continuación. Además, el antiguo sitio web de la lotería de Missouri posiblemente estaba asignado al subdominio loterry[.]missouri[.]com. Su contenido ahora se aloja en molottery[.]com, que también utiliza servidores de nombres DME.

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

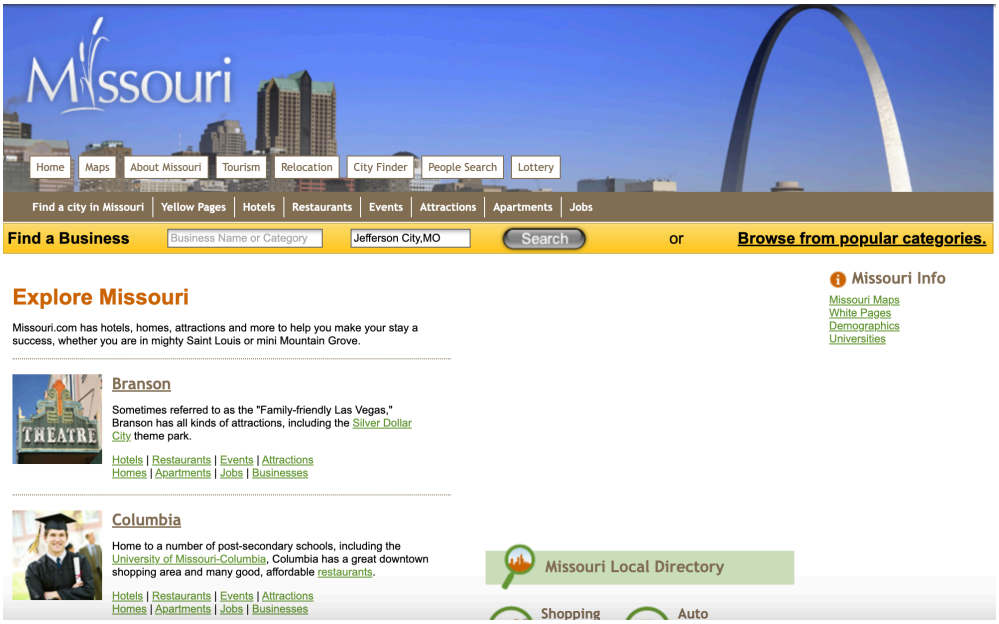

Figura 14. Página web de `missouri[.]com` *en septiembre de 2018, posiblemente la página oficial del estado de Missouri antes de que la secuestraran*

AFILIADO DE VEXTRIO GOREFRESH

GoRefresh es un afiliado de VexTrio Viper que opera campañas falsas de productos farmacéuticos en línea y participa en otras campañas de afiliados, como estafas de juegos en línea o citas. GoRefresh ha secuestrado dominios de proveedores de servicios DNS vulnerables DME y GoDaddy. Este afiliado utiliza estos dominios secuestrados para redirigir el tráfico web comprometido a VexTrio y otros afiliados, así como a sus propias páginas de destino de productos farmacéuticos.

Al igual que Vacant Viper, GoRefresh suele responder a los usuarios con un código de estado de respuesta de error HTTP 404 No encontrado. Como alternativa, cuando asignan un recurso como redirector, omiten la respuesta tradicional de redirección HTTP 302 y, en su lugar, "actualizan" la página web de la víctima a la siguiente URL mediante un meta refresh en HTML. Un ejemplo de este código de redirección HTML:

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

SECUESTRO ROTACIONAL

Un hecho común que hemos observado al investigar Sitting Ducks es el secuestro rotacional, cuando un dominio es secuestrado por múltiples actores a lo largo del tiempo. Los actores de amenazas a menudo usan proveedores de servicios explotables que ofrecen cuentas gratuitas, como DNS Made Easy, como bibliotecas prestadas, secuestrando dominios durante 30 a 60 días; sin embargo, también hemos visto otros casos en los que los actores mantienen el dominio durante un período prolongado. Una vez que caduca la cuenta gratuita a corto plazo, el primer actor de amenazas "pierde" el dominio y, luego, otro actor de amenazas lo deja sin usar o lo reclama.

Hemos visto a afiliados de VexTrio Viper hacer esto con bastante frecuencia, especialmente cuando secuestran dominios que previamente fueron comprometidos por Vacant Viper. A modo de ejemplo, en la Figura 15 a continuación mostramos la línea de tiempo del secuestro de `mcpennsylvania[.]com`, que primero fue secuestrado por Vacant Viper y después por un afiliado de VexTrio Viper. Según la información de WHOIS, el registrador (CSC Digital Brand Services) y el proveedor del servidor de nombres (DME) permanecieron en su mayoría sin cambios a lo largo de los diversos secuestros.

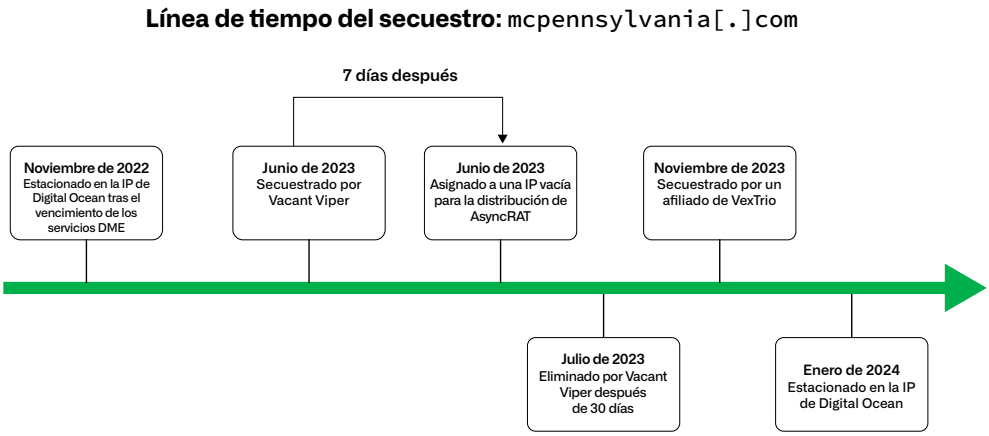

Figura 15. Línea de tiempo del secuestro de mcpennsylvania[.]com

CONCLUSIÓN

Los actores de amenazas que hemos descrito son solo una muestra de aquellos que se han aprovechado de este poderoso y oscuro vector de ataque. Si bien los efectos del vector de ataque de Sitting Ducks son de gran alcance, también se pueden prevenir por completo, aunque son complicados de abordar. Los actores seguirán explotando este vector de ataque si no se toman medidas activas para mitigar y, en última instancia, prevenir el problema. Como compartimos en nuestro blog de divulgación, todo el mundo desempeña un papel para detener los ataques Sitting Ducks, desde los proveedores y registradores de DNS autorizados hasta las organizaciones gubernamentales y los organismos de normalización. Necesitamos mejores formas de detectar los secuestros y mitigarlos lo más rápido posible. Los propietarios legítimos de dominios no solo deben mantener sus registros DNS, sino también ser receptivos a los informes de abuso, al igual que los registradores y los proveedores.

Debido a la dificultad de detectar este ataque, no cabe duda de que los actores maliciosos seguirán aprovechándose de él. Hemos encontrado varios actores que han secuestrado dominios y los han mantenido durante períodos prolongados, pero no hemos podido determinar el propósito del secuestro. Estos dominios suelen tener una gran reputación y, por lo general, los proveedores de seguridad no los notan, lo que crea un entorno en el que los actores astutos pueden entregar malware, cometer fraudes desenfrenados y suplantar las credenciales de los usuarios sin consecuencias. Con suerte, a medida que la comunidad de inteligencia de amenazas se vuelva más consciente de la técnica, destacarán el uso de actores y permitirán rastrear y corregir los dominios secuestrados.

Si bien los productos de Infoblox no son vulnerables a Sitting Ducks, nuestros clientes aún pueden verse afectados dependiendo de cómo hayan elegido operar el DNS de los dominios que registren. . Por lo tanto, recomendamos que todos los propietarios de dominios, especialmente aquellos que usan sistemas DNS de terceros y no son conscientes de su estado de servicio, evalúen su nivel de riesgo siguiendo las tres preguntas de la Figura 16.

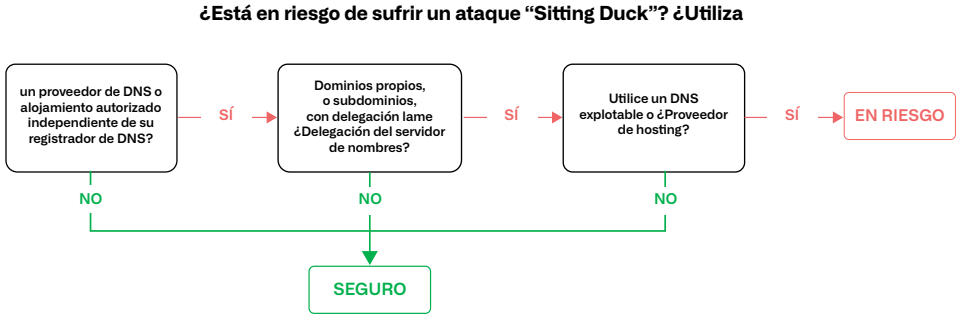

Figura 16. Tres preguntas para determinar si corre el riesgo de sufrir un ataque Sitting Ducks

VÍCTIMAS DE SITTING DUCKS

Los dominios secuestrados que describimos en este informe pertenecían a organizaciones legítimas de diversos sectores industriales. Un dominio puede tener múltiples propietarios diferentes durante su vida útil. La siguiente lista incluye los propietarios legítimos que identificamos antes de que sus dominios fueran secuestrados.

Dominio secuestrado	Propietario legítimo del dominio
agbizwichita[.]org	Consejo de Agronegocios de Wichita
alonbyacarian[.]com	Altavoces Alon Capri de Acarian Systems
aphecalenterprises[.]com	Aphecal Enterprises, Inc.
clickermediacorp[.]com	CBS Interactive
iccps[.]org	International Conference on Cyber-Physical Systems
jmnet[.]com	JM Eagle
mbhs[.]com	MISSISSIPPI BAPTIST HEALTH SYSTEMS, INC.
mcpennsylvania[.]com	McDonald's Corporation
missouri[.]com	State Ventures, LLC y posiblemente el estado de Missouri
mosaicmedicalsupply[.]com	Mosaic Medical Supplies (proveedor de suministros ortopédicos y cosméticos)
mpinc[.]com	MPR Associates (bufete de abogados)
mstouchenaturals[.]com	MS TOUCHE
mygemcon[.]com	Grupo Gemcon
ncbtv[.]com	NCBTV (proveedor de servicios de IPTV)
successbusinesspages[.]com	Success Business Pages (directorio de negocios en línea)
thebagshelf[.]com	Tienda de ropa tailandesa en línea
tmsec[.]com	T&M USA (empresa de seguridad privada e investigaciones)
uni-t[.]com	Bridgestone (compañía de venta de neumáticos Firestone)

INDICADORES DE ACTIVIDAD

La tabla a continuación proporciona indicadores de actividad (IOA) utilizados por estos actores de amenazas; para más información, visite el repositorio de Inteligencia sobre amenazas de Infoblox en GitHub: https://github.com/infobloxopen/threat-intelligence/tree/main.

Indicador	Tipo	Nota
oil-poland[.]site balticpipe[.]playroom8[.]site	Dominio	Dominios similares registrados por Horrid Hawk y utilizados en sus campañas
mstouchenaturals[.]com covidianmuseum[.]com alhej[.]com agbizwichita[.]org aphecalenterprises[.]com	Dominio	Dominios secuestrados utilizados en las campañas de Horrid Hawk
thebagshelf[.]com successbusinesspages[.]com aventodesigns[.]com twilliroll[.]com	Dominio	Dominios secuestrados utilizados en campañas de Hasty Hawk
aerospaceavenue[.]com affixio[.]com adventsales[.]co[.]uk afarm[.]net affiliatebash[.]com amikamobile[.]com afcmanager[.]net adztrk[.]com clickermediacorp[.]com mcpennsylvania[.]com	Dominio	Dominios secuestrados utilizados en campañas de Vacant Viper
mpinc[.]com iccps[.]org jmnet[.]com ncbtv[.]com uni-t[.]com tmsec[.]com mbhs[.]com	Dominio	Dominios secuestrados utilizados en las campañas de VexTrio Viper

Indicador	Tipo	Nota
missouri[.]com mcpennsylvania[.]com	Dominio	Dominios secuestrados utilizados en campañas de afiliados de AntiBot Cloud
mosaicmedicalsupply[.]com	Dominio	Dominios secuestrados utilizados por el afiliado GoRefresh de VexTrio
vipshopevent[.]su	Dominio	Dominio utilizado en las campañas farmacéuticas de VexTrio GoRefresh
alonbyacarian[.]com fixedsights[.]com mygemcon[.]com sauda-pati[.]com tewksenterprises[.]com ummatie[.]com xiangmanlou[.]com	Dominio	Dominios secuestrados utilizados por un actor de estafas de salud
hXXps://ecole-artcom[.]com/wdown/ hXXps://www[.]mediasimulasi[.]com/wazxd	URL	URL relacionadas con la descarga de AsyncRAT
https://wercosliuhqgheirn[.]COM/ hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]PHP	URL	URL asociadas con la descarga de DarkGate
hXXps://antibotcloudapi[.]com/9.php antibotcloudapi[.]com antibot[.]nube antibotcloud[.]com ipv4[.]mikifox[.]com ipv6[.]mikifox[.]com admin[.]mikifox[.]com	FQDN	FQDN utilizados en el servicio AntiBot Cloud

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.

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

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

+1.408.986.4000
www.infoblox.com

Versión: 20241030v1