infoblox®

UNA MIRADA MÁS PROFUNDA A LOS ATAQUES A DOM1NIOS SIMILAR3S

UN NUEVO ESTUDIO REVELA LOS ÚLTIMOS VECTORES DE AMENAZAS

abril 2023

DOMINIOS SIMILARES DIRIGIDOS A TODOS

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

Desde la aparición de Internet, los actores de amenazas han utilizado dominios visualmente similares para engañar a los usuarios y hacerles visitar sitios web maliciosos. Estos dominios, denominados dominios similares, son comunes en los ataques de phishing que la formación en seguridad incluye aprender a inspeccionar los enlaces para detectar su presencia.

Sin embargo, a pesar de las campañas de concienciación y los avances tecnológicos, los dominios similares representan una amenaza persistente para los consumidores y las organizaciones, que los actores adaptan continuamente. Todo el mundo es un objetivo, desde consumidores hasta gobiernos, desde grandes marcas minoristas hasta pequeños restaurantes, desde empresas tecnológicas de renombre mundial hasta empresas menos conocidas como las nuestras. En este artículo, verá que "todos son un objetivo" con ejemplos de dominios y campañas reales. Como empresa de tamaño modesto en un sector bastante especializado, también nosotros somos el objetivo.

Este informe describe el panorama actual de las amenazas con ejemplos del mundo real de todos los sectores y grupos de usuarios. Infoblox lleva años detectando dominios similares y analiza más de 70 000 millones de eventos del sistema de nombres de dominio (DNS) a diario para encontrar nuevas y posibles amenazas. Para este artículo, nos centramos en las detecciones de enero de 2022 a marzo de 2023. De más de 300 000 dominios similares, hemos seleccionado una serie que destaca los desafíos y los riesgos asociados a estos ataques.

Los dominios similares se asocian con ataques amplios y no dirigidos a los consumidores a través de correo no deseado, publicidad, redes sociales y mensajes SMS. Cada día hay miles de nuevos dominios registrados que imitan software populares, instituciones financieras y servicios de entrega de paquetes. Los ataques de phishing que tienen como objetivo robar credenciales de usuarios o infectar máquinas con malware son tan frecuentes y, a menudo, tan poco sofisticados, que se han convertido en una fuente de numerosos memes que incluyen "no puedes caer en estafas de phishing si no revisas tu correo electrónico". Aunque a menudo resultan graciosos, el phishing es una industria seria. El Grupo de Trabajo Antiphishing (APWG) informa que el phishing alcanzó un nivel récord en el tercer trimestre de 2022.[1]

[ ] ***Todos los indicadores contenidos en este documento han sido desactivados, independientemente de su condición de maliciosos o legítimos. Hemos desvirtuado los indicadores colocando corchetes alrededor de los puntos [.] y evitando así que se convierta en un enlace sobre el que se puede hacer clic.***

+70 MIL MILLONES

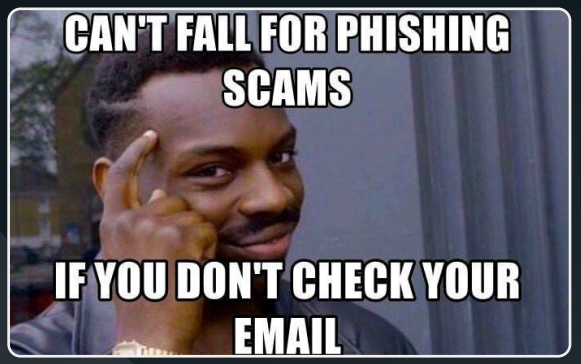
Infoblox analyses over 70 billion DNS events daily to identify new threats.

+300K

dominios similares se han seleccionado para este informe con el fin de destacar el desafío y el riesgo de estos ataques.

UN EJEMPLO DE UN MEME DE PHISHING.

Un ejemplo es este tweet de 2019.[2]



Crédito de la imagen: se desconoce el origen de este meme.

Pero los dominios similares no son solo una amenaza para los consumidores, sino que se utilizan para obtener acceso a las redes corporativas.

Las divulgaciones recientes han revelado ataques dirigidos en los que los actores maliciosos han engañado a los empleados para que proporcionaran sus credenciales de autenticación multifactor (MFA). En la mayoría de los casos, los dominios similares no solo imitaban a la empresa, sino que también incluían palabras clave MFA, lo que aumentaba aún más la ilusión de los empleados de que la conexión era segura. Descubrimos que los actores han dirigido empresas grandes y pequeñas en muchos sectores, incluidos proveedores de servicios de Internet, banca y criptomonedas, software y servicios, y compañías de seguros de todo el mundo. Estos ataques comenzaron a principios de 2022 y cobraron impulso con el tiempo.

El uso de dominios similares es rentable porque es un ataque asimétrico. Los usuarios deben estar siempre atentos para proteger sus finanzas personales y la información de sus empleadores. Los precios baratos de registro de dominios y la capacidad de distribuir ataques a gran escala dan ventaja a los actores. Los atacantes tienen la ventaja de la escala, y aunque las técnicas para identificar actividades maliciosas han mejorado a lo largo de los años, los defensores luchan por mantener el ritmo.

No sólo está prosperando el phishing por semejanza, sino que el uso de lookalikes se ha vuelto más complejo de una forma que se revela más claramente en los registros DNS. Nuestra investigación muestra que los dominios similares se están aprovechando más allá de los propósitos tradicionales de phishing y typosquatting. También se utilizan de formas no denunciadas anteriormente: por ejemplo, como servidores de nombres y para la distribución de correo mediante suplantación de identidad. Existen grandes redes resilientes que prestan servicios únicamente a dominios similares y que se dirigen tanto a consumidores como a empleados gubernamentales.

Infoblox tiene varios algoritmos para identificar dominios similares. Utilizamos una combinación de métodos, entre ellos: ver variantes de objetivos comunes en los sectores de compras, banca, software y financiero; ver variantes de dominios especificados por el cliente; y ver actores de infraestructura DNS especializados en dominios similares. Este enfoque polifacético nos brinda una amplia cobertura del panorama de amenazas.

> ***NOTA IMPORTANTE: este informe contiene una serie de ejemplos que ilustran la amplitud y profundidad de dominios similares en la naturaleza; no tienen como objetivo implicar ataques de éxito o violaciones de cualquier entidad.***

CONTEXTO

Como todos los buenos trabajos de investigación, comenzaremos con algo de contexto. Se trata sobre todo de vocabulario. Sabemos que la mayoría de los lectores se saltan la sección de contexto, por eso la hemos hecho breve.

Los lookalikes maliciosos (dominios registrados por atacantes que tienen el mismo aspecto o muy similar a un dominio conocido) son una amenaza persistente y muy conocida en el panorama cibernético. Por lo general, los lookalikes tienen aplicaciones tanto ofensivas como defensivas. En el sentido ofensivo, los lookalikes se utilizan para engañar dondequiera que pueda haber ojos humanos. Los autores utilizan imitaciones para robar dinero, obtener credenciales o acceso, recopilar información personal identificable, distribuir malware u obtener ingresos por publicidad. También se utilizan con fines políticos y para empañar la reputación de la marca. En resumen, son un medio para lograr un fin para los ciberdelincuentes. En el sentido defensivo, muchas organizaciones registran de forma proactiva dominios similares al suyo para evitar que los atacantes los reclamen y los utilicen.

Los Lookalikes tienen diferentes formas. En el espacio DNS, los dominios pueden ser:

- **Homógrafos**
- **Combosquats**
- **Typosquats**
- **Soundsquats**

Pueden ser casi indistinguibles del dominio de destino original u objetivamente bastante distintos. Gran parte del éxito de los dominios similares como vector de ataque se debe a la carga aplicada a las personas.

Como veremos, se pueden encontrar miradas en todos los elementos de un ataque, desde direcciones de remitente de correo electrónico hasta URL de phishing y comando y control de malware (C2). Aunque normalmente se asocian a los registros de direcciones (A/AAAA), hemos llegado a encontrar lookalikes utilizados para registros de servidores de nombres (NS), punteros (PTR) y nombres canónicos (CNAME). Pueden implementarse a través de correos electrónicos, SMS o mensajes de texto, sitios web comprometidos, redes de publicidad maliciosa y llamadas telefónicas. En la siguiente sección, describimos brevemente las diferentes formas de miradas y damos ejemplos de cada una.

LA CULPA ES DE LA MÁQUINA DE ESCRIBIR

De hecho, este asunto de moda se remonta a los primeros días de las máquinas de escribir. En muchas máquinas de escribir antiguas, no había teclas 0 o 1, ya que se esperaba que los mecanógrafos utilizaran O mayúscula y L minúscula para representar estos dígitos.[4]

HOMOGRAPHS (NÉE HOMOGLYPHS)

Aunque la palabra homógrafo significa "dos palabras que se escriben igual, pero no necesariamente se pronuncian igual, y tienen significados diferentes", el término homógrafo se ha utilizado durante muchos años en la literatura de investigación de seguridad para hacer referencia a "dos dominios que parecen visualmente iguales".[3] Un término más exacto es homóglyfos. Estos dominios se parecen entre sí y, en algunos casos, pueden ser casi indistinguibles. *Para mantener la coherencia con la literatura de investigación, utilizaremos el término incorrecto de homógrafo en este artículo.*

Esta forma de similitud aprovecha el hecho de que muchos caracteres del mismo juego de signos, o alfabeto, se parecen entre sí. Por ejemplo, 0 (el dígito cero) y O ("o" mayúscula) o "l" ("L" minúscula) e "I" ("i" mayúscula). Algunas fuentes acentúan aún más este aspecto. Ejemplos clásicos de esto son g0ogle.com e lnfoblox.com, en los que la "o" de Google se sustituye por un cero (0) y la "i" de Infoblox se sustituye por una "L" minúscula, respectivamente.

A medida que Internet maduró y más personas que no hablaban inglés comenzaron a conectarse a la World Wide Web, creció la necesidad de nombres de dominio internacionalizados (IDN). Un IDN es un dominio que contiene al menos un carácter en alfabeto no latino; la introducción de Unicode permitió que surgiesen tales dominios. Con los IDN llegó una nueva forma de parecido: el homógrafo de IDN. Sigue siendo un homógrαfo, pero uno que usa caracteres de otros conjuntos de caracteres o alfabetos que se parecen a él. Gabrilovich y Gontmakher demostraron el poderdelos IDN hoɱógrafos en su artículo de 2002 "The Homograph Attack" (El ataque homógrafo). Los autores registraron un parecido del dominio auténtico de Microsoft microsoft[.] com que contenía las letras cirílicas "c" y "o".[5] El resultado final es un dominio www.microsoft[.] com que es visualmente indistinguible del dominio auténtico de Microsoft.

El Consorcio Unicode ha publicado una herramienta que muestra la gran cantidad de caracteres confundibles disponibles para una cadena determinada.[6] La cadena “hola” tiene 684 variaciones con caracteres Unicode; para una cadena como “infoblox”, el número aumenta a más de 2,2 billones de variaciones. Algunas variaciones son menos efectivas para un lookalike que otras. Por ejemplo, el Consorcio Unicode enumera "৯" (dígito cinco árabe-índico extendido) como un carácter potencialmente confuso para "o" (letra minúscula latina "O").

Claramente, inf৯bl৯x[.]com com no es un lookalike muy efectivo; pero, ¿puede detectar la diferencia, cuando se muestra en la fuente Arial de uso común, entre el dominio propio {infoblox[.]com} y {infoblox[.]com} (contienen una “i” minúscula bielorrusa o ucraniana y una letra minúscula armenia “vo”, escrita como “n”)? Nosotros tampoco.

TYPOSQUATS

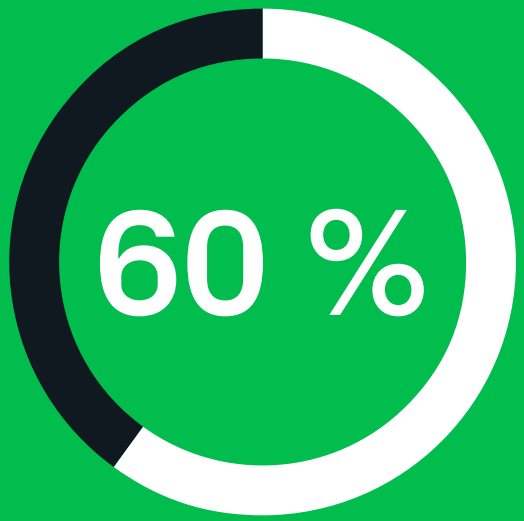
Los dominios typosquat sacan provecho de los nombres de dominio populares y de los errores tipográficos que cometen los usuarios o que se producen al escribir con teclados estropeados. Este término suele estar asociado a dominios registrados, pero no utilizados, con el fin de dibujar dinero publicitario. Por ejemplo, uno de los autores intentó recientemente pagar el alquiler a través del portal online de su grupo de gestión inmobiliaria, alojado en appfolio[.]com. (una conocida empresa de software que ofrece soluciones SaaS a grupos de administración de propiedades y propietarios). En lugar de eso, pasaron de largo y casi visitaron appfollio[.]com,que se registró en 2013 pero está parado actualmente.

Curiosamente, otro aparente dominio typosquat para Appfolio, apfolio[.]com, parece ser propiedad de Appfolio. Redirige al dominio correspondiente y tiene el mismo registrante, organización registrante y registrador, y se registró justo un mes después del dominio legítimo appfolio[.]com. Este es un ejemplo del uso defensivo de los parecidos. Por desgracia, los agentes malintencionados tienen la sartén por el mango, ya que hay demasiadas posibilidades para que las organizaciones registren todas las variantes parecidas.

Los typosquats se perciben principalmente como un método de monetización, pero pueden tener un propósito nefasto. Aunque se utilizan para vender anuncios de terceros o para vender al propietario legítimo del dominio, también se pueden utilizar para programas de marketing de afiliados "BlackHat" y como dominios de malware C2, como se mostrará más adelante. Las marcas y las empresas sí disponen de protección civil contra la "typosquatting" en virtud de la Ley de Protección de los Consumidores contra la "typosquatting". Debido a estas amenaza de acciones legales, la typosquatting se considera una forma de monetización de “sombrero negro” en la comunidad de cambio/estacionamiento de dominios, y los flippers de dominios serios como iGoldrush recomiendan no usar typosquatting con fines de lucro.[7]

EJEMPLOS DE TYPOSQUAT

gikthub[.]com
5whatsapp[.]com
Hdfcbank[.]vip
royalbsank[.]com
sportybet[.]city
bamgkokbank[.]com
1337x[.]asia
moneycont5rol[.]com



de dominios de combosquatting abusivos están activos durante más de 1000 días

de dominios de combosquatting abusivos aparecen en al menos una lista de bloqueo pública 100 días después de las resoluciones iniciales

COMBOSQUATTING

Combosquatting es una forma de lookalike que combina nombres populares de marcas o empresas con otras palabras clave. Términos como soporte, ayuda, seguridad y correo son comunes. Considere, por ejemplo, wordpresssupport[.]ru, wordpresssupport[.]store y wordpress-security[.] cloud. Todos estos dominios están alojados en la misma dirección IP con sede en Rusia y se parecen a WordPress, el popular software de contenido web. La inclusión del apoyo y la seguridad en el dominio indica que están destinados a los usuarios de WordPress. Pueden usarse para recopilar credenciales con el fin de secuestrar sitios de WordPress o recopilar detalles de pago e información de identificación personal (PII).

Además de generar dominios combosquat por sí mismos, los autores también tienen la capacidad de usar algoritmos de generación de dominios de diccionario (DDGA) para crear parecidos. En segundos, se pueden generar miles de dominios candidatos para multitud de marcas o empresas. Por suerte, el algoritmo puede crear dominios candidatos con las palabras clave adecuadas para que el dominio sea efectivo. La comunidad de usuarios de Steam, una de las principales plataformas de juegos, es un objetivo habitual para los actores que utilizan DDGA combosquat. Algunos ejemplos de dominios dentro de un conjunto observado recientemente son: steamcommiity[.]com[.]ru, steamcommucnity[.] com[.]ru steamcommunityjp[.]top y steamcommunityiq[.]top. Observe la superposición entre typosquatting y combosquatting en este conjunto de dominios.

Kitsin et al. realizaron un estudio longitudinal de combosquatting en 2017, donde analizaban alrededor de 468 mil millones de registros DNS (procedentes de conjuntos de datos activos y pasivos), y encontraron resultados inquietantes:

- **Los dominios combosquat son 100 veces más frecuentes que los dominios typosquatting**
- **El 60 % de los dominios combosquatting abusivos están activos durante más de 1000 días**
- **El 20 % de los dominios combosquatting abusivos aparecen en al menos una lista de bloqueo pública 100 días después de las resoluciones iniciales**
- **La resolución de dominios de combosquatting aumentó año tras año[8]**

Coincidimos con la conclusión de los autores sobre la prevalencia de los dominios combosquat. Encontramos más dominios combosquat que typosquats puros u homoɡrafos puros (IDN o de otro tipo) a través de nuestros análisis.

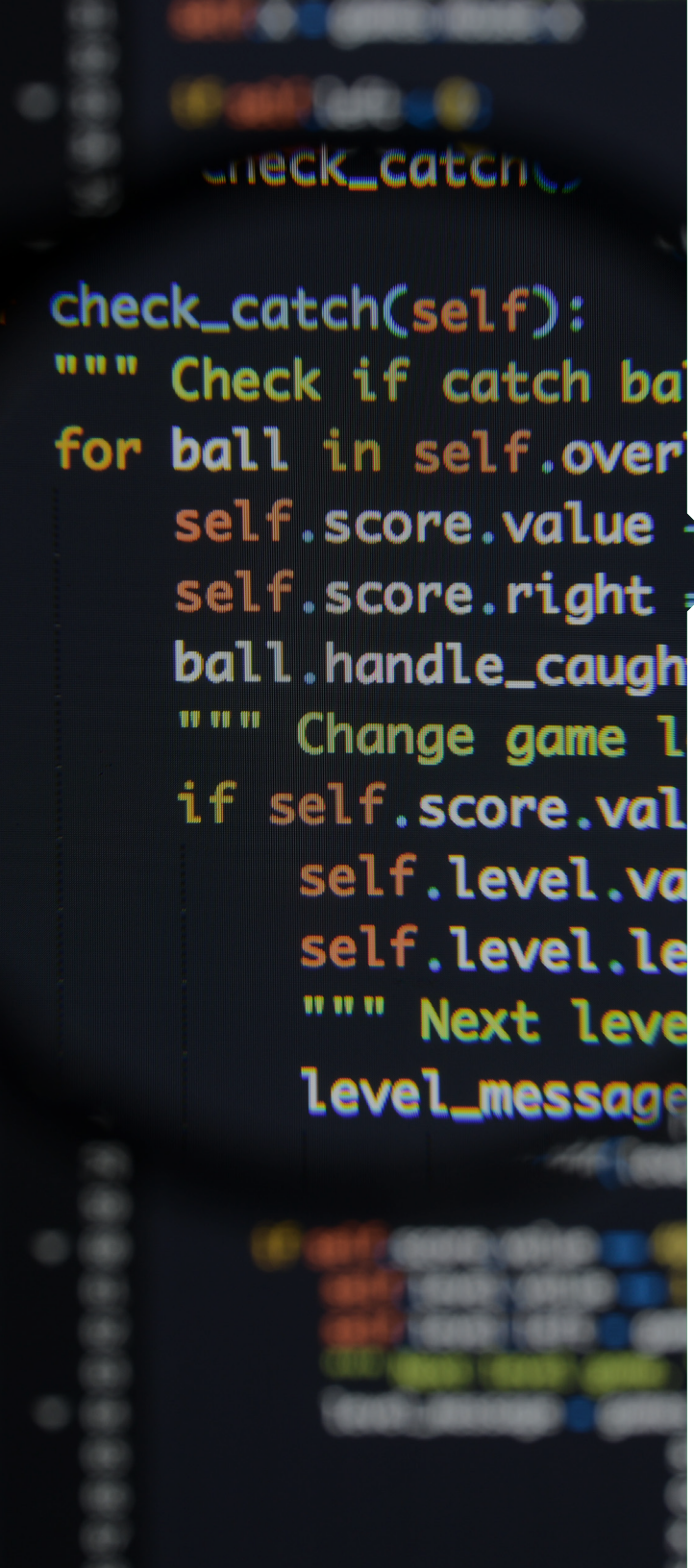
SOUNDSQUATTING

Los dominios Soundsquat aprovechan el uso de homófonos, palabras que suenan igual pero se escriben diferente. Soundsquatting es la forma de lookalike identificada más recientemente y apareció por primera vez en la literatura en 2014.[9] Soundsquatting ha recibido más atención por parte de los investigadores recientemente debido a la proliferación de parlantes inteligentes al estilo Alexa, Siri y Google Voice.[10] Los dominios Soundsquat se superponen con otros tipos de dominios similares, en el sentido de que pueden sonar y verse similares. Hemos descubierto que los dominios de soundsquatting puros, es decir, aquellos que no parecen visualmente similares pero suenan parecidos, son raros; por lo general, estos dominios también se pueden encontrar mediante técnicas de similitud basadas en texto.

Es importante señalar que los lookalikes en la naturaleza no suelen encajar en cubos ordenados como los que hemos expuesto aquí.Se utiliza una combinación de formas para maximizar la eficacia de un dominio similiar. Muchos de los dominios combosquat que vemos tienen elementos de typosquats y homógrafos (IDN o de otro tipo). Los typosquats utilizan elementos de homógrafos, los soundsquats utilizan elementos de typosquats, y así sucesivamente. El resultado final es un panorama de amenazas asimétricas en el que los atacantes pueden dejar a los defensores boquiabiertos.

SOUND EL ATAQUE

La prevalencia del soundsquatting ha despegado con la llegada de la tecnología activada por voz como Alexa, Siri y Google Voice.



OTRAS FORMAS DE LOOKALIKES

Aunque el enfoque de este documento está en dominios similares y su papel en el panorama actual de amenazas, existen otros tipos de miradas que pueden explotar a los usuarios vulnerables. Un ejemplo notable de esto se encontró recientemente en los paquetes Python PyPi.

https://infosec.exchange/@tweedge@cybersecurity.theater/109846797159938702

Los gestores de paquetes de los lenguajes de programación populares, como Python, tienen los mismos puntos débiles que los dominios. Cualquier persona puede subir un paquete con cualquier nombre (siempre y cuando ese nombre no esté ya en uso) que contenga un código que pueda o no estar libre de riesgos de seguridad. En 2016, el investigador de seguridad Nikolai Tschacher utilizó esta forma de ocupación tipográfica para obligar a más de 17 000 servidores distintos a ejecutar código arbitrario.[11] Después, en 2021, el investigador de seguridad Alex Birsan tomó la idea de Tschacher y la amplió, acuñando el término "confusión de dependencias".[12]

Birsan encontró los nombres de paquetes privados e internos de las principales empresas a través de varias fuentes abiertas. Esto incluía explorar el código fuente en sitios web, buscar paquetes en GitHub o incluso encontrar nombres de paquetes en foros públicos. Más tarde, cargó paquetes con el mismo nombre que los paquetes internos privados a los gestores de paquetes públicos. Finalmente, Birsan utilizó canalizaciones CI/CD automatizadas, “confundiendo” los paquetes públicos con los privados e internos. En lugar de importar e instalar los paquetes privados, las canalizaciones automatizadas encontraron e importaron los paquetes públicos de Birsan. Birsan utilizó entonces la exfiltración de DNS para notificarle que se había ejecutado su código arbitrario, y no el paquete privado previsto. La técnica de imitación de Birsan le permitió penetrar en 35 organizaciones, a veces pocas horas después de subir sus paquetes.

Independientemente del tipo de Lookalike o del campo en el que se utilice un lookalike, los lookalikes son una amenaza persistente. Parte del reto de estudiar los lookalikes es que son indefinidos: hay más posibilidades de las que se pueden calcular y todo es un objetivo. En las siguientes secciones, mostramos ejemplos específicos de estas diversas formas de lookalikes en la naturaleza, incluidos los objetivos, los métodos de implementación, la infraestructura, por qué son efectivos, los desafíos y las soluciones de Infoblox al problema.

TODOS SON UN OBJETIVO

Creemos que encontrará al menos un objetivo sorprendente en nuestros ejemplos.

Una de las conclusiones más impactantes de nuestra revisión de dominios similares en DNS fue que todo el mundo es un objetivo: encontramos dominios similares para todos los objetivos esperados, pero también para empresas y servicios más pequeños. Los agente malintencionados utilizan estos dominios para aprovecharse de las personas en el trabajo y en casa.

Como ha observado recientemente Akamai, la mayoría de las campañas similares solo reciben prensa una vez que se ve afectado un objetivo grande.[13] Nuestro objetivo es arrojar luz sobre esos destinatarios infravalorados y pasados por alto junto con los destinatarios "típicos". Aquí se muestran algunos ejemplos selectos para demostrar este punto, pero también destacaremos el impacto en diferentes industrias y el uso de diversas metodologías con más detalle más adelante.

¡NOS ATACAN!

Infoblox es una empresa de tamaño modesto con menos de 2000 empleados en todo el mundo.

Si bien tenemos una gran participación en el mercado de DNS, Dynamic Host Configuration Protocol (DHCP) y administración de direcciones IP (IPAM), conocidos colectivamente como DDI, esta industria es bastante específica e Infoblox no es un nombre conocido. Uno podría sorprenderse de que los autores maliciosos fueran siquiera conscientes de nosotros, y mucho menos de que se dirigieran activamente a nosotros con dominios parecidos. Sin embargo, encontramos muchos dominios diseñados para engañar tanto a nuestros empleados como a nuestros clientes. Lookalikes de servicios internos, incluido nuestro portal de beneficios, así como los nombres de nuestros productos se han registrado el año pasado.

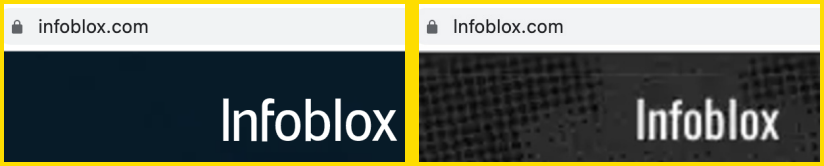


Figura 2. Comparación de logotipos entre el sitio web oficial de infoblox[.]com (L) y el Infoblox[.]com (R)

Algunos dominios registrados que no son propiedad de Infoblox incluyen:

Homógrafo **Infoblox[.]com**	El uso de una “L” minúscula para hacerse pasar por una “i” mayúscula se registró en julio de 2022 y, aunque se ofrece a la venta, el sitio muestra en la esquina superior izquierda una representación que es casi indistinguible de la de nuestro sitio web corporativo. *Vea una comparación en la Figura 2.*
Typosquat **infobloxbenifits[.]com**	Este dominio se registró en China en abril de 2022 y es un leve error tipográfico de nuestro portal de beneficios para empleados. Este dominio está aparcado actualmente con Bodis.
TLD Squat **infoblox[.]info**	En agosto de 2022 se registró un dominio de nivel superior diferente, o TLD, a través del registrador Sav[.]com, del que se ha abusado mucho. Está aparcado en dan[.] com, que permite a los usuarios vender dominios.
Combosquat **infobloxgrid[.]com**	Un combosquat similar a nuestro producto local estrella utilizado por miles de clientes en todo el mundo. Nuestra tecnología patentada Grid permite a los administradores de red combinar diversas aplicaciones de red en un solo sistema. Este dominio también está disponible en dan[.] com y se registró en abril de 2022.
Combosquat **infoblox-updater[.]com**	Un ejemplo de la técnica de utilizar palabras de software comunes dentro del dominio como "update" o "support". En este caso, a un cliente se le puede engañar para que se conecte con un sistema falso pensando que estaba relacionado con las actualizaciones del sistema Infoblox. Con frecuencia se aprovechan nombres o productos de empresas de tecnología para este tipo de dominio combosquat, que podría usarse como dominio de phishing o como malware C2. Otros ejemplos incluyen dev[.]gitlabs[.]me y jira[.] atlas-sian[.]net, ambos utilizados por el actor de amenazas persistentes avanzadas (APT) Iron Tiger en su malware SysUpdate.[14]

Además de dirigirnos a pequeñas empresas tecnológicas como la nuestra, hemos visto una amplia gama de lookalikes que son variantes engañosas de restaurantes, firmas de abogados y otras pequeñas empresas.

Además, un solo autor puede utilizar desde marcas conocidas hasta pequeñas empresas como señuelos. Un autor al que Infoblox ha estado rastreando durante algún tiempo creó dominios parecidos para el restaurante Cotenna de Nueva York y copió su sitio web, presumiblemente para atraer a los visitantes a hacer reservas en línea con sus tarjetas de crédito.[15] El sitio cotenna[.]nyc se registró en abril de 2022 y es similar al sitio web del restaurante cotenna[.]com. Este mismo autor tiene dominios similares dirigidos a grandes empresas de redes sociales como Twitter.

En las secciones que siguen, profundizaremos en las industrias que son objetivo más frecuente hoy en día, así como en algunas de las muchas formas en que los dominios pueden utilizarse para un ataque con éxito. Dado que todo el mundo es un objetivo, destacaremos aquellas áreas en las que hemos observado una mayor actividad maliciosa, basándonos en una revisión de 300 000 dominios similares.

DOMINIOS SIMILARES DIRIGIDOS A TODOS

amėricafirst[.]com
ınstagram[.]dev,
caterpillarespaña[.]com
steamcommunltly.net[.]ru
boatairbuds[.]in
secure1-scotiabank[.]com
saveukraine[.]xyz
expressvpn-app[.]com

SE DIRIGEN A LOS EMPLEADOS

Hasta hace poco, muchas corporaciones sentían que el uso de la autenticación multifactor (MFA) protegía sus redes internas de los ataques de phishing.

Pero a principios de 2023, Coinbase reveló que sus empleados habían sido víctimas de ataques de suplantación de identidad selectivos que utilizaban dominios similares para el inicio de sesión interno de la MFA de la empresa.
A esta revelación le siguieron rápidamente informes que lo corroboraban de otras empresas que habían sido objeto de ataques similares. Basándonos en los informes de las víctimas, sabemos que los autores maliciosos enviaron a los empleados mensajes SMS, así como correos electrónicos, instándoles a iniciar sesión en los sistemas internos. En algunos casos, también se realizaron llamadas telefónicas, durante las cuales el atacante proporcionó un nombre de dominio para que el empleado lo visitara en su navegador web. Los atacantes utilizaron técnicas de intermediario (AitM) para hacer creer a los empleados que estaban interactuando con la red real de la empresa. A los empleados se les pedía un código MFA, que era captado por el atacante y utilizado para acceder a los sistemas internos.

Microsoft había advertido en julio de 2022 de que más de 10 000 organizaciones eran objetivo de ataques AitM diseñados para robar las credenciales MFA de los usuarios en tiempo real.[16] Esos ataques eran específicos al uso de la autenticación de Outlook 365, pero Microsoft informó además en febrero de 2023 de que un kit de phishing que permitía los ataques MFA estaba a la venta en julio de 2022 y era ampliamente utilizado.[17] Otras empresas, incluida Twilio, habían revelado ataques similares en el verano de 2022, pero la amplitud del ataque no fue bien publicitada hasta las revelaciones de Coinbase.[18]

Para investigar este incidente, realizamos un análisis retrospectivo de dominios similares que imitaron la autenticación multifactor utilizando palabras clave como "mfa," "okta" y "2fa". Nuestra investigación encontró una amplia gama de objetivos y un claro repunte de la actividad a partir de julio de 2022, aunque hubo un número significativo de dominios similares utilizados para estos ataques a principios de año. Más de 1600 dominios contenían una combinación de características similares corporativas y MFA. Los objetivos iban desde las grandes empresas señaladas, como Coinbase, Reddit y Twilio, hasta grandes bancos, empresas de software, proveedores de servicios de Internet, entidades gubernamentales y plataformas de juegos de todo el mundo. También fueron objeto de ataques, pero no se informaron lo suficiente, empresas de tecnología más pequeñas, tiendas de comestibles y minoristas.

+10 000 ORG

En julio de 2022, Microsoft advirtió que más de 10 000 organizaciones eran objeto de ataques AitM diseñados para robar credenciales MFA de los usuarios en tiempo real.

+1600

Nuestra investigación descubrió que más de 1.600 dominios contenían una combinación de rasgos corporativos y similares a los de MFA.

Como ejemplo de objetivos menos conocidos, varios dominios similares a la MFA imitaban al Consejo Coordinador de Electricidad Occidental (WECC).
El WECC promueve la fiabilidad del sistema eléctrico a granel para una gran parte de los Estados Unidos occidentales. Los lookalikes incluían wecc-okta[.]org, wecc-oktc[.]org y wecc-okta[.]com. Todos se registraron en febrero de 2023 y compartieron una dirección IP.

Otro ejemplo sorprendente es Feldman Auto Group, que consta de varios concesionarios de automóviles en los Estados Unidos.
Si bien la compañía tiene una relación de marca con el actor estadounidense Mark Wahlberg, por lo demás es una empresa de tamaño moderado con 18 ubicaciones en el medio oeste.[19] Un MFA similar a este dominio, feldmanauto-okta[.] com, se registró a finales de enero de 2023.

Algunos de los objetivos de la empresa de los lookalikes de la MFA son más inciertos.
El dominio frb-okta[.]com muestra un aviso de inicio de sesión con un anodino logotipo FRBOkta que podría ser el Banco de la Reserva Federal, First Reserve Bank, o un símil de un sitio como la empresa de ropa polaca Farbokta.[20] En muchos casos, no podemos estar seguros de cuál era el objetivo, y el kit de phishing puede haber estado activo durante poco tiempo. *Hemos incluido una captura de pantalla del inicio de sesión en la Figura 3 para que pueda adivinar por sí mismo.*

Estos ataques AitM también se utilizaron contra los consumidores en 2022, en particular los de la comunidad de jugadores que utilizan la MFA para proteger sus compras dentro del juego.
En un caso conocido por los autores, la víctima fue atraída por visitar un sitio web de una transmisión en directo de Twitch de un popular juego en línea. Tras introducir sus credenciales MFA experimentaron un breve ataque de denegación de servicio (DoS) contra su red doméstica, que provocó un corte de Internet durante varios minutos. Cuando pudieron regresar a su cuenta de juego, le habían robado todas sus compras. *Podríamos pensar en los jugadores como adolescentes que viven en el sótano de sus padres, pero la cantidad de dinero que se gasta en compras dentro de la aplicación hace que los juegos y sus jugadores, desde Roblox hasta Counter-Strike, sean un objetivo lucrativo.*

FRBOKTA.COM MFA LOOKALIKE

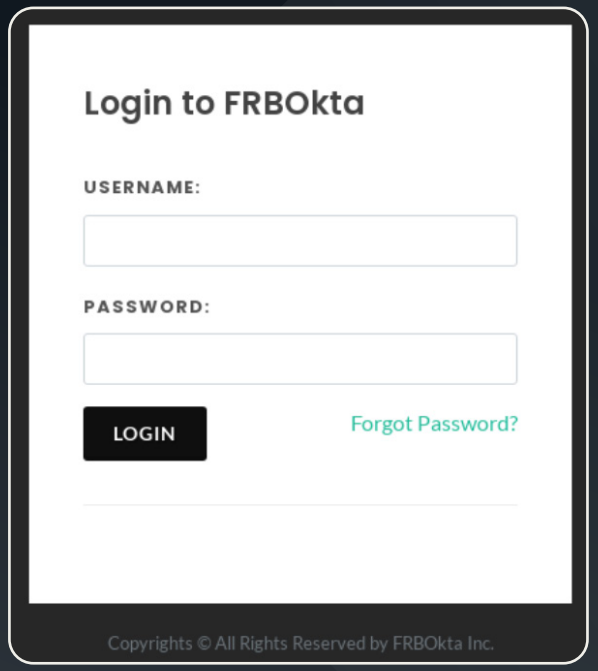


Figura 3. El sitio web de frb-okta[.]com muestra una página de inicio de sesión anodina con una referencia a FRBOkta. Crédito de imagen: URLScan.[21]

PÁGINA SIMPLE DEL MINISTERIO TURCO

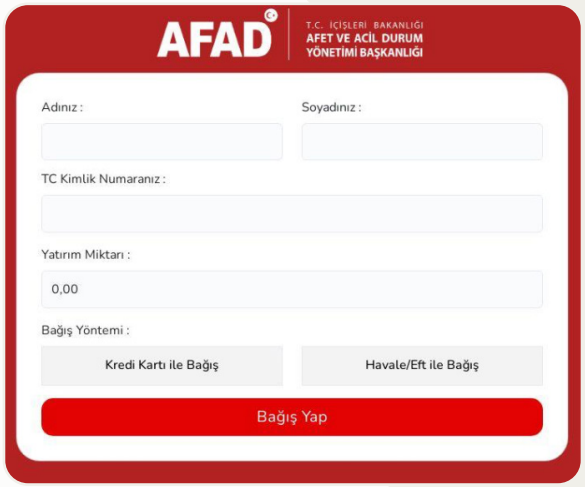


Figura 4. Lookalike de AFAD afadestek[.]net Créditos de imagen: DomainTools.

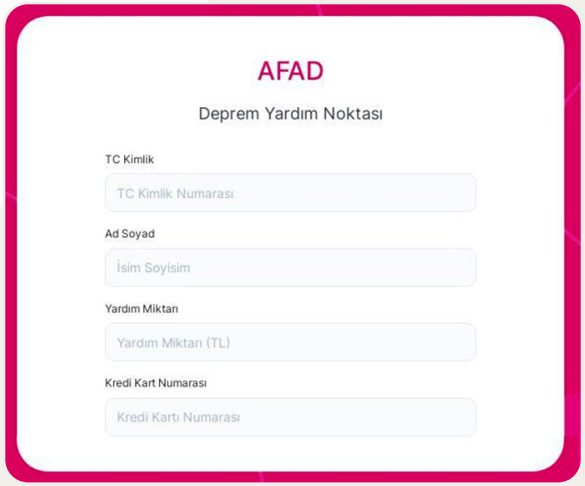


Figura 5. Dominio similar de AFAD afadbagislari[.]net Crédito de la imagen: DomainTools.

SE DIRIGEN A LOS BENEFACTORES

Los estafadores que buscan robar dinero suelen ser los "primeros intervinientes" cuando se trata de utilizar eventos y desastres mundiales para ganancias mal habidas.

Infoblox ha descubierto que los estafadores se aprovechan rápidamente de cualquier suceso de las noticias, como crisis de salud como la COVID-19 o la invasión rusa de Ucrania. Por desgracia, 2023 provocó una crisis humanitaria con el terremoto turco-sirio deprincipios de febrero.[22] Tras el primer terremoto del 6 de febrero, varios dominios fraudulentos intentaron imitar sitios web de la Autoridad de Gestión de Desastres y Emergencias (AFAD) del Ministerio del Interior turco. Estos dominios aprovecharon 'AFAD' en el nombre de dominio completo, intentando parecerse al dominio legítimo afad[.]gov[.]tr. Los siguientes ejemplos son dominios que se registraron recientemente y, aunque tienen un nombre de dominio completo (FQDN) largo, todos comienzan con 'AFAD'.

El uso de FQDN más largos ofrece a los estafadores más permutaciones del dominio legítimo para su uso en múltiples campañas temáticas de AFAD:

- **afad-kizilay[.]yardim-yap[.]net**
- **afad-kizilay[.]yardimbagis[.]net**
- **afad-online-odeme-bagis[.]net**
- **afadtr[.]bagislama[.]net**

Además de la comercialización, algunos de estos sitios utilizan el logotipo legítimo de AFAD para ayudar a engañar a los visitantes a donar a los sitios. Por ejemplo, el sitio fraudulento afadestek[.]net fue registrado el 7 de febrero, y mostraba un diseño web similar al del sitio legítimo turco de AFAD, como se muestra en *la figura 4*. Según la traducción automática, parece recaudar donativos mediante tarjeta de crédito o giro postal a través de transferencia electrónica de fondos, además de recoger IIP como nombres y apellidos y números de identidad nacionales.

Otros dominios fraudulentos no se molestaron en usar el logotipo oficial de la AFAD y se crearon rápidamente para maximizar la cantidad de dinero que podían obtener de los donantes. Dos ejemplos son afadbagislari[.]net y afadyardimyap[.]net, ambos alojados en la misma dirección IP. La infraestructura dedicada para lookalikes es común y la analizaremos con más detalle más adelante. Ambos sitios tienen el mismo diseño y contenido, como se muestra en *la Figura 5*, y solicitan donaciones para la ayuda tras el terremoto mediante pagos con tarjeta de crédito.

SE DIRIGEN A LAS CRIPTOMONEDAS

Además de los estafadores que buscan ganar dinero rápido, los lookalikes se utilizan mucho para robar credenciales.

Un dominio similar es probablemente en lo que piensa la mayoría de la gente cuando imaginan un sitio web genérico de "phishing" que intenta obtener credenciales de los usuarios. Con el aumento de la popularidad de las criptomonedas, los atacantes apuntan a estos servicios financieros, incluidos mercados, billeteras e intercambios. Encontramos una serie de imitaciones muy convincentes para el popular intercambio Coinbase con sede en EE. UU. Uno de esos sitios se muestra en *la Figura 6*.[23]

Los dominios de la tabla siguiente, por ejemplo, se registraron en enero de 2023:

Tabla 1. Ejemplos de dominios similares de intercambio de criptomonedas de Coinbase.

securefinancialcoinbase[.]com	reconfirminfocoinbase[.]com
secureaccountreverify-coinbase[.]com	reconfirmaccount-coinbase[.]com
secure4-coinbase[.]com	kyc-reverifycoinbase[.]com
secure2reconfirm-accountcoinbase[.]com	ap-coinbase[.]com
secure2financial-coinbase[.]com	accountupdate-financialcoibase[.]com
secure2-financialcoinbase[.]com	2farecoverycoinbase[.]com
secure-2faupdatecoinbase[.]com	recovery-financialcoinbase[.]com
2fa-accountupdatecoinbase[.]com	2fa-updatecoinbase[.]com

Con el crecimiento de los tokens no fungibles (NFT), cuyas operaciones superaron los 2000 millones de dólares en febrero de 2023, los actores se apresuraron a ir más allá de las criptomonedas tradicionales en sus esfuerzos por robar dinero a los inversores.[24] Por ejemplo, el mercado de Blur abrió sus puertas en octubre de 2022 y el token Blur se lanzó unos meses después, lo que impulsó una inversión récord en NFT desde mayo de 2022.[25] Empezamos a ver lookalikes de Blur poco después del lanzamiento del producto, y luego vimos un aumento drástico de los parecidos a medida que la plataforma ganaba popularidad.

COINBASE LOOKALIKE

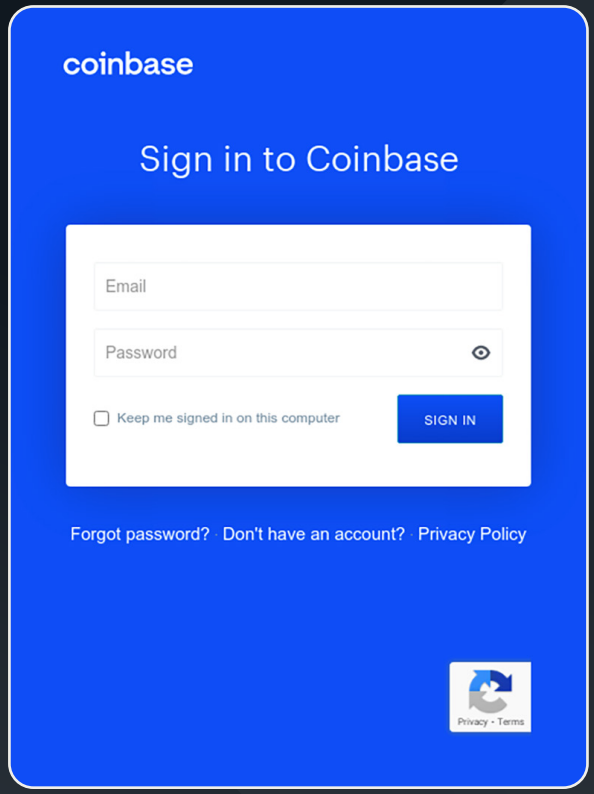


Figura 6. Lookalike de coinbase a click-coinbase[.]com
Crédito de la imagen: DomainTools.

LOOKALIKE BLUR NFT

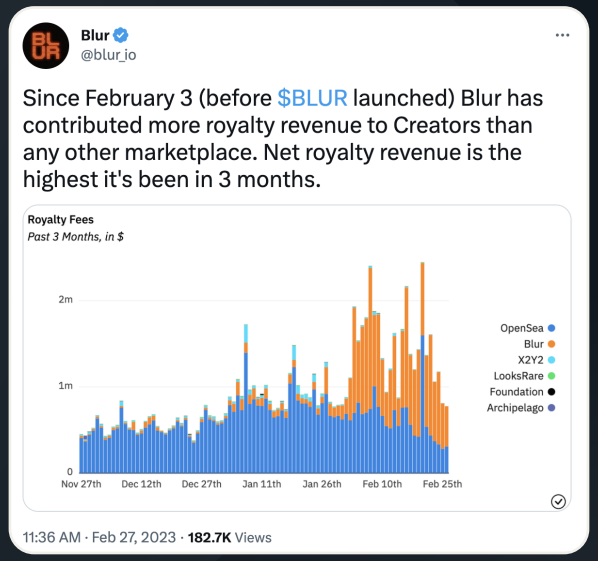


Figura 7. El mercado de Blur NFT es uno de los principales impulsores de las operaciones de NFT de 2000 millones de dólares en febrero de 2023.[26] Image credit: Infoblox

En el período previo al lanzamiento del Blur Token el 14 de febrero de 2023, vimos un aumento de cinco a seis veces en la cantidad de imitaciones relacionadas con Blur. Incluso con la cantidad cayendo en marzo de 2023, este patrón demuestra la voluntad de los autores de mantenerse al día con las tendencias en el mundo de las criptomonedas para estafar rápidamente.

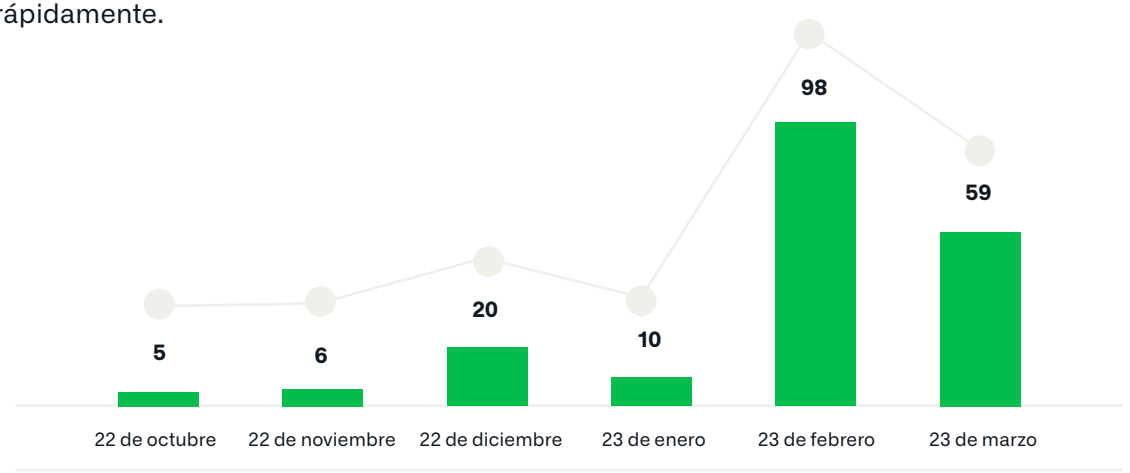


Gráfico 8. Aumento drástico de los miradores relacionados con Blur desde el anuncio del mercado en octubre de 2022.

Infoblox rastrea a múltiples actores que se especializan en imitaciones relacionadas con criptomonedas. Estos autores se dirigen a todas las principales entidades del mercado, incluidos Blur y su competidor Yuga Labs, propietario de ApeCoin y la popular NFT Bored Ape Collection. En la siguiente tabla, proporcionamos una pequeña muestra de estos dominios. Las técnicas utilizadas por estos actores incluyen cambios simples en el dominio de nivel superior (TLD), la adición de una sola letra y nombres de dominio Unicode, que pueden ser particularmente difíciles de reconocer. Observe que en la siguiente tabla hay tilde sobre la “i” en apecoíns[.]com. En DNS, este dominio se parece a xn--apecons-cza[.] com, que es algo difícil de reconocer como parecido, pero en un navegador web sería prácticamente indistinguible del original.

Tabla 2. Ejemplos de dominios similares del token Blur y Yuga Labs.

Dominios similares a Blur [blur.io]	**Dominios similares a Yuga Labs [yuga.com]**
blurclaim[.]com	yugaslabs[.]com
blurdrop[.]com	apecoíns[.]com
blurnft[.]pw	apecoinstake[.]world
blur-nft[.]org	yugas[.]app
blur-coin[.]com	ape-claim[.]com

También hay menos lookalikes relacionados con criptomonedas tradicionales que utilizan YouTube como vector para atraer objetivos a sus dominios.

Estos planes comienzan con actores de amenazas que lanzan suplantación de identidad a populares creadores de YouTube con ofertas de patrocinio falsas que parecen estar relacionadas con productos legítimos.[27]
Los correos electrónicos piden al creador que descargue y abra un archivo supuestamente relacionado con la oferta de patrocinio, como una copia del software que se promociona o un archivo PDF con un contrato de patrocinio.[28] En realidad, estos archivos son cargas de malware que, al abrirse, roban las cookies de sesión del navegador de la víctima. Las cookies robadas permiten que el atacante obtenga acceso a la cuenta de YouTube de la víctima, incluso si la autenticación multifactor está habilitada.

Una vez que el atacante tiene acceso a la cuenta de YouTube del creador, intenta ocultar el hecho de que el canal ha sido pirateado cambiando su nombre y su foto de perfil para que coincida con el tema de su ataque, que a menudo es algo relacionado con Elon Musk o una de sus empresas.[29]
El atacante también puede borrar u ocultar los vídeos existentes del canal para cubrir aún más sus huellas. El atacante comienza a transmitir una versión editada de un video relacionado con la criptomoneda, como el discurso Ark Invest de Elon Musk, para atraer a los suscriptores existentes del canal.

Estos vídeos editados incluyen una superposición de texto que dirige a los usuarios a visitar el dominio similar relacionado con criptomonedas del atacante, y también se incluye un enlace al dominio en la descripción de la secuencia.
Los propios dominios son estafas estándar "duplique su dinero" que invitan a las víctimas a enviar una determinada cantidad de criptomonedas a una dirección de billetera específica con la promesa de que recibirán el doble de esa cantidad. En estos ataques, el propósito del dominio similar es mejorar la creencia de la oferta al combinar su tema con el video editado y el canal de YouTube de nueva marca.

LOOKALIKE DE TESLA

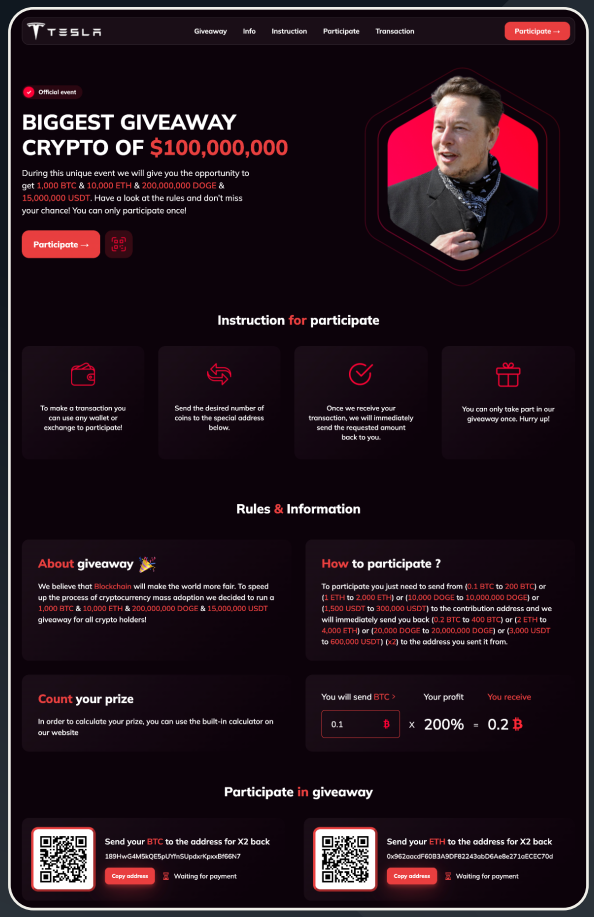


Figura 9. El dominio similar de Tesla relacionado con criptomonedas tesla-online[.]net pide a los usuarios que envíen criptomonedas a direcciones específicas para recibir el doble a cambio. Crédito de imagen: Infoblox.

REDES SOCIALES Y MÓVILES

Las plataformas de redes sociales, como Instagram y Twitter, junto con las principales marcas como Apple, también son objetivos populares de phishing dominios similares.

Cada marca y servicio popular se dirige continuamente a estos ataques, pero usaremos solo algunos ejemplos de estas tres marcas como una ilustración de la amenaza actual. La recopilación de credenciales no es nada nuevo; antes de que aparecieran plataformas de identificación universal y de redes sociales como Apple ID, los agentes malos intentaban acceder a tu cuenta de correo electrónico. Sin embargo, con lo profundamente entrelazadas que están ahora las redes sociales y las plataformas de identificación universal con nuestras vidas, estos imitadores suponen una amenaza persistente.

Los actores de amenazas perseguirán las cuentas de redes sociales de cualquier persona, no solo las cuentas de influencers y famosos. Hay muchos parecidos a Instagram: algunos combosquats, otros homógrafos. A menudo, esos dominios aparecían en grupos de dominios registrados simultáneamente, lo que sugiere que formaban parte de una campaña coordinada creada mediante una DDGA. Todos los ejemplos de abajo forman parte de una colección de Instagram que combina la marca con palabras como ayuda y comentarios.

Tabla 3. Ejemplos de Instagram admiten dominios similares.

help-instagram-notice[.]com	help-instagram-about[.]com
feedback-instagram[.]com	help-Instagram-notice[.]com
help-Instagram-about[.]com	help-Instagram-notice[.]gq

El contenido de estos dominios afirma que el usuario ha violado las reglas de derechos de autor de Instagram y le pide al usuario que ingrese su nombre de usuario para apelar el veredicto; *véanse las Figuras 10 y 11.*

LOOKALIKE DE INSTAGRAM

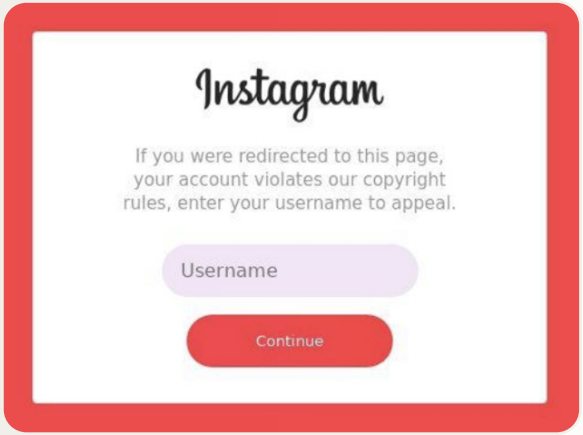


Figura 10. El lookalike de Instagram help-Instagram-notice[.]com muestra una llamada a la acción por infracción de derechos de autor. Crédito de la imagen: DomainTools.[30]

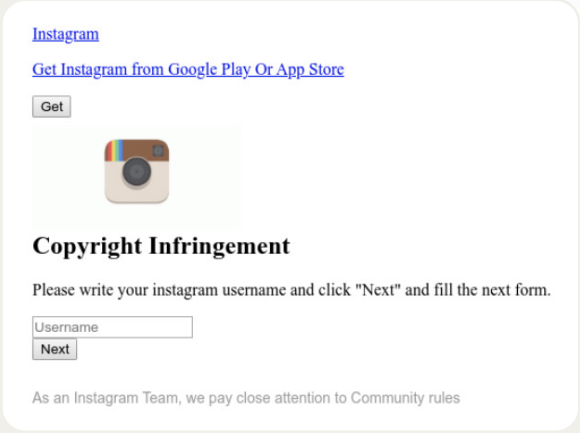


Figura 11. Lookalike de Instagram help-instagram-about[.] com, que muestra otra llamada a la acción por infracción de derechos de autor. Crédito de imagen: URLScan.[31]

LOOKALIKE DE TWITTER

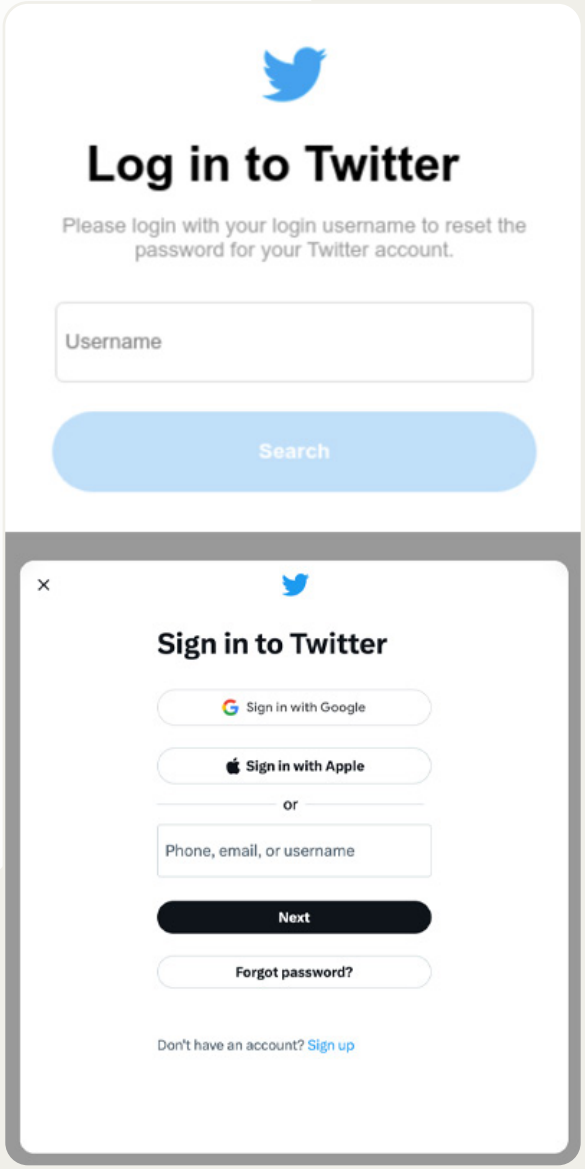


Figura 12. Convincente portal de restablecimiento de contraseña en Twitter help-twitter-centre[.]net. La imagen de phishing está en la parte superior, la legítima está en la parte inferior.[32]

Otros imitadores de Instagram apuntan a la codiciada "marca de verificación azul" (el enfoque de Instagram para la verificación como figura pública), usando una "L" minúscula en lugar de una "i" mayúscula. Irónicamente, Instagram introdujo la marca de verificación azul para personalidades o empresas conocidas como una forma de combatir la suplantación de identidad. *No deje de lado a los malos actores que utilizan imitaciones dirigidas a soluciones anti-lookalike.*

Algunos ejemplos son:

Tabla 4. Ejemplos de dominios similares de verificación de Instagram.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Al hacer un seguimiento de los lookalikes de Instagram, descubrimos que los actores no ponían todos los huevos en la misma cesta de las redes sociales.

También se alojaron lookalikes de Twitter junto con los lookalikes de "infracción de derechos de autor" de Instagram. Estos looka1iks de Twitter eran dominios combinados que suplantaban las credenciales de los usuarios, y las páginas de destino parecen ser un portal legítimo de restablecimiento de contraseñas; *consulte la Figura 12.*

Además de los lookalikes de las redes sociales, durante nuestra investigación vimos a menudo lookalikes de iCloud, el servicio en la nube de Apple que ofrece almacenamiento en la nube y sincronización entre dispositivos Apple. Estos dominios aprovecharon un número relativamente pequeño de palabras clave; observamos con mayor frecuencia "apple", "findmy", "id" e "icloud". No faltaron dominios similares relacionados con Apple.

A continuación se muestran algunos ejemplos, incluidos algunos que parecen dirigirse a usuarios que hablan español:

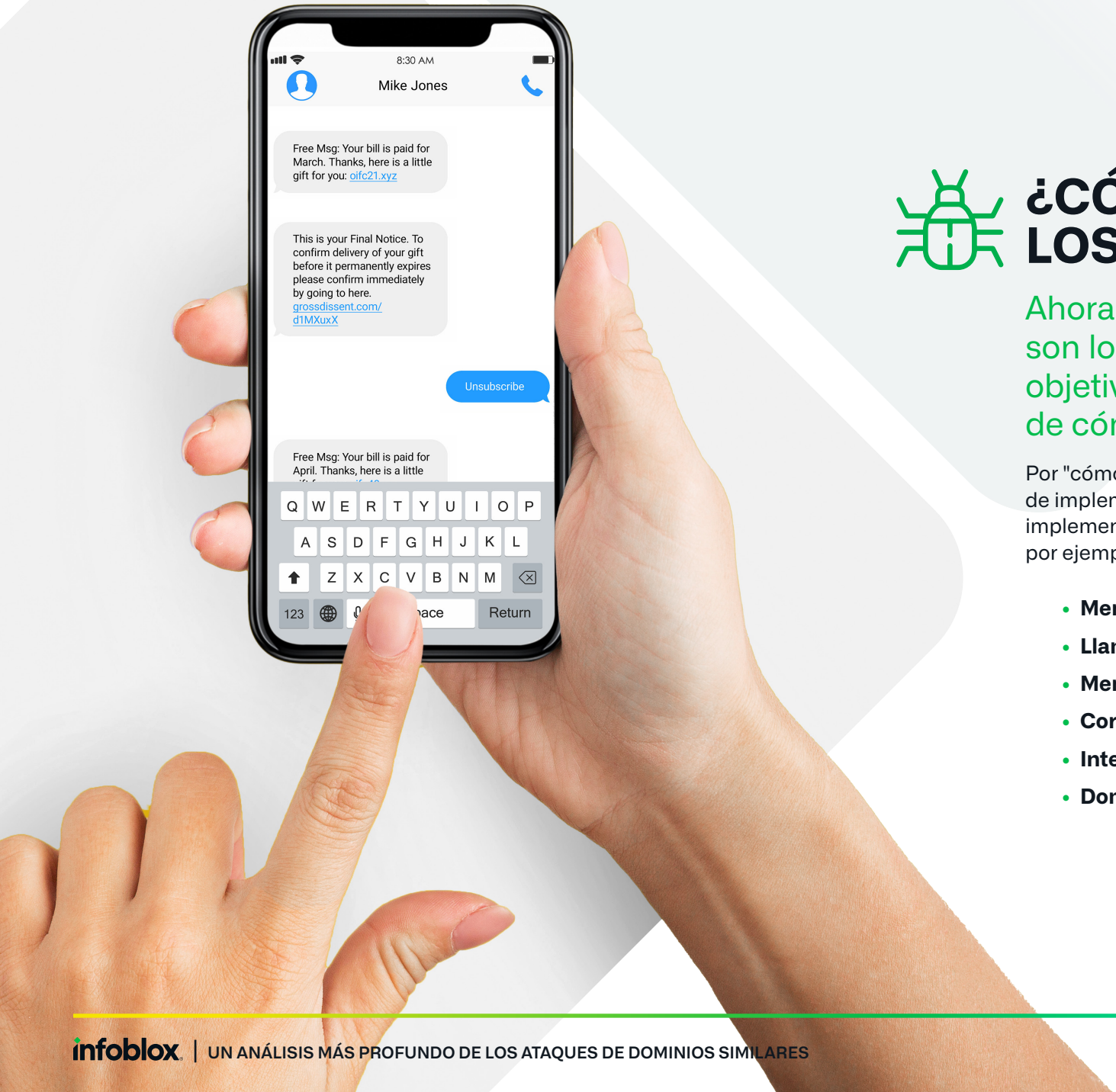
Tabla 5. Dominios similares dirigidos a servicios relacionados con Apple.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

SE DIRIGEN A TODOS

Nuestros algoritmos de detección identifican miles de nuevos dominios similares cada día. Cualquier empresa o servicio, grande o pequeño, donde actores maliciosos puedan robar dinero o identidades será el objetivo. Cerraremos esta sección con una variedad de dominios similares que hemos observado en la naturaleza y su objetivo.

Tabla 6. Dominios similares y sus objetivos.

Dominios similares	Objetivo similar
mee6bot[.]ru	Bot de Discord, Mee6
vulcan[.]pm	Bot de Discord, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	Oficina de Impuestos de Australia
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Sitios web de verificación de estafas
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	Servicios postales y de entrega
crarebate-info[.]com	Reembolso de impuestos canadienses
ebl-ch[.]com	Empresa energética suiza EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.] fi, servicio finlandés de banca digital y seguros
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	La empresa de tecnología india BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Empresas de calzado
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amèricafirst[.]com	Bancos
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Proveedores de servicios de Internet y en la nube
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Autenticación multifactor y dominios de inicio de sesión único



¿CÓMO SE UTILIZAN LOS LOOKALIKES?

Ahora que hemos cubierto qué son los lookalikes y algunos objetivos de ejemplo, hablemos de cómo se utilizan.

Por "cómo" nos referimos a sus métodos de implementación. Infoblox vio imitaciones implementadas de diversas maneras, como por ejemplo:

- **Mensajes SMS**
- **Llamadas telefónicas**
- **Mensajes directos en redes sociales**
- **Correos electrónicos**
- **Integrado en códigos QR**
- **Dominios en la World Wide Web**

ENVÍAN TEXTOS

A pesar de las mejoras en los filtros de spam para los mensajes de texto de telefonía móvil (SMS), el uso de SMS para enviar mensajes de phishing, a menudo denominado smishing, sigue aumentando.

Los actores pueden distribuir rápidamente una gran cantidad de mensajes y evitar algunos de los mecanismos de seguridad que se utilizan para protegerse de los ataques de suplantación de identidad por correo electrónico. Los SMS se utilizan tanto en amplios ataques a los consumidores como en estrechos ataques de spearphishing contra los empleados de las organizaciones. En esta sección describiremos a dos actores de amenazas que han utilizado SMS y dominios parecidos para atacar a consumidores y empleados gubernamentales.

Durante casi un año, Infoblox ha estado rastreando a un autor persistente de smishing de lookalike, al que llamamos OpenTangle. Hasta donde sabemos, no se ha informado de este autor en ningún otro lugar. En un principio, OpenTangle se dirigió a los consumidores occidentales utilizando lookalikes de instituciones financieras, proveedores de Internet y minoristas en línea. El autor recientemente comenzó a apuntar a empleados y contratistas del gobierno. Conocemos más de 1500 dominios similares controlados por OpenTangle desde que comenzaron a operar hace aproximadamente dos años. Algunos de los dominios de OpenTangle incluyen mtbsuportz0610[.]com, americafirst0nline[.]com y mygov03-ato[.]com.

Observe su uso de diferentes técnicas similares.

Uno de los autores de este artículo recibió varios textos de OpenTangle, que incluían lookalikes de M&T Bank, con los que el autor no tiene relación. Al principio de sus campañas, OpenTangle incluía enlaces URL acortados en sus textos smishing, tal vez con la esperanza de que el engaño tuviera éxito. Sin embargo, en mayo de 2022, se convirtieron a dominios similares. *La figura 13* muestra un ejemplo de una de sus campañas bancarias en la que solicitan las credenciales del usuario.

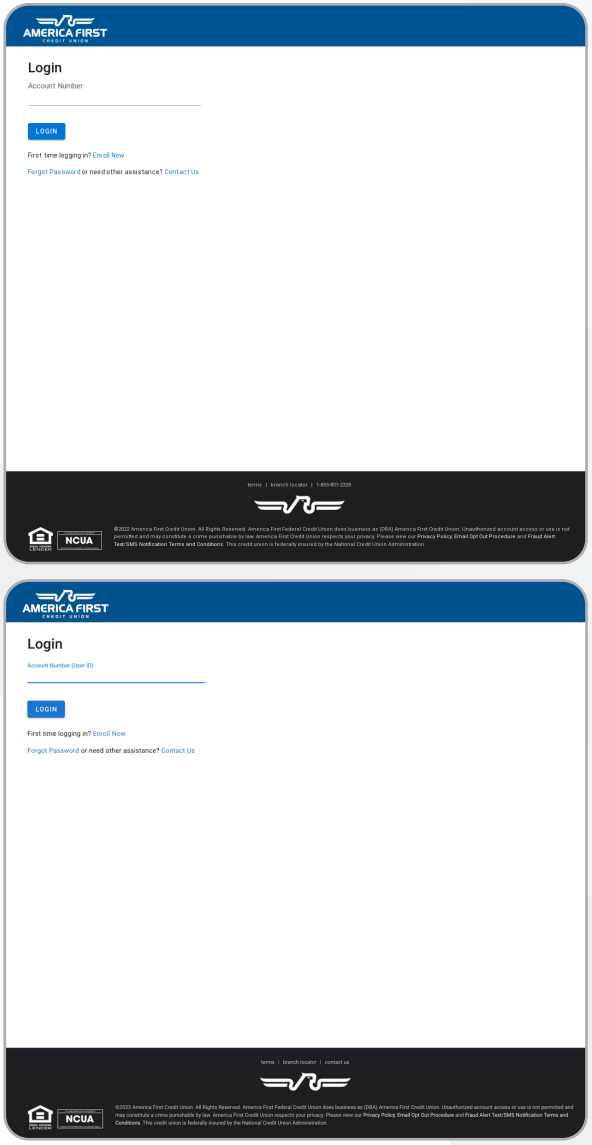


Figura 13. Una página de phishing en el dominio americafirst0nline [.] com dirigida a los titulares de cuentas de America First Credit Union. La imagen de arriba es la página de phishing, la imagen de abajo es la página legítima. Crédito de la imagen: URLScan.[33]

OpenTangle comenzó a explotar MFA utilizando kits de phishing AitM en el último año. Si bien sus campañas anteriores utilizaban páginas de inicio de sesión de phishing estándar y, por lo general, se dirigían a los consumidores, *la Figura 14* muestra un ejemplo de cómo han avanzado sus campañas. En este caso, se dirigen a los titulares de cuentas MyGov del Gobierno australiano y solicitan un código de MFA, en lugar de un simple inicio de sesión. También incluían un enlace para llamar al servicio de asistencia, otra técnica que surgió en 2022 como medio para convencer a los usuarios de que visitaran sitios web malintencionados.

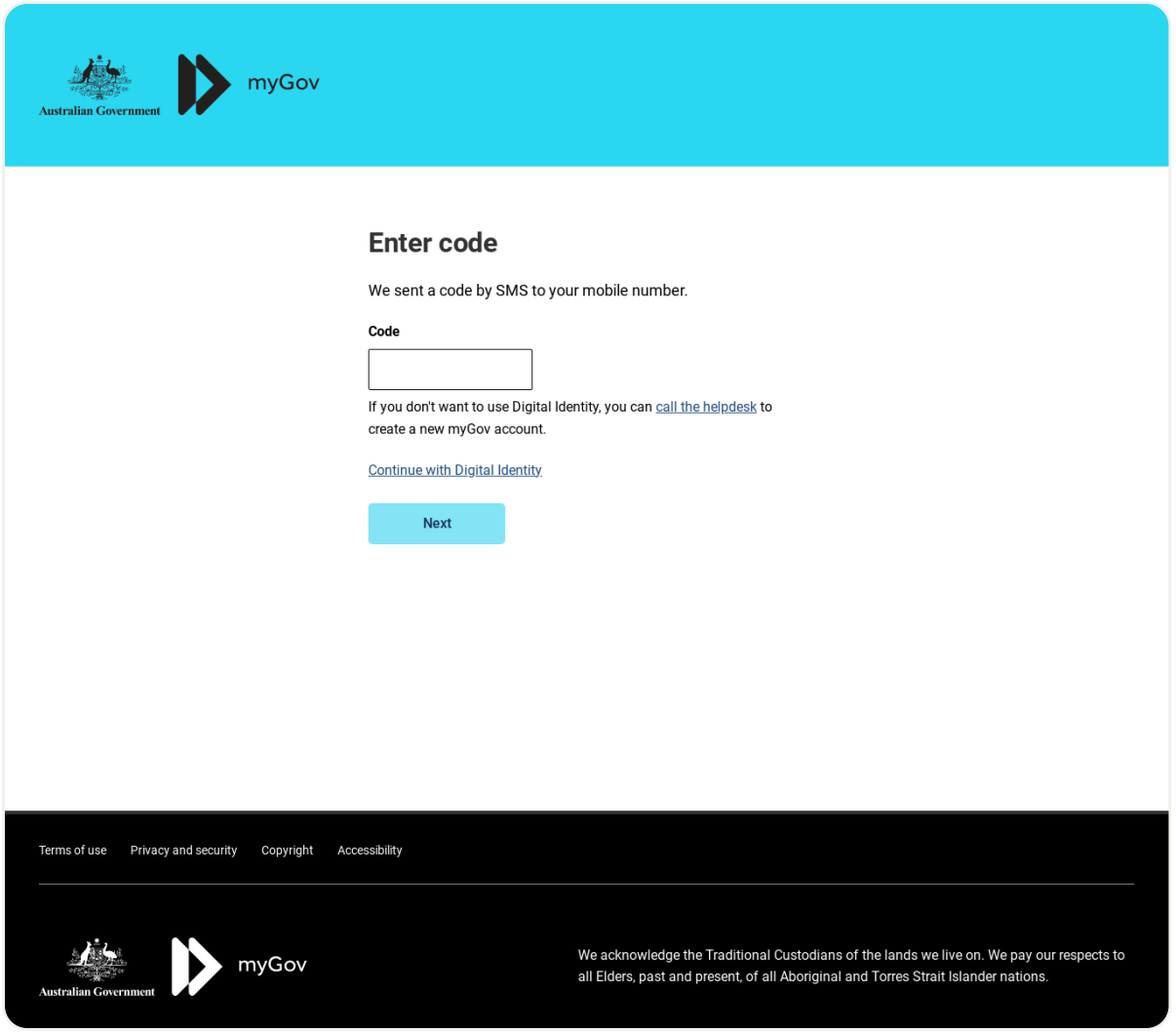


Figura 14. Dominio similar de OpenTangle www.mygovsupport-ato[.]com, que imita myGov, el portal en línea del gobierno australiano para la nube. Crédito de imagen: URLScan.[34]

Scamélie es otro ejemplo de un autor que utiliza mensajes de smishing para difundir lookalikes.

El autor que llamamos Scamélie es una colección de grupos e individuos vagamente afiliados implicados en una larga lista de estafas procedentes de países francófonos y dirigidas principalmente a ellos. También los hemos visto involucrados en una segmentación más general en Europa y Emiratos Árabes Unidos. Los dominios similares de Scamélie suplantan principalmente a ISP, bancos, servicios gubernamentales y empresas de entrega. Debido a la escasa afiliación del grupo, también hemos visto estafas a empresas menos esperadas, como compañías de viajes, de ropa deportiva y tiendas de comestibles.

Los dominios similares de los estafadores suelen estar alojados en grandes proveedores en la nube o en empresas de alojamiento "a prueba de balas". En algunos casos, los estafadores han creado los suyos propios o utilizan proveedores de alojamiento creados por otros estafadores no afiliados. Hemos visto tanto dominios dirigidos como dominios de uso general (my-account, resolve-an-issue, etc.) registrados a través de identidades robadas y pagados con tarjetas de crédito virtuales o criptomonedas.

Una vez que los autores han recopilado la información de la tarjeta de crédito, llaman a la víctima, haciéndose pasar por un empleado del banco o emisor de la tarjeta de crédito de la víctima.
Explican que la información de la tarjeta de crédito de la víctima ha sido robada, pero que ayudarán a solucionar el problema. A continuación, la persona que llama dice que la víctima recibirá dos códigos MFA que tendrán que leer de nuevo a la persona que llama para la seguridad de la cuenta. En realidad, el atacante necesita los códigos MFA para robar dinero a la víctima en tiempo real. El primer código MFA aumenta el importe de la transferencia bancaria y el segundo permite que la transacción se realice. Para aumentar la eficacia de sus llamadas, el autor utiliza a personas que llaman que, idealmente, son mujeres jóvenes o individuos que hablan francés de una manera que no despertarán la sospecha de un orador nativo.

Al ser un grupo desorganizado, Scamélie es difícil de rastrear y analizar. Suelen atacar durante la noche a sus víctimas y acaban con sus dominios al cabo de un par de horas o días. Utilizan scripts anti-bot y anti-scraping para obstruir aún más a los investigadores de seguridad.

SCAMÉLIE EJEMPLOS DE LOOKALIKE

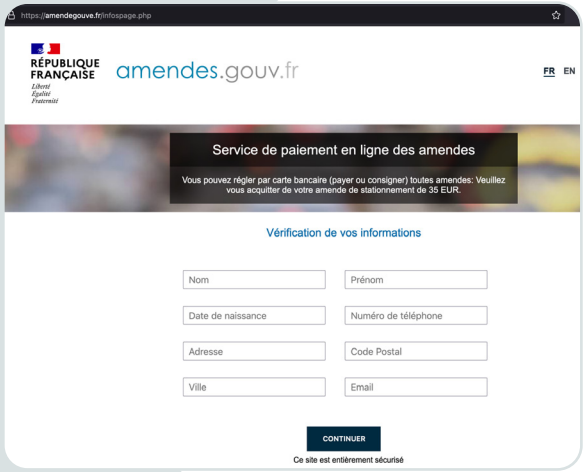


Figura 15. Un servicio de lookalike de Scamélie[.]fr, que imita un portal de servicios del gobierno francés.

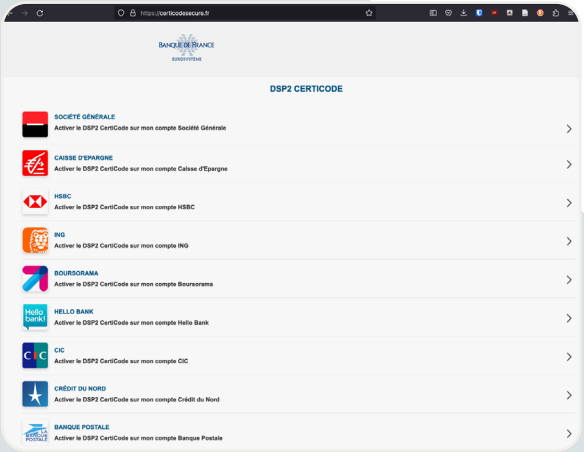


Figure 16. A Scamélie lookalike site certicodesecure[.]fr, spoofing a French banking service and enticing victims to link their bank account information.
Image credit: Infoblox.

LLAMAN POR TELÉFONO A LA ANTIGUA USANZA

La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) lanzó un Asesor de Ciberseguridad (CSA) el 2023 de enero de 35 sobre el uso malicioso del software de supervisión y gestión remota (RMM).[35]

CISA identificó una campaña en octubre de 2022, en la que los agentes maliciosos enviaron correos electrónicos de phishing que contenían un número de teléfono y pidieron a los usuarios que llamaran. El correo electrónico estaba diseñado para pasar por un mensaje de atención al cliente y, cuando los usuarios llamaban al número de teléfono, los actores les inducían a visitar un dominio malicioso. Cuando el usuario lo hacía, se descargaba un archivo ejecutable y se ponía en contacto con un segundo dominio malicioso, desde el que se descargaba software RMM adicional. Este software, AnyDesk y ScreenConnect, era legítimo, pero estaba preconfigurado para conectarse al servidor RMM del actor para lograr persistencia.

Los dominios utilizados son similares a los de servicios conocidos; la probabilidad de que acepten el dominio es aún mayor para las víctimas a las que se lo dieron por teléfono, debido a la ingeniería social adicional utilizada para crear los guiones y los personajes de las personas que llaman. Realizamos una revisión retroactiva de nuestros datos y encontramos pruebas de que el actor lleva más tiempo en activo del que indica la CSA.[36] Estas campañas estuvieron activas al menos desde la primavera de 2021, más de un año antes de los incidentes que CISA y Silent Push, en un artículo separado, describieron. También vimos cierta reutilización de dominios. Por ejemplo, el dominio amzsupport[.]live, de Amazon, formó parte de una campaña activa en abril de 2020 y volvió a utilizarse en octubre de 2021.

A medida que los ataques contra la protección MFA de los sistemas corporativos internos salieron a la luz a principios de 2023, se fue revelando que en algunos casos los autores llamaron por teléfono a la víctima, haciéndose pasar por su departamento de TI. Esto se hizo después de que la víctima no hubiera respondido a la solicitud inicial y se utilizó para dar más legitimidad a la necesidad de que el usuario visitara el dominio de aspecto similar. Los usuarios que cumplieron permitieron al actor robar sus credenciales corporativas.

ENVÍAN SPAM

Aunque hemos visto a astutos autores utilizar el smishing y las llamadas telefónicas para distribuir parecidos y atrapar a las víctimas, el correo electrónico de phishing nunca ha pasado de moda.

Infoblox analiza decenas de miles de correos electrónicos maliciosos cada día, revelando un flujo aparentemente interminable de campañas que distribuyen dominios similares. Destacaremos algunas de estas campañas, pero enfatizaremos la importancia de que las organizaciones mantengan una monitorización diligente de los correos electrónicos de phishing.

Una de estas campañas se dirige a Xfinity, una importante empresa estadounidense de telecomunicaciones. Estos parecidos tienen características similares a la DGA y son de la forma xfnity<short or partial word>. com. Tenga en cuenta que "Xfinity está mal escrito porque le falta la primera "i". El actor también aseguró que el nombre del remitente apareciera legítimo, mostrando como "Xfinity Mobile", que utiliza una letra mayúscula cirílica "X". Los correos electrónicos remitentes utilizaban sus propios dominios y parecían tener también características similares a las de la DGA en el nombre de usuario, consistente en el patrón noreply <keyword>, como noreply-corporate@xfnitycard[.]com Los autores no utilizaron dominios únicos para cada correo electrónico. En algunos casos, los dominios se repitieron, pero se cambió la palabra clave, como en: noreply-corporate@xfnitycard[.]com y noreply-active@xfnitycard[.]com

Tabla 7. Dominios similares a Xfinity.

xfnitykuri[.]com	xfnitycomp[.]com
xfnitystarter[.]com	xfnityhlaty[.]com
xfnityersa[.]com	xfnityothie[.]com
xfnitykaris[.]com	xfnityrkles[.]com
xfnityrayton[.]com	xfnitycard[.]com

Los dominios identificados en la campaña utilizan una técnica que hemos denominado aparcamiento con señuelos: cuando se visita un dominio directamente y parece que está aparcado, pero en realidad, el servidor de correo del dominio está activo y envía correos electrónicos malintencionados. Hemos descubierto que el aparcamiento con señuelo es bastante común y no nos han denunciado otros vendedores. *Consulte la Figura 17 para ver un ejemplo de una página de aparcamiento con señuelo*

XFINITY LOOKALIKE

Figura 17. Página de aparcamiento señuelo mostrada por el lookalike de Xfinity xfnityrayton[.]com. Crédito de imagen: URLScan.[37]

LOOKALIKE DE WEDO MACHINERY

Dear you

Good day !
How are you?
How is your project going?
Do you receive my message?

Hope we can establish long term cooperation.

We got recommendation of your company from our UK partner about

below order as attached

Please confirm if your can deliver the products specifield

Mrs. ConnieXu
Mob: 0086 131 0941 7901 [WhatsApp/Wechat]

Wedo Machinery (Zhangjiagang) CO., LTD.

Add: Zhenbei Road, Leyu Town, Zhangjiagang City, Jiangsu Province, China.

Figura 18. Cuerpo de la campaña de malspam usando Wedo Machinery como señuelo y el dominio similar de acrobat-adobe[.]com como malware C2.
Crédito de imagen: Infoblox

Nuestro análisis encontró estos lookalikes de Xfinity en documentos de Word maliciosos distribuidos.

Los asuntos de las campañas se duplicaban como llamada a la acción y se centraban en la denegación del pago o en una amenaza de cancelación del servicio, como "[Anuncio] Su servicio corre el riesgo de ser cancelado" o "[Acción necesaria] No podemos realizar el cargo en su tarjeta, solucione este error". El cuerpo de estos correos electrónicos se enmarcaba como procedente del servicio de atención al cliente, pidiendo a los destinatarios que "vieran los detalles del caso en el archivo adjunto".

Otra campaña que había identificado Infoblox utilizó una empresa china de reciclaje, Wedo Machinery, para lanzar un cargador de ransomware. Identificamos 176 correos electrónicos en esta campaña, cada uno con un archivo.zip que contenía un único ejecutable llamado Zmutzy. *Consulte la figura 18 como ejemplo de correo electrónico dentro de la campaña.* Hemos visto dos nombres de archivo en la campaña: PO-0097 (1) .zip y PO-29862K.zip. El cargador de Zmutzy utiliza el dominio similar acrobat-adobe[.]com para descargar cargas útiles adicionales.

UTILIZAN CÓDIGOS QR

Además de los lookalies de criptomonedas directos, observamos el uso de suplantación de identidad con código QR cuando se utiliza un código QR para ofuscar un destino de URL y entregar contenido malicioso en conjunto con dominios similares creados para animar a los usuarios a reclamar premios gratuitos y proporcionar información sobre la cuenta de la criptocartera.

En un ejemplo, el código QR redirigía a la víctima a un puente[.]walletconnect[.] com link, un mecanismo utilizado para robar fondos. En esta estafa, los actores crearon una cuenta de Twitter, @adidas_weare, para generar credibilidad y compartir sus dominios similares; véase *la Figura 19*. La cuenta acumulaba 16 000 seguidores hasta el 21 de febrero de 2023; afortunadamente, ya ha sido eliminada o retirada.

Los autores anunciaron regalos falsos de diferentes artículos, incluidos coches Porsche y ropa o zapatos Adidas. Los dominios son predominantemente combosquats que contienen las palabras clave "adidas" o "porsche". Al visitar los dominios similares, como se muestra a continuación en *la Figura 20*, se les pidió a los usuarios que escanearan un código QR que les permitía reclamar el artículo que se regalaba y, a continuación, los redirigieran a la aplicación descentralizada WalletConnect, que daba al actor acceso a los fondos del usuario.

Si los usuarios escanean el código QR y vinculan sus carteras de criptomonedas a la aplicación descentralizada, los autores pueden obtener criptomonedas del usuario. Estos dominios utilizan servidores de nombres compartidos y se alojan en una dirección IP de resolución rusa, 185[.]149[.]120[.]83, que está completamente controlada por autores y contiene otros miradores de Blur, así como Arbitum, una solución para mejorar la velocidad y escalabilidad de los contratos inteligentes de Ethereum.

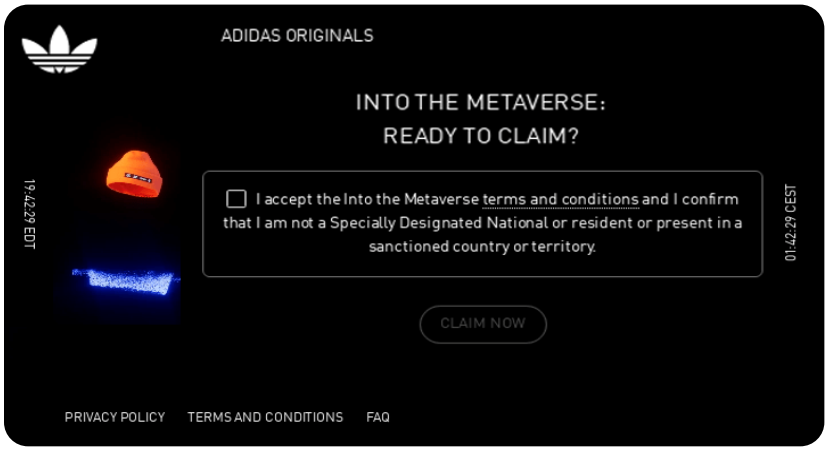


Figura 20. El dominio similar de adidas adidas-go[.]com atrae a los usuarios a hacer clic para reclamar un artículo gratuito. Crédito de imagen: URLScan.[39]

LOOKALIKE DE ADIDAS

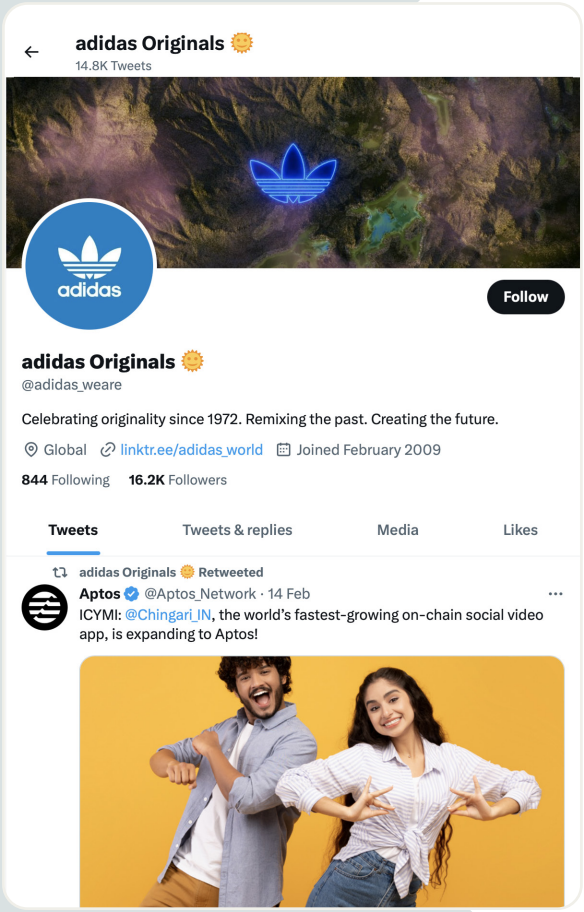


Figura 19. Lookalike de la cuenta de Twitter @adidas_weare de Adidas Originals @adidasoriginals. Crédito de la imagen: Infoblox.

UTILIZAN DNS

Los lookalikes no solo se producen como dominios del sitio web.

Hemos descubierto que se usan en varias capacidades de DNS, entre ellas:

- **Servidor de nombres**
- **Servidor de correo**
- **Registros CNAME**
- **Registros PTR**

En la mayoría de los casos, estos dominios no tendrán un registro A típico o presencia en el sitio web y a menudo pueden aparecer estacionados en el marco de un estacionamiento de decoy que describimos en una sección anterior. Los atacantes también utilizan dominios similares para la redirección y la comunicación C2 en DNS.

SERVIDORES DE NOMBRES

Como ejemplo deservidores de nombres looƙalike los dominios bitkeep[.]dev y flutter[.]direct se registraron en noviembre de 2022. Ambos son lookalikes de dominios diferentes, pero comparten una infraestructura. BitKeep es una criptocartera descentralizada multicadena que pretende ser un centro único para todas las transacciones de criptodivisas. El dominio oficial de BitKeep es bitkeep[.]com y la empresa lleva funcionando cinco años con más de 8 millones de usuarios.[40] Flutter es el conjunto de herramientas de interfaz de usuario (UI) portátil de Google para crear aplicaciones compiladas de forma nativa para móviles, web y escritorio a partir de un único código base. El dominio oficial de Flutter es flutter[.]dev.[41]

Ambos dominios legítimos alojan contenido web en el dominio principal, pero ninguno de los dominios similares lo hace. Cuando se registró inicialmente, ambos dominios actuaban como servidor de nombres para otro dominio, get-flutter[.]com, que es otro lookalike de Flutter. En ese momento, los dominios estaban alojados en el proveedor suizo de alojamiento offshore Private Layer. Esta red también acogió a flutter[.]vision. Aunque no podemos atribuir definitivamente estos dominios a actividades maliciosas, demuestran un patrón de aprovechamiento de dominios similares con fines no tradicionales. Resultan bastante difíciles de analizar incluso para investigadores experimentados y es poco probable que para activar muchos algoritmos de inteligencia de amenazas.

SERVIDORES DE CORREO

Además de los servidores de nombres, hemos visto que se utilizan lookalikes como servidores de correo. Los dominios whirlpoolmxonline[.]com y whirlpoolservicesmx[.]com apuntan a la principal marca de electrodomésticos Whirlpool y comparten infraestructura común. Están alojados en la misma dirección IP, propiedad de Lyra Hosting, un proveedor de alojamiento y VPS de baja calidad situado en las Seychelles, y comparten servidores de nombres comunes.

Si bien se dirigen a Whirlpool directamente con el nombre de dominio de segundo nivel (SLD), también hemos identificado características dentro de cada dominio que muestran que también se dirigen a otras marcas importantes de electrodomésticos. La SLD whirlpoolmxonline[.]com tiene tres subdominios: mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.]whirlpoolmxonline[.]com, y lg-onlinemx[.]whirlpoolmxonline[.]com. Mabe es una empresa mexicana de electrodomésticos. El SLD whirlpoolservicesmx[.]com no tiene subdominios, pero la cadena histórica de certificados SSL asociados con el dominio apunta a la orientación de marcas de dispositivos similares como whirlpoolmxonline[.]com: www[.]lgservicesmx[.]mabeservice[.]com y *.lgservicesmx[.]com.

El uso de lookalikes como servidores de correo ofrece un reto adicional para la detección de correos electrónicos de suplantación de identidad en un punto final debido a la apariencia de legitimidad con un primer vistazo a las cabeceras de los correos electrónicos.

MALWARE C2

En la sección anterior de implementación del correo electrónico, mencionamos que una campaña de correo no deseado que identificamos, que consistía en dejar caer el cargador de ransomware Zmutzy, utilizaba el dominio similar acrobat-adobe[.]com como servidor C2 de malware. Los lookalikes son perfectos para los C2 del malware porque pueden mezclarse fácilmente con el tráfico de la red junto con los dominios legítimos. Los investigadores de ESET, una empresa eslovaca de software de seguridad, identificaron el malware C2 para FatalRAT (un troyano de acceso remoto) que se hacía pasar por Telegram, la aplicación de mensajería,en febrero de 2023.[42]

Tabla 8. Los lookalikes de Telegram funcionan como malware C2.

12-03.telegramxe[.]com	12-25.telegraem[.]org
12-25.telegraxm[.]org	12-25.telegraem[.]org

Los dominios que alojan el .exe malicioso Los archivos también se parecían a Telegram, así como a WhatsApp, Skype, Google Chrome y Firefox.

REDIRECCIONES

Los lookalikes también pueden emplearse como redirecciones. Hemos identificado una gran red de dominios typosquat que redirigen a los visitantes a choto[.]xyz, un dominio C2 que redirige condicionalmente a las víctimas al dominio de aterrizaje lotto60[.]com. El actor utiliza servicios de proxy inverso y protección contra bots de Cloudflare en choto[.]xyz, presumiblemente para evitar la detección y exploración por parte de los investigadores de seguridad. El dominio de aterrizaje parece estar ejecutando un programa fraudulento de marketing de afiliación. Al analizar el modelo de objetos de documento (DOM), podemos ver que el HTML contiene una función gtag() en línea que envía los datos de los visitantes a Google Analytics con el ID de análisis G-DT4YWT5VP8. Además de inflar los números de marketing de afiliados del agente, hemos visto que Lotto60[.]com se solicita a través de HTTP mediante archivos potencialmente maliciosos que coinciden con firmas de archivos confirmadas como troyano de acceso remoto Nighthawk.[43]

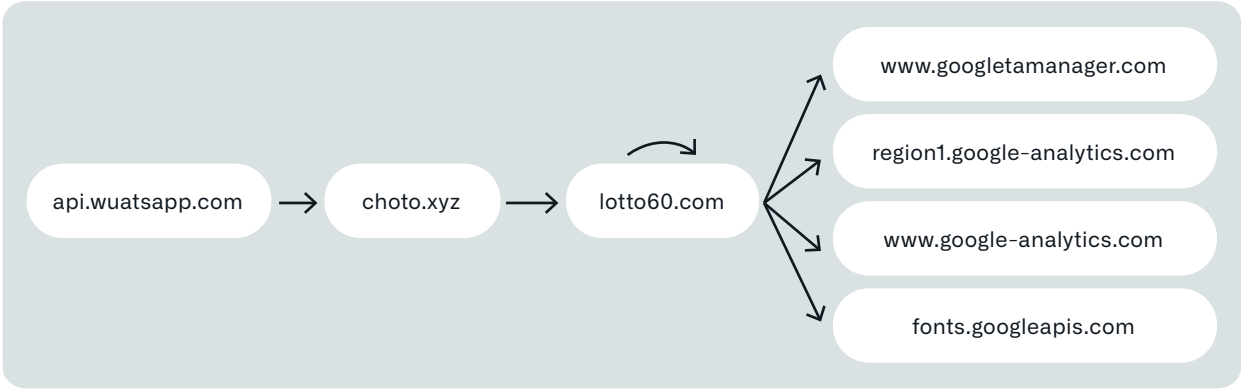


Figura 21. Ejemplo de cadena de redirección de un dominio de Typosquat a Google Analytics. Crédito de imagen: URLQuery.[44]

Los dominios typosquat de primera fase imitan a diversas empresas. Algunos ejemplos incluyen →

Tabla 9. Lookalikes funciona como redirecciones en una campaña fraudulenta de marketing de afiliados.

gi6hub[.]com	whatysapp[.]com
bankofamegica[.]com	babgkokbank[.]com
intuhit[.]com	scotiasbank[.]com

Estos typosquats suelen estar aparcados durante uno a tres meses antes de usarse como redirecciones. El autor ha puesto mucho cuidado en la creación de estos dominios typosquat. Cada carácter incorrecto es directamente contiguo al carácter correcto en un teclado QWERTY en inglés estadounidense. Se trata de errores que cualquier mecanógrafo medio podría cometer varias veces en un solo día, salvo aquellos usuarios que todavía escriben con uno o dos dedos.

¿POR QUÉ SON EFICACES?

Estimado lector, ¿se ha dado cuenta de los lookalikes que hemos esparcido en este artículo hasta ahora? Algunos son muy difíciles de ver.

Pista: Hay unos cuantos más. A ver si puede encontrarlos

Hasta ahora hemos cubierto algunos objetivos específicos, así como la infraestructura de los métodos de implementación de dominios similares. Pero, ¿por qué son tan eficaces? ¿Qué los convierte en una amenaza tan persistente?

La respuesta es complicada e implica aspectos de la psicología, implementaciones técnicas y errores humanos simples, ¡es decir, **lo que nos hace humanos, después de todo!**

PSICOLINGÜÍSTICA

Desde el punto de vista psicológico, el cerebro humano entra en cortocircuito (en este caso, nos referimos a la definición literal de una corriente que toma un camino involuntario de menor resistencia) mientras lee. Probablemente haya visto un meme que dice algo como:

> ***De aceurdo con las invesitgacioens de la Uinervsidad de Cmabrigde, no improta en qué oredn vaayn las lteras en una palbara, lo úinco iprmoetant es que la pirmera y la úlitma ltera estén en la poisción corercta. El rseto peuden ser un compeleto dessatre y aun así pordás lerelo sin porblema. Etso se dbee a que el ojo hmuano no lee cada ltera, sino la palbara compelta.***

Aunque la afirmación carece de fundamento en el sentido de que nunca se publicó una investigación de este tipo en Cambridge, el concepto subyacente parece tener mérito. Por ejemplo, investigaciones reales recientes sugieren que "ver una palabra desordenada activa una representación visual que se compara con palabras conocidas".[45] Aunque demostrar o refutar cuestiones fundamentales de la psicolingüística está fuera del alcance de este artículo, sí queremos mostrar cómo la psicolingüística desempeña un papel importante en la eficacia de los lookalikes.

Específicamente, el cortocircuito del cerebro humano juega un papel en lo que respecta a homógrafos y typosquats. Cuando ve un dominio como Infoblox[.]com, su cerebro no necesariamente analiza cada letra individual en ese nombre de dominio y nunca se nota "L".

Por razones similares, cuando ve el dominio goooogle[.]com, es posible que su cerebro no se detenga a reconocer que hay tres de la letra "o" en lugar de las dos adecuadas... al menos, no hasta que sea demasiado tarde y ya haya hecho clic en ella.

SOPORTE DE PUNYCODE: ACIERTOS Y ERRORES

Los navegadores web tienen formas de defender a los usuarios contra los ataques de nombres de dominio internacionalizados (IDN) homоgrafo. La primera y más prominente línea de defensa es "traducir" el dominio Unicode a Punycode, que puede ser reconocido por su "xn--" inicial y parece ser un galimatías a simple vista. Esto se debe a que Punycode asigna caracteres Unicode al subconjunto mucho más limitado de caracteres del Código Estándar Americano para el Intercambio de Información (ASCII) que contiene solo letras, dígitos y guiones. Cada uno de los principales navegadores es compatible con los dominios de Punycode. Google ofrece una descripción detallada de la heurística involucrada en el algoritmo que determina si mostrar la versión internacionalizada o la versión Punycode de un dominio en Chromium.[46] Mozilla da una descripción similar.[47]

Mozilla también ofrece este texto inspirador en la descripción de su algoritmo de visualización de IDN:

> ***Nuestra respuesta a este problema es que, en última instancia, corresponde a los registros asegurarse de que sus clientes no puedan estafarse unos a otros. Los navegadores pueden imponer algunas restricciones técnicas, pero no estamos en condiciones de hacer este trabajo por ellos y mantener al mismo tiempo la igualdad de condiciones para los alfabetos no latinos en la web. Los registros son los únicos que pueden realizar aquí un control adecuado. Por nuestra parte, queremos asegurarnos de no tratar a las escrituras no latinas como ciudadanos de segunda clase.***

En 2017, el investigador de seguridad Xudong Zheng registró un dominio que ya estaba en Punycode, xn--80ak6aa92e[.]com, que se traduce como "apple[.]com", contiene caracteres cirílicos que imitan la apariencia de los caracteres latinos de "apple".[48] En ese momento, los navegadores web Internet Explorer, Microsoft Edge, Safari, Brave y Vivaldi no eran vulnerables, pero Chrome, Firefox y Opera sí. En este momento, solo Firefox sigue traduciendo el Punycode, dejando a los usuarios vulnerables al ataque (no hemos probado últimamente el dominio en Internet Explorer o Microsoft Edge).

¿QUÉ ES PUNYCODE?

Punycode es una codificación especial que se utiliza para convertir caracteres Unicode a ASCII, que es un conjunto de caracteres más pequeño y restringido. Punycode se utiliza para codificar nombres de dominio internacionalizados (IDN).

SMISHING CON HOMÓGRAFOS DE IDN DE IMESSAGE

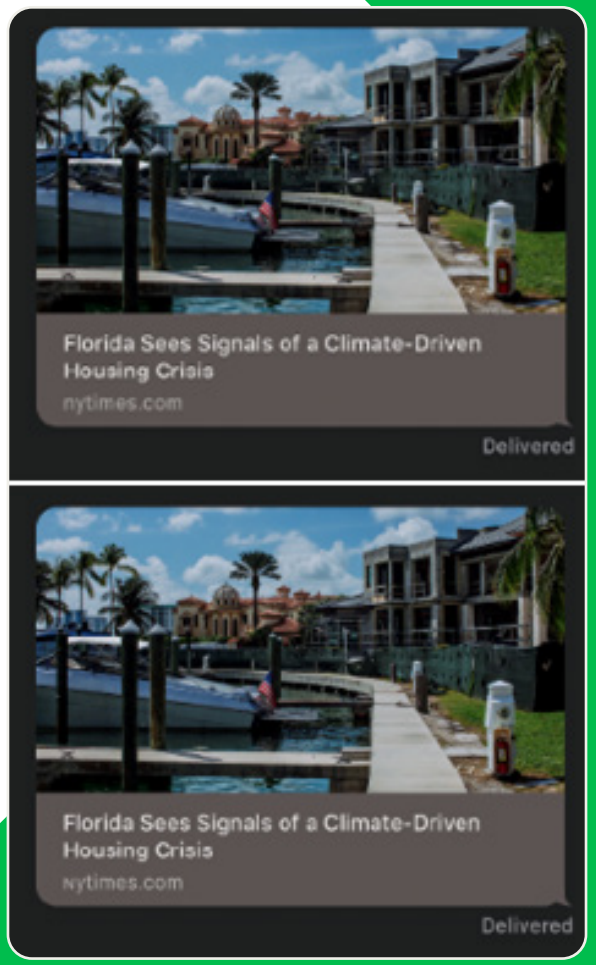


Figura 22. Imagen principal procedente de Tyler Butler que muestra un artículo real del New York Times enviado a través de iMessage. Imagen inferior obtenida a través de Tyler Butler mostrando un artículo falsificado de NYT en un dominio homógrafo IDN.
Crédito de imagen: Tyler Butler.

Hu et al. realizó un análisis longitudinal y cuantitativo sobre la eficacia de las defensas basadas en navegador contra ataques homógrafos de IDN.[49]

Se propuso responder tres preguntas:

1. ¿Qué políticas implementan los principales navegadores y qué tan bien las aplican?
2. ¿Hay formas de eludir sistemáticamente las políticas existentes?
3. ¿Hasta qué punto reconocen los internautas los homógrafos de IDN? ¿Son más o menos engañosos los homógrafos de IDN que eluden las políticas de los navegadores?

Para responder a las preguntas, los autores analizaron cinco navegadores principales (Chrome, Firefox, Safari, Microsoft Edge e Internet Explorer) durante cinco años (de enero de 2015 a abril de 2020). Generaron 9000 casos de prueba para responder a sus primeras dos preguntas y realizaron un estudio de usuario para responder a la tercera. Chrome y Edge tuvieron más éxito al mostrar Punycode en lugar de sus homógrafos IDN correspondientes; ambos navegadores tenían una tasa de fallos global (mostraron la versión IDN en lugar de Punycode) del 20,62 %. Safari y Firefox fueron mucho peores, con una tasa de error global de 42,91 % y 44,46 %, respectivamente. Cada navegador tenía diferentes tasas de error según la categoría de IDN. Además, los autores descubrieron que los internautas tienen dificultades para identificar los IDN homógrafos, y aquellos IDN que los navegadores bloqueaban eran los que más problemas daban para determinar su autenticidad: el 48,8 % de los usuarios pensaban que sí lo eran, el 48,5 % de los usuarios pensaban que no lo eran y el 2,7 % no sabían decirlo.

Hasta ahora solo nos hemos centrado en los navegadores de escritorio. Pero como hemos visto con los ataques de smishing de dominios similares descritos anteriormente en este documento, los dominios homógrafos de IDN también se sienten como en casa en los dispositivos móviles. De hecho, podrían ser más peligrosos. Las pantallas más pequeñas, las barras de direcciones más pequeñas y la falta general de vista previa de enlaces pueden dar lugar a ataques de dominios similares más eficaces. Incluso cuando hay una vista previa de vínculos, los homógrafos de IDN pueden seguir siendo eficaces en dispositivos móviles. En 2021, el investigador de seguridad Tyler Butler publicó sobre la plausibilidad del smishing mediante homógrafos de IDN en iMessage.[50] iMessage ofrece vistas previas enriquecidas de enlaces, pero un atacante inteligente puede sortear esto con bastante facilidad con un dominio similar lo suficientemente bueno y un poco de trabajo de estilo para la página web en sí. Como señala Butler, esta forma de ataque se puede utilizar para difundir información errónea, robar credenciales o entregar malware o spyware dirigido.

Butler describe que Apple afirmó que no abordaría la vulnerabilidad debido a que los homógrαfos son "distinguibles visualmente". *Dada la figura 22, ¿qué opina? ¿Puede ver la diferencia*?

ERRAR ES HUMANO, PERDONAR ES DIVINO... PERO AUTOMATIZAR ES SABIO

En la World Wide Web, otros seres humanos no son tan indulgentes con los errores de los demás. Como hemos mencionado, los autores utilizan dominios typosquat para presumir de errores ortográficos naturales de otros. Todo lo que un atacante tiene que hacer para que un typosquat sea efectivo es registrar un dominio plausible y esperar. Eso es todo. Tarde o temprano, un humano cometerá ese error de ortografía y aterrizará en un dominio que nunca tuvo la intención de visitar. Por supuesto, los agentes maliciosos no sólo esperan, sino que atraen proactivamente a las personas a hacer clic. Y en nuestro mundo en rápido movimiento, muchas veces ni siquiera nos damos cuenta de que hemos cometido un error.

Al fin y al cabo, los lookalikes reciben ese nombre en inglés por una razón: se parecen a dominios conocidos con la intención de engañar a un humano. Como hemos visto, algunos lookalikes son más efectivos que otros, pero la elección del nombre de dominio es solo una parte de la efectividad de un lookalike. La forma en que se implementa un dominio similar también puede tener un impacto significativo en el éxito general de la campaña. Tomemos, por ejemplo, un lookalike de Okta o MFA como okta[.] Infoblox[.] com, o okta-Infoblox[.]com. Una persona perspicaz que verifique tres veces cada nombre de dominio antes de visitarlo (buena suerte para encontrar a una de esas personas) podría notar que la "i" en el dominio de segundo nivel (SLD) es en realidad una "L" minúscula. Pero ese lookalike, junto con un mensaje SMS bien elaborado al número de teléfono que tienen en el perfil en línea de su empleador, por ejemplo, podría marcar la diferencia. Agregue a la ecuación una llamada telefónica con una llamada urgente a la acción, y se acabó el juego. Por supuesto, este es un ejemplo ficticio (con todos los componentes que se utilizan) de spearphishing, y no una campaña general que emplea similares, pero el punto sigue siendo: las técnicas similares se pueden aplicar de manera efectiva a dominios de múltiples maneras y a múltiples partes de la infraestructura de DNS.

Todo esto para decir que el proverbio tan citado de "si me engañas una vez, te avergüenzo; si me engañas dos veces, me avergüenzo" no se aplica a los lookalikes. Incluso las personas más conscientes de la seguridad y con ojos de halcón pueden ser víctimas de un lookalike y hacerlo una y otra vez. Los agentes maliciosos llevan ventaja en esta guerra, pero aún no está perdida. Infoblox tiene soluciones a nivel de DNS para garantizar que las organizaciones tengan la capacidad de contraatacar y defenderse de manera efectiva.

IOCs

La lista completa de este documento se puede encontrar en GitHub en https://github.com/infobloxopen/threat-intelligence.

SOLUCIONES DE INFOBLOX

Los dominios similares siguen siendo populares entre los atacantes debido a su eficacia y a la dificultad de detectarlos a escala. El reto se ve agravado por la dificultad de identificar automáticamente un dominio sospechoso que pretende imitar a un objetivo legítimo. Esto ha provocado que las empresas y las agencias gubernamentales se preocupen cada vez más por dominios similares que suplantan sus dominios corporativos o su cadena de suministro.

Infoblox BloxOne Threat Defense (B1TD) Advanced ofrece una solución única y completa contra amenazas similares. Aprovechando el DNS a gran escala, Infoblox puede aplicar una serie de análisis a cientos de miles de nuevos SLD cada día. Esto incluye múltiples análisis para la detección de similitudes, como una evaluación automática de similitudes visuales en homógrafos de IDN.

Los clientes pueden seleccionar entre dominios de destino común o crear una lista personalizada para monitorización y análisis similares especializados. Se puede acceder a los resultados de este análisis en profundidad a través de la interfaz de usuario de informes de lookalike, que también señala casos en los que el lookalike detectado está asociado con actividad sospechosa o de phishing. En general, las políticas se pueden personalizar para satisfacer las necesidades del entorno específico y el nivel de tolerancia al riesgo de un cliente. Y los datos detallados del dominio incluyen anotaciones valiosas a las que se puede acceder a través de las IU y API avanzadas de B1TD, lo que brinda a los clientes un contexto que puede acelerar las investigaciones de amenazas y hacer que las respuestas a incidentes sean más efectivas.

Estas capacidades de detección de amenazas similares son solo uno de los muchos servicios que ofrece BloxOne Threat Defense que le permiten ver amenazas que otras soluciones no ven y detener los ataques en una etapa más temprana del ciclo de vida de la amenaza. A través de la automatización generalizada y la integración del ecosistema, puede impulsar una mayor eficiencia en SecOps, aumentar la eficacia de la pila de seguridad existente, proteger los esfuerzos digitales y de trabajo desde cualquier lugar y reducir el coste total para la ciberseguridad.

FOR MORE INFORMATION

Visit infoblox.com

Follow-us on LinkedIn

Follow-us on Twitter

REFERENCIAS

[1] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

[2] https://twitter.com/kgroupcompanies/status/1188878363068391425

[3] https://en.wikipedia.org/wiki/IDN_homograph_attack

[4] https://i.imgur.com/68oL4U9.jpg

[5] https://www.researchgate.net/publication/220420915_The_Homograph_Attack

[6] https://util.unicode.org/UnicodeJsps/confusables.jsp

[7] https://www.igoldrush.com/domain-guide/domain-legal-issues/cybersquatting-and-typosquatting

[8] https://dl.acm.org/doi/pdf/10.1145/3133956.3134002

[9] https://core.ac.uk/download/pdf/34615371.pdf

[10] https://iris.polito.it/retrieve/handle/11583/2970511/1dd2efbb-9eed-4db5-be4f-ecfcc362572c/_Workshop__Data_driven_Soundsquatting_Generation%20(7).pdf

[11] https://incolumitas.com/2016/06/08/typosquatting-package-managers/

[12] https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[13] https://www.akamai.com/blog/security-research/combosquatting-keyword-analysis-support

[14] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate- reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

[15] https://urlscan.io/result/41e8b29f-55cc-4887-9186-41a064ffb2ac/

[16] https://thehackernews.com/2022/07/microsoft-warns-of-large-scale-aitm.html

[17] https://thehackernews.com/2023/03/microsoft-warns-of-large-scale-use-of.html

[18] https://www.hackread.com/hackers-employee-accounts-twilio-internal-system/

[19] https://www.feldmanauto.com/

[20] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[21] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[22] https://blogs.infoblox.com/cyber-threat-intelligence/scammers-first-on-the-scene-for-turkiyes-disaster-of-the-century/

[23] https://urlscan.io/result/4f295f57-7d46-49e9-94f6-d90858a4cfeb/

[24] https://www.coindesk.com/web3/2023/03/02/nft-trading-volumes-hit-2b-in-february-highest-since-luna-crash-thanks-to-blur/

[25] https://nftnow.com/guides/blurs-token-just-dropped-heres-what-you-need-to-know/

[26] https://twitter.com/blur_io/status/1630290782211981312/

[27] https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/

[28] https://twitter.com/FoolishBB/status/1627059614654279682

[29] https://www.bleepingcomputer.com/news/security/fake-crypto-giveaways-steal-millions-using-elon-musk-ark-invest-video/

[30] https://www.domaintools.com/

[31] https://urlscan.io/result/8e94bf31-7295-47e8-9de4-756743937f46/

[32] https://www.domaintools.com/

[33] https://urlscan.io/result/7f3c8f83-1922-4570-a9b1-1542e32ccc89/

[34] https://urlscan.io/result/f60f5548-4b54-4a97-add5-1f37a89f4e7e/#summary

[35] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

[36] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/dont-dial-that-number-distribution-of-phishing-lookalikes-through-fake-support-calls/

[37] https://urlscan.io/result/41a6ef99-fef1-4d08-80e1-623123280b6a/

[38] https://walletconnect.com/

[39] https://urlscan.io/result/a79ba8e3-9f9a-4a9c-b54b-b26a300afc23/

[40] https://bitkeep.com/

[41] https://docs.flutter.dev/

[42] https://www.welivesecurity.com/2023/02/16/these-arent-apps-youre-looking-for-fake-installers/

[43] https://www.virustotal.com/gui/file/ 271229d5d007baf5324fb2705b7a0b3751bd228bbdb08a86e7b7e2856bbf9b08

[44] https://urlquery.net/report/ef86060b-39e3-4e41-a480-a2b138ee0a49

[45] https://elifesciences.org/articles/54846

[46] https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[47] https://wiki.mozilla.org/IDN_Display_Algorithm

[48] https://www.xudongz.com/blog/2017/idn-phishing/

[49] https://www.usenix.org/system/files/sec21-hu-hang.pdf

[50] https://tbutler.org/2021/04/16/considering-the-plausibility-of-idn-homograph-attacks

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

+1.408.986.4000
www.infoblox.com