infoblox

Threat Intel

PROLIFIC PUMA: UN OSCURO SERVICIO DE ACORTAMIENTO DE ENLACES HABILITA LA CIBERDELINCUENCIA

Autores:
Laura da Rocha
Renée Burton
Stelios Chatzistogias
Darby Wise

ÍNDICE

RESUMEN EJECUTIVO

Tal vez Halloween sea la época más espeluznante del año, pero los actores de amenazas nos aterran en internet todos los días. El mes pasado introdujimos dos términos: actores de amenazas del Domain Name System (DNS) y RDGA, o algoritmo de generación de dominios registrados. También ofrecimos un apunte sobre un tipo de actor de amenazas del DNS, el suplantador de identidad persistente, mediante revelaciones sobre Open Tangle.

Hoy presentamos al segundo actor de esta serie, **Prolific Puma**. Desde hace cuatro años, tal vez más, Prolific Puma opera entre las sombras, sin que los defensores lo reconozcan. Aunque desconocemos su origen, podemos detectar a Prolific Puma a través del DNS y hacernos una idea de su carácter a través de los registros de nombres de dominio elegidos. ¿Qué significa el nombre? «Prolific» viene del simple hecho de que se trata de una red en expansión continua, que registra nuevos dominios casi a diario. En cuanto a «Puma»... analizaremos su procedencia más tarde en este documento.

La economía de la ciberdelincuencia es la tercera más grande del mundo, con un valor estimado de 8 billones de dólares en 2023; Prolific Puma forma parte de la cadena de suministro.[1] Crean nombres de dominio con un RDGA y los utilizan para ofrecer servicios de acortamiento de enlaces a otros actores maliciosos, ayudándolos a evadir la detección al distribuir phishing, estafas y malware. Si desmantelamos Prolific Puma, paralizamos un gran segmento de la economía delictiva. La Figura 1 ofrece una visión general de las operaciones de Prolific Puma y de cómo habilita a los delincuentes. Prolific Puma genera grandes volúmenes de dominios con algoritmos, que luego utiliza para crear enlaces acortados en nombre de otros actores maliciosos, lo que permite a estos ocultar su verdadera actividad.

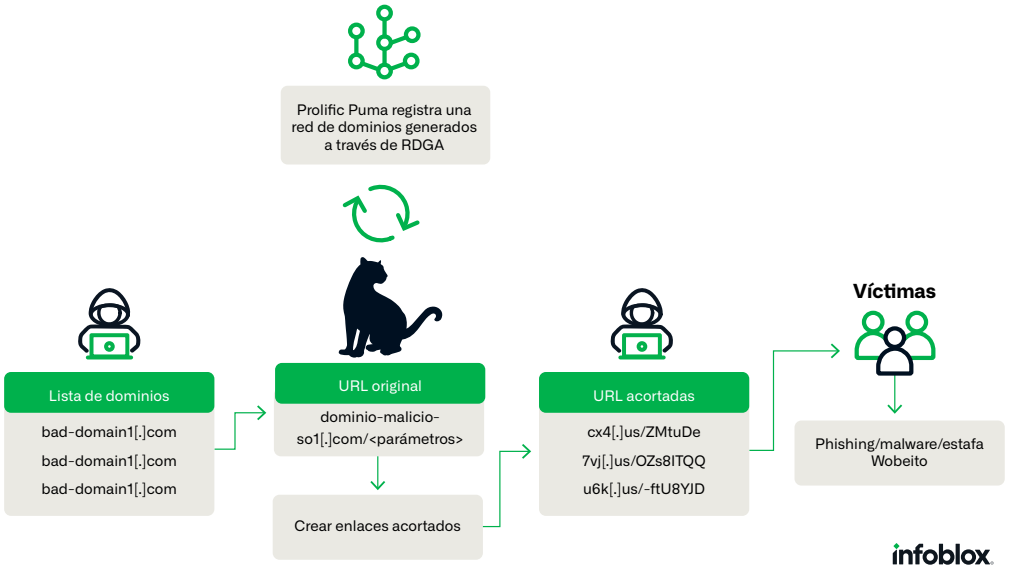


Figura 1. Visión general del papel de Prolific Puma en la cadena de suministro de la ciberdelincuencia.

Según nuestros datos, este documento ofrece la primera descripción de un extenso servicio clandestino de acortamiento de enlaces. Además, **el actor no se descubrió a través de malware o sitios de phishing, sino de análisis del DNS**. Prolific Puma es digno de mención porque ha sido capaz de facilitar actividades maliciosas durante más de 18 meses y pasar desapercibido en el sector de la seguridad. Gracias a su ingente catálogo de nombres de dominio, logra distribuir tráfico malicioso y eludir la detección.

1 https://cybernews.com/editorial/cybercrime-world-third-economy/

Este descubrimiento demuestra el poder de usar el DNS y los datos de registro de dominios tanto para detectar actividades sospechosas como para resumir esa información en una vista consolidada sobre un actor de amenazas del DNS. Si bien hemos podido detectar y rastrear a Prolific Puma a través del DNS, su caso pone de relieve los retos a los que se enfrentan los registradores y registros de dominios para controlar los abusos. Cuando los actores se distancian del delito real, las políticas pueden dificultar la capacidad de identificar y eliminar los dominios facilitadores.

Nos **percatamos por primera vez de los dominios de Prolific Puma hace seis meses a través de un detector de RDGA**. Desde entonces, hemos desarrollado una mejor comprensión de su actividad, utilizando detectores del DNS especializados para rastrear la red a medida que evoluciona. En los apartados siguientes, hablaremos del servicio de acortamiento de enlaces Prolific Puma, de cómo registra y aloja dominios, de su abuso del dominio de primer nivel .us (usTLD) y del papel que desempeña en la facilitación de la delincuencia en internet. A efectos de la presente publicación, nos centramos expresamente en el actor y su uso del DNS, más que en las campañas que utilizan sus servicios. Incluimos un ejemplo detallado de una campaña desarrollada con la infraestructura de Prolific Puma, que provocó tanto phishing como entrega de malware basado en navegador a los usuarios.

OSCUROS SERVICIOS DE ACORTAMIENTO DE ENLACES

Prolific Puma ofrece un servicio sumergido de acortamiento de enlaces a delincuentes.[2] Al acceder a un dominio de segundo nivel (SLD) activo, se envía directamente el siguiente mensaje:

```
{"type": "service","name":"@link-shortener/handler-service"}
```

El propósito original de los acortadores era facilitar la distribución de enlaces web y respetar las limitaciones de longitud de las redes sociales. Por ejemplo,

- el enlace `https://tinyurl.com/c6u6myhw` es una versión abreviada de
- https://blogs.infoblox.com/cyber-threat-intelligence/introducing-dns-threat-actors/, nuestro documento que introdujo el concepto de actores de amenazas del DNS.

Cuando un usuario hace clic en el enlace acortado, se le redirige a otra URL. En segundo plano, se envía una solicitud al DNS para resolver la dirección IP del dominio del servicio de acortamiento, por ejemplo, `tinyurl[.]com`. A continuación, se envía la solicitud web a esa dirección con el valor hash utilizado para identificar el sitio original. En el ejemplo anterior, el servicio TinyURL utilizará el valor c6u6myhw para determinar adónde debe redirigir la conexión. Se efectuarán solicitudes adicionales al DNS para localizar la dirección IP que aloja el contenido de destino, en este caso, en `blogs.infoblox.com`. Mientras que los usuarios legítimos crearán un simple enlace acortado para compartir una URL, un actor malicioso puede utilizar múltiples capas de redireccionamiento antes de llegar a la página de destino final. Este proceso se representa en la Figura 2.

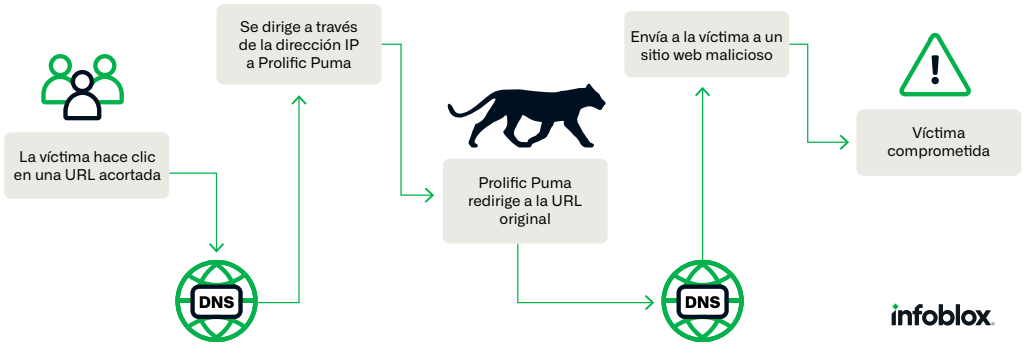


Figura 2: Una ruta teórica muestra cómo una URL acortada interactúa con el DNS y el servicio de acortamiento para redirigir a la víctima hacia contenido malicioso.

2 https://es.wikipedia.org/wiki/Acortador_de_URL

Es sabido que los actores maliciosos abusan de los acortadores de enlaces para destinarlos al phishing.[3] Sin embargo, en los casos más difundidos, los acortadores de enlaces son servicios conocidos y disponibles de forma pública, como TinyURL, BitLy y Google. Este abuso es tan desenfrenado que la firma de marketing Rebrandly recomienda a las empresas legítimas que eviten usar los acortadores populares en sus correos electrónicos.[4]

Prolific Puma no publicita abiertamente sus servicios. Durante un tiempo, sabíamos que estábamos rastreando un servicio de acortamiento de enlaces, pero no estaba claro qué ofrecían ni a quién prestaban sus servicios. La dificultad de investigar acortadores de enlaces es que, sin una URL completa, no es posible determinar la página de destino final. Nuestros detectores habían hallado un gran número de dominios interconectados con comportamientos sospechosos y sin presencia pública, pero nos costó determinar para qué se utilizaban.

Al final, captamos varios casos de enlaces acortados que redirigían a páginas de destino final de phishing y estafas. Curiosamente, la secuencia de redirecciones hasta la página final variaba ampliamente. En algunos casos, los enlaces acortados llevaban directamente al contenido.[5] En otros, había múltiples capas de redirección previas a la página de destino final.[6] También vimos enlaces acortados de Prolific Puma redirigidos a otro enlace acortado generado por un servicio distinto.[7] En algunos casos, el enlace acortado conducía a un CAPTCHA.[8] También hallamos denuncias de que los enlaces de Prolific Puma se habían enviado a través de SMS con notificaciones de entregas de Amazon falsas ya en enero de 2020.[9] Por la variación en la forma en que se manejaron los enlaces y el contenido entregado, es muy probable que Prolific Puma preste servicio a diversos actores. Las pruebas sugieren que los enlaces acortados se entregan principalmente a las víctimas a través de SMS, pero podrían usarse en otros contextos, por ejemplo, redes sociales y anuncios.

Prolific Puma no es el único servicio ilícito de acortamiento de enlaces que hemos descubierto, pero sí el más extenso y el más dinámico. No hemos encontrado ningún contenido legítimo que se sirva a través de su acortador. Más adelante en este informe se detalla un ejemplo específico de un enlace acortado que conduce a un proceso de phishing para obtener información del usuario, solicitar un pago fraudulento y distribuir malware en el navegador.

Como proveedor de servicios para el ecosistema de la ciberdelincuencia, Prolific Puma ayuda a otros actores maliciosos a no ser detectados, táctica incluida en el marco empresarial MITRE ATT&CK.[10] Sin embargo, su papel indirecto en la presentación de phishing, estafas y malware a los consumidores también le ayuda a evitar la detección. Si bien los proveedores de seguridad pueden identificar y bloquear el contenido final, sin una visión más amplia es difícil ver el alcance total de la actividad y asociar los dominios a un mismo actor de amenazas del DNS. Como veremos a continuación, podemos conseguirlo mediante análisis del DNS.

3 https://portswigger.net/daily-swig/cybercriminals-use-reverse-tunneling-and-url-shorteners-to-launch-virtually-undetectable-phishing-campaigns

4 https://support.rebrandly.com/hc/en-us/articles/228632488-Blacklisted-URL-Shorteners-Stop-Using-Them-in-Emails-

5 https://urlscan.io/result/3be86d9f-e596-4a9b-9260-d331811262e5/

6 https://urlscan.io/result/00c1d82d-0f03-44b6-96d3-63b503fff464/

7 https://urlscan.io/result/26077ac3-1559-4329-ab48-120181555586/

8 https://urlscan.io/result/726b6baa-d259-4f67-a4f9-aef3bd93aca3/

9 https://turbolab.it/amazon-2444/sms-amazon-hai-messaggio-riguardante-articolo-nome-arrivato-3.-classifica-2960

10 https://attack.mitre.org/tactics/TA0005/

DETECCIÓN Y CARACTERÍSTICAS DE LOS NOMBRES DE DOMINIO

Con el fin de proporcionar inteligencia original para los productos Infoblox de detección y respuesta del DNS en la nube e in situ, hemos diseñado un extenso corpus de algoritmos independientes para detectar dominios sospechosos y maliciosos, así como direcciones IP relacionadas y otros recursos del DNS. **Mediante la agregación de registros de consultas al DNS pasivo (pDNS) y otras fuentes de datos, ejecutamos una serie de análisis sobre una colección de dominios recién consultados, registrados o configurados**. Estos análisis, que caracterizan los dominios de forma independiente, comprenden desde marcar un dominio como sospechoso hasta asignarlo a un actor de amenazas del DNS.

El descubrimiento de Prolific Puma siguió una ruta común a muchos de los actores de amenazas del DNS que nombramos y rastreamos internamente. A partir de nuestros análisis automatizados, primero etiquetamos como sospechosos algunos dominios relacionados individualmente. Esta asociación permitió bloquear los dominios en nuestros solucionadores recursivos del DNS para proteger a los clientes, pero no captó la actividad en toda su amplitud ni correlacionó los dominios con un único actor. **Cuando desplegamos algoritmos para descubrir RDGA en primavera de 2023, empezaron a identificarse dominios de Prolific Puma en grupos**. Estos grupos también se determinaron automáticamente, pero se utilizaron métodos estadísticos para garantizar con un alto grado de confianza que los dominios RDGA habían sido registrados por el mismo actor de amenazas del DNS. Por último, otro algoritmo identificó comportamientos atípicos en las resoluciones de IP y correlacionó los grupos RDGA individuales. El ingente tamaño de la actividad nos hizo derivar el perfil de este actor de amenazas del DNS en particular a la investigación con contribución humana, y diseñamos huellas del DNS especializadas con fines de rastreo. En el resto de esta sección, daremos detalles sobre las características de los nombres de dominio de Prolific Puma y los rasgos que los identifican.

Puesto que la conexión entre los dominios de Prolific Puma y las páginas de destino final es indirecta, el actor tiene cierta protección frente a la detección. No obstante, también fortalece su capacidad de persistir y de pasar desapercibido mediante el registro de un elevado número de dominios. El tráfico malicioso se divide entre estos dominios, que reciben volúmenes bastante bajos. Con el tiempo, los dominios pueden incluso obtener «buena» reputación por medio del envejecimiento estratégico, técnica utilizada por Prolific Puma que detallaremos más adelante en este artículo.

Prolific Puma controla una de las mayores redes que rastreamos. Desde abril de 2022, ha registrado entre 35.000 y 75.000 nombres de dominio únicos. La Figura 3 muestra el número de nombres de dominio únicos registrados al día utilizando denominaciones de 3 o 4 caracteres de longitud. Como comunicamos recientemente, los RDGA sustituyen cada vez más a los DGA tradicionales y plantean nuevos retos a los defensores. El uso de esta técnica les permite automatizar fácilmente sus operaciones a escala; los dominios de Prolific Puma se cuentan entre los miles de nuevos dominios que Infoblox detecta a diario, generados por un RDGA.

Prolific Puma utiliza NameSilo como registrador de nombres de dominio y tiende a envejecer estratégicamente sus dominios antes de alojar su servicio con proveedores anónimos. Pese a la falta de una relación clara con Estados Unidos, Prolific Puma abusa constantemente del dominio de nivel superior . us (USTLD), TLD en principio reservado para ciudadanos y organizaciones estadounidenses. Prolific Puma es conocido por registrar tanto dominios nuevos como dominios caducados. Por ejemplo, 3ty[.]us había sido utilizado por otro actor en junio de 2022 para llevar a cabo campañas de phishing en Facebook Messenger. Después, Prolific Puma lo registró cuando caducó su registro en julio de 2023.

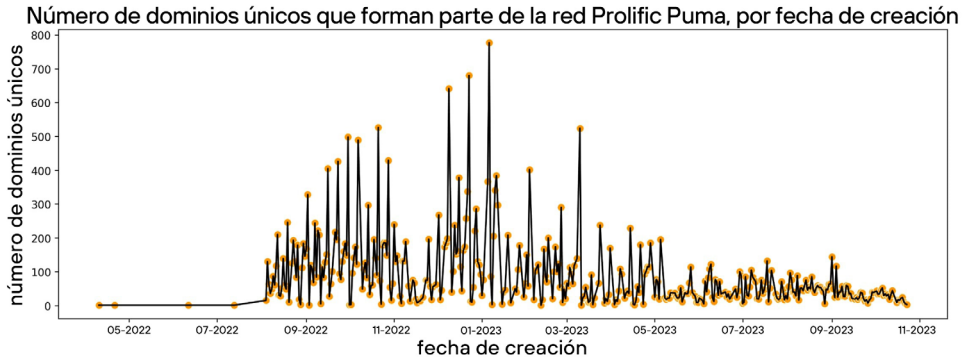


Figura 3. Cronología del registro de dominios de Prolific Puma que contienen denominaciones de 3 o 4 caracteres.

Los dominios de Prolific Puma son alfanuméricos, pseudoaleatorios, de longitud variable, normalmente de 3 o 4 caracteres, aunque hemos observado también denominaciones SLD de hasta 7 caracteres. Los dominios están registrados en 13 TLD de los que abusan actores maliciosos con frecuencia, entre ellos: `info`, `us`, `site`, `in`, `link`, `me`, `cc`, `website`, `life`, `xyz`, `club`, `buzz` y `best`. infoTLD representó la mayor parte de los dominios hasta mayo de 2023. Desde entonces, el actor ha utilizado usTLD en aproximadamente el 55% del total de dominios creados. De media, observamos 43 nuevos dominios a diario desde mayo de 2023.

TLD	us	link	info	com	cc	me
Dominios	vf8[.]us	cewm[.]link	uelr[.]info	kfwpr[.]com	jlza[.]cc	scob[.]me
	2ug[.]us	wrzt[.]link	ldka[.]info	trqrh[.]com	hpko[.]cc	xnxk[.]me
	z3w[.]us	hhqm[.]link	fbvn[.]info	nhcux[.]com	ddkn[.]cc	zoru[.]me
	yw9[.]us	ezqz[.]link	baew[.]info	khrig[.]com	mpsi[.]cc	mjzo[.]me
	8tm[.]us	zyke[.]link	shpw[.]info	dvcgg[.]com	wkby[.]cc	ouzp[.]me

Tabla 1: Ejemplos de dominios registrados por Prolific Puma en diferentes TLD con denominaciones de 3 o 4 caracteres.

En los últimos 18 meses, Prolific Puma ha utilizado principalmente NameSilo para registros y servidores de nombres. NameSilo, proveedor de nombres de dominio y alojamiento de bajo coste, sufre abusos frecuentes por parte de actores maliciosos. Además de precio económico, ofrece una API —al igual que muchos registradores— que facilita el registro masivo tanto por parte de usuarios legítimos como de delincuentes. Para registrar un dominio con NameSilo solo es necesaria una dirección de correo electrónico y un método de pago. Sin embargo, para configurar el dominio para su uso, se requiere un nombre y un domicilio físico. Los dominios registrados pero no configurados se aparcan; la dirección IP que comunica el DNS pertenece a SEDO Gmbh y forma parte del Servicio de Listado Múltiple premium que ofrece SEDO a los registradores.

> ***Infoblox utiliza una amplia gama de puntuaciones de reputación como características de análisis. Nuestro algoritmo de reputación está públicamente disponible, se aplica a todos los tipos de datos y es estadísticamente óptimo, lo que significa que no hay otro algoritmo más preciso para los mismos datos. Las puntuaciones se ajustan a una distribución normal, que puede interpretarse de forma uniforme a lo largo del tiempo y del tipo de datos. Una puntuación de 7 se considera de alto riesgo y se sitúa entre 1,5 y 3,5 desviaciones típicas por encima de la media. El análisis histórico de la reputación de los registradores y la reputación de los servidores de nombres se halla en nuestros informes trimestrales de inteligencia sobre amenazas correspondientes al 3T y 4T de 2022, respectivamente.***

NameSilo es un registrador sometido a numerosos abusos, según el algoritmo de reputación de Infoblox. Actualmente calificamos el riesgo de los dominios registrados con NameSilo con un 7 en una escala de 0 a 10, donde 10 se considera un riesgo extremadamente alto y 5 es el valor medio. Más allá de los TLD, también podemos aplicar nuestro algoritmo de reputación a servidores de nombres. Prolific Puma utiliza los servidores de nombres predeterminados de NameSilo, asignados al `dominio dnsowl[.]com`.[11] Actualmente, nuestro algoritmo califica el riesgo de los servidores de nombres `dnsowl[.]com` con un 6, que es moderado, aunque algo elevado en comparación con todos los demás servidores de nombres conocidos.

Aunque no es extraño que los actores de amenazas del DNS utilicen un mismo registrador para todas sus operaciones, no es lo habitual; usar un único registrador es una característica definitoria en nuestra taxonomía de actores de amenazas de DNS. Los actores que rastreamos suelen llevar más de un año en activo y, a menudo, se basan en motivaciones económicas. Vemos que con frecuencia eligen los registradores y TLD más baratos y que crean menos complicaciones. Aunque NameSilo es un registrador de bajo coste, no es el único y no ofrece el precio más bajo para dominios en un período prolongado. En el pasado, Prolific Puma registró un gran número de dominios con otros proveedores baratos, en particular NameCheap. El uso continuo de NameSilo durante largo tiempo es digno de mención, pero se desconocen los motivos subyacentes.

ABUSO DE usTLD

Desde mayo de 2023, Prolific Puma ha registrado miles de dominios usTLD. Es un dato notable porque, de acuerdo con la Política de Requisitos Nexus de usTLD, solo los ciudadanos estadounidenses —o las empresas afiliadas a EE. UU.— pueden registrar dominios con esta extensión.[12] Además, usTLD exige transparencia; no es posible registrar ningún nombre de dominio de forma privada. Como resultado, la dirección de correo electrónico, el nombre, el domicilio y el número de teléfono asociados con el dominio están expuestos públicamente. Aunque pueda parecer un probable elemento disuasorio para delincuentes, no ha sido eficaz; usTLD es famoso por los abusos que sufre.

Como informó recientemente Krebs on Security, usTLD es uno de los TLD con código de país (ccTLD) de los que más se abusa, y no se verifica en modo alguno la relación del registrante con Estados Unidos.[13] Si bien Krebs responsabiliza a GoDaddy como registro, el TLD sufrió abusos antes de que asumieran las responsabilidades del registro en 2020. Si bien en principio era un TLD altamente estructurado y controlado, los registros de dominio de segundo nivel (SLD) comenzaron en 2002, cuando se adjudicó a Neustar el contrato para administrar el TLD.[14] Infoblox asigna a usTLD un riesgo moderado, ligeramente elevado, con una puntuación de 6, en comparación con los demás TLD.

Para registrar un dominio `.us` con NameSilo, se requiere una dirección de correo electrónico, así como seleccionar una de las cinco categorías Nexus y la finalidad de la solicitud, como se muestra en la Figura 4. Estos datos se utilizan para determinar la asociación del registrante con Estados Unidos; sin embargo, los criterios de aceptación son muy amplios.[15] Durante el proceso de registro, se advierte al usuario de que debe cumplir los requisitos de una de estas opciones y efectuar una selección. El requisito de la finalidad de la aplicación separa los registros personales de los registros empresariales.

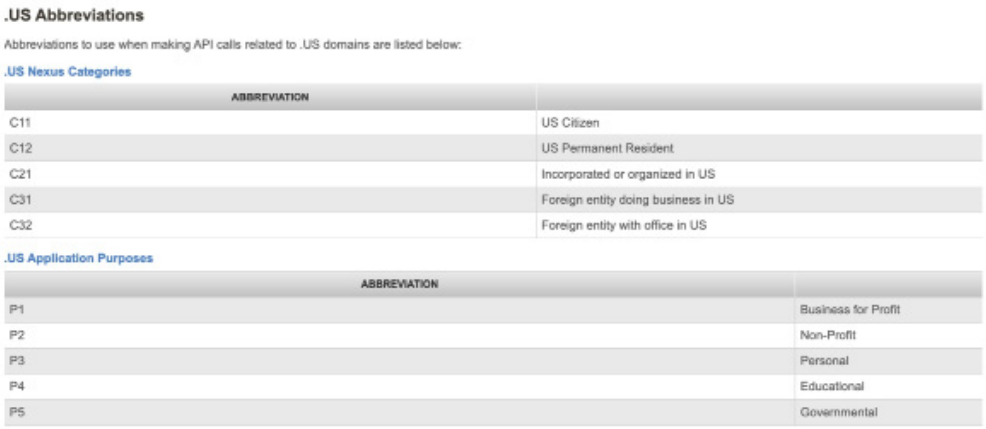
11 https://www.namesilo.com/support/v2/articles/domain-manager/dns-troubleshooting

12 https://www.about.us/faqs

13 https://krebsonsecurity.com/2023/09/why-is-us-being-used-to-phish-so-many-of-us/

14 https://es.wikipedia.org/wiki/.us

15 https://www.namesilo.com/popups/us_abbreviations.php



.US Abbreviations

Abbreviations to use when making API calls related to .US domains are listed below:

.US Nexus Categories

ABBREVIATION	
C11	US Citizen
C12	US Permanent Resident
C21	Incorporated or organized in US
C31	Foreign entity doing business in US
C32	Foreign entity with office in US

.US Application Purposes

ABBREVIATION	
P1	Business for Profit
P2	Non-Profit
P3	Personal
P4	Educational
P5	Governmental

Figura 4. Los registrantes de nombres de dominio con usTLD deben elegir una categoría Nexus relacionada y la finalidad de la aplicación entre las enumeradas previamente. Esta información se publica en el registro WHOIS.

Para configurar el dominio con NameSilo por completo, el registrante también debe proporcionar un nombre, un domicilio físico y un número de teléfono, si bien estos no se verifican y los registros WHOIS asociados no se actualizan automáticamente. A falta de actualización, solo está disponible públicamente la dirección de correo electrónico asociada con la compra. El registrante puede optar por vincular la información de contacto con nombres de dominio adquiridos anteriormente, pero es una configuración independiente, sin conexión con los datos del titular de la cuenta. Todo este proceso se puede completar con datos falsos y el dominio se puede abonar con Bitcoin, lo que permite a los actores de amenazas abusar del servicio sin gran dificultad. Si bien NameSilo es el registrador del que se abusa en este caso concreto, las dificultades aquí señaladas son comunes en todo el sector.

En un principio, los registrantes de los dominios de Prolific Puma afirmaban ser ciudadanos estadounidenses (C11) y utilizar los dominios para actividades con ánimo de lucro (P1), aunque este patrón ha cambiado recientemente. **Desde el 4 de octubre, observamos que los dominios de Prolific Puma en usTLD han pasado a ser dominios para uso personal (P3) con configuraciones de registro privadas, tanto para los registros ya existentes como para los nuevos**. Esta actividad ha despejado todas las dudas acerca de si Prolific Puma era un actor malicioso o no. Desde mediados de octubre, cerca de 2000 dominios de Prolific Puma en usTLD tienen registro privado.

La presencia de registros privados en usTLD es alarmante y vulnera las condiciones de usTLD. La falta de información detallada en los datos de WHOIS ha obstaculizado las investigaciones de inteligencia en los últimos años; es más, según nuestra experiencia directa con NameSilo, no es posible seleccionar el registro privado de dominios en usTLD a través de su interfaz y, aun así, ha sucedido. Al profundizar en la cuestión y evaluar todos los dominios que procesamos entre el 1 de septiembre y el 15 de octubre, vemos que Prolific Puma era responsable de la gran mayoría de los dominios .us con protección de PrivacyGuardian, pero había más. De los más de 200 registradores que informaron notificaron usTLD en ese periodo, solo cuatro estaban relacionados con datos de registro privados, como se muestra en la tabla siguiente. **Del total de dominios con registro privado, más del 99% se hallaban en NameSilo**. De momento, no podemos explicar esta conducta.

Registrador	Número de dominios (1/9/23–15/10/23)
NameSilo – Prolific Puma	1062
NameSilo – posiblemente no de Prolific Puma	411
PorkBun	5
NameCheap	4
Sav.com	1

Tabla 2. Dominios con registro privado en usTLD por registrador. Infringen las políticas de usTLD.

Aunque las limitaciones de los nombres de dominio `.us` pueden parecer estrictas, si se examinan con más detalle, solamente se excluye del registro de dominios del TLD a las entidades totalmente extranjeras. Si se sospecha que el registrante ha facilitado información WHOIS falsa, la Corporación de Internet para la Asignación de Nombres y Números (ICANN) exige al registrador que investigue y actualice la información.[16] Según la política de requisitos de Nexus, los registradores deben conceder a los registrantes un plazo de 30 días para que actualicen la información incompleta o incorrecta. NameSilo y GoDaddy están mejor posicionados para desactivar dominios por actividad maliciosa que por su calificación en Nexus. No obstante, en el caso de adversarios de capa media, como Prolific Puma, ¿cómo lo hacen exactamente?

El abuso de usTLD, similar al de otros como `.xyz` y `.website`, es real, pero con las normativas y tecnologías de privacidad modernas, distinguir entre abuso y uso legítimo no es tan sencillo, sobre todo a la escala del DNS. Proteger a los consumidores y a las organizaciones contra los actores de amenazas del DNS requiere la colaboración del sector. Por lo que a nosotros respecta, informamos tanto a NameSilo como a GoDaddy de la actividad de Prolific Puma en septiembre. Sin embargo, aparte de la posible violación de los requisitos de usTLD, es difícil para un registrador tomar medidas relativas a dominios que no se utilizan con fines maliciosos directos. También hemos remitido un extenso listado de dominios recientes a Spamhaus y otros proveedores.[17]

CARÁCTER DE PROLIFIC PUMA

En esencia, los actores de amenazas son personas con peculiaridades propias, que a menudo se manifiestan en sus tácticas, técnicas y procedimientos (TTP). Los actores de amenazas de malware pueden distinguirse por los nombres de variables elegidos o por la forma de comentar el código. Estas elecciones pueden reflejar sus intereses, costumbres y sentido del humor. Los actores de amenazas del DNS no son distintos, aunque por lo general tenemos poca información con la que trabajar en los registros de dominios y el DNS.

En Infoblox, nos centramos en la actividad sospechosa y maliciosa en el DNS. Si bien atribuimos nombres de dominio a un actor de amenazas del DNS, rara vez tratamos de determinar su verdadera identidad o ubicación. Este tipo de trabajo de atribución, en el que los analistas intentan vincular la actividad de internet con el mundo físico, es un campo especializado que requiere mucho tiempo. Sin embargo, dado que Prolific Puma registra dominios en usTLD, donde no se permite el registro privado, podemos analizar brevemente la personalidad de Prolific Puma.

16 https://www.icann.org/resources/pages/inaccuracy-2013-03-22-es

17 https://www.spamhaus.org/

Siempre que sea posible, Prolific Puma utiliza el registro de dominios privado, pero el registro en usTLD es público. Para estos dominios, el actor utiliza siempre una dirección de correo electrónico que hace referencia a la canción October 33 de Black Pumas.[18] Black Pumas es una banda de soul psicodélico procedente de Austin (Texas), que saltó a la fama en 2019 con el tema Colors.[19] La canción October 33 no llegó a los primeros puestos de las listas de éxitos y, al igual que Prolific Puma, guarda algo de misterio.[20] Si bien las letras son una clara carta de amor, hacen referencia a la soledad; la música pretendía generar inquietud.[21] Pese a su nominación a los Grammy como mejor artista revelación en 2019, Black Pumas no son un grupo muy conocido. Prolific Puma utiliza el nombre de Leila Puma, de nuevo un nombre inventado, para referirse a Black Pumas. El nombre Leila proviene del árabe y significa «noche».

Aunque desconocemos la identidad real de Prolific Puma, tenemos una interesante perspectiva acerca de su personalidad, formada a partir de sus datos de registro. Además de referencias a Black Pumas y su misteriosa canción October 33, Prolific Puma utiliza una dirección de correo electrónico personal ucraniana. La dirección que proporciona es la de una escuela primaria en Polonia, un edificio anodino que podría hallarse en cualquier ciudad industrial. Łódź, la tercera ciudad de Polonia, acoge a refugiados ucranianos desde la invasión rusa en febrero de 2022.[22] Una versión de Black Pumas de la canción «Strangers» de The Kinks se utilizó para crear un emotivo vídeo que presenta a refugiados ucranianos en YouTube, titulado «Ukraine Strangers». Aunque no tiene nada que ver con las actividades de Prolific Puma, este vídeo tuvo un alcance importante en otoño de 2022.[23] Como hemos indicado antes, la información del registrante no está verificada por NameSilo y parece falsa, pero las opciones elegidas nos permiten hacernos una idea de quiénes están detrás de Prolific Puma.

OPERACIONES DE PROLIFIC PUMA

Después de registrar un dominio, Prolific Puma suele dejarlo sin usar o aparcado varias semanas. Esta técnica se conoce como **envejecimiento estratégico**.[24] Dado que los ataques de phishing suelen estar vinculados a dominios recién registrados, muchos sistemas de seguridad bloquean el acceso a ellos. En respuesta, los actores de amenazas descubrieron que, si esperaban un tiempo antes de usar los dominios en sus campañas (los envejecían), podían eludir muchas protecciones de seguridad.

Prolific Puma efectúa una cifra baja de consultas al DNS durante el periodo de envejecimiento, método que utilizan los actores de amenazas para crear una buena reputación para los nombres de dominio. Durante este período, los dominios se aparcan con NameSilo. Luego, Prolific Puma los transferirá a proveedores de alojamiento «a prueba de balas», suscritos con Bitcoin, en un servidor privado virtual (VPS) con una dirección IP dedicada. Hemos descubierto que, al cabo de un tiempo, abandonan los dominios y dejan el registro de DNS enlazado con la dirección IP dedicada.

Basándonos en la variedad de técnicas operativas observadas, sospechamos que Prolific Puma proporciona servicios a terceros y que las páginas de destino final no están bajo su control. Sin embargo, aun así es posible que el mismo actor de amenazas controle tanto el

18 https://www.blackpumas.com/

19 https://es.wikipedia.org/wiki/Black_Pumas

20 https://www.youtube.com/watch?v=an3AkQL62F8

21 https://www.facebook.com/theblackpumas/videos/black-pumas-oct-33-song-breakdown/461719384620852/

22 https://eurocities.eu/latest/ukrainian-refugee-integration-in-lodz-and-timisoara/#:~:text=The%20city%20of%20Lodz%20in,refugees%20since%20the%20Russian%20invasion

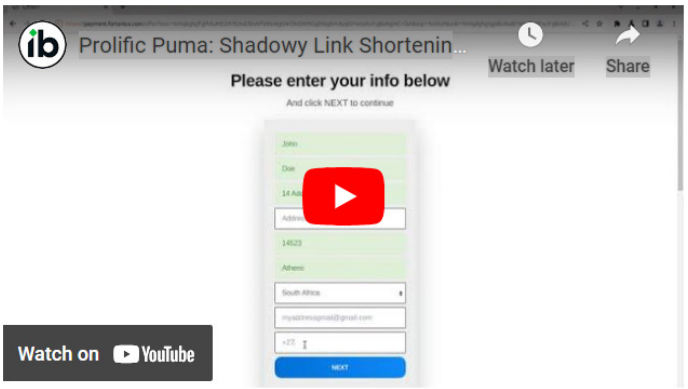
23 https://www.youtube.com/watch?v=D_Ap_7wjHIs

24 https://heimdalsecurity.com/blog/aged-domains-the-silent-danger-to-cybersecurity-new-report/

servicio de acortamiento de enlaces como toda la actividad maliciosa que se lleva a cabo a través de él. No hemos determinado cómo publicita sus servicios Prolific Puma, cómo reciben sus usuarios las URL acortadas o si gestiona también tráfico legítimo. En las campañas a través del servicio de Prolific Puma, hemos visto extensas redes de dominios controlados por otros actores de amenazas del DNS, a menudo registrados con proveedores de bajo coste como NameCheap. Algunos dominios de estas campañas se han generado mediante RDGA.

EJEMPLO DE CAMPAÑA

Prolific Puma gestiona un servicio de acortamiento de enlaces para diversas actividades de phishing, estafas y malware. Aquí describimos un ejemplo de una de estas campañas. Las Figuras 5.1-5.4 muestran capturas de pantalla de lo que ve una víctima al hacer clic en el enlace acortado inicial, `http://bwkd[.]me/ZFjfA3`. El enlace redirige a una página de phishing diseñada a semejanza de un correo electrónico, en la que se solicita al usuario que facilite datos personales y efectúe un pago. A continuación, infecta al usuario con malware mediante una extensión del navegador. También hemos capturado el proceso en pantalla; se muestra a continuación.



Los pasos técnicos entre el enlace acortado y el malware como extensión del navegador en esta campaña son los siguientes:

- El primer enlace acortado `http://bwkd[.]me/ZFjfA3` redirige a
- `http://ksaguna[.]com/click.php?key=<censurado>`, que a su vez redirige a
- `https://www[.]asdboloa[.]com/ZA/AB_zagopb/?uclick=<redacted>`
  - » La web final es un mensaje de Gmail falso, que indica al usuario que ha obtenido la posibilidad de probar el nuevo iPhone 15.
- Se solicita al usuario que, para obtener su teléfono, haga clic en el enlace `https://www[.]game[.]co[.]za/2023program` e introduzca sus datos de envío. El sitio web `www[.]game[.]co[.]za` es una tienda de descuentos sudafricana que utiliza campañas promocionales para atraer consumidores.
- Al hacer clic en este enlace en las condiciones adecuadas, se abre una interfaz que requiere pagar 18 rands sudafricanos (ZAR) para participar en la prueba.
- Después, se presenta al usuario una página que afirma ser de seguimiento postal y se le solicita que acepte las notificaciones de `fubsdgd[.]com`. Al hacer clic en «Aceptar», se activa la instalación de un malware en el navegador, que utiliza el servicio OneSignal para enviar notificaciones. Si bien se asocia normalmente con anuncios, según nuestra experiencia, el malware en extensiones de navegador suele utilizarse para remitir estafas, phishing y otros tipos de malware, además de anuncios.
- Por último, la víctima recibe una serie de indicaciones para que compruebe sus preferencias de envío e introduzca sus datos personales.

No sabemos cómo se envía la URL acortada original a la víctima; puede ser a través de SMS, dado que abre un mensaje de Gmail falso. Los dominios utilizados durante la explotación de la víctima cambian y forman parte de una extensa red. En esta campaña se utilizan diversas técnicas para garantizar a la víctima que la oferta es genuina, incluido un flujo activo de reseñas de otros «destinatarios» en cada paso.

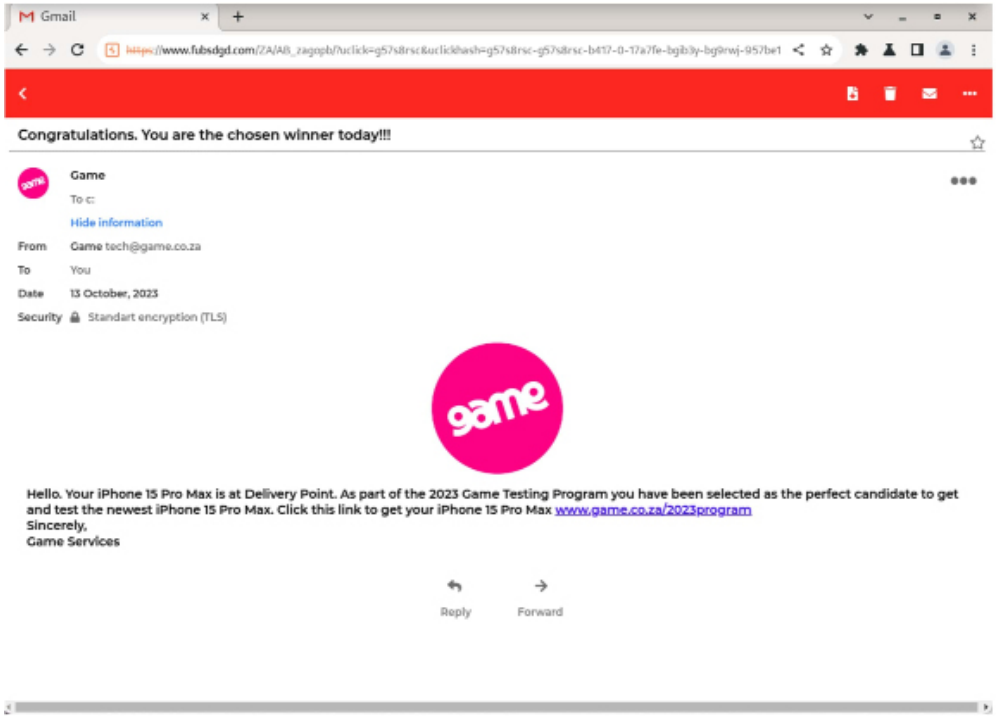


Figura 5.1: Ejemplo del contenido al que redirigen los acortadores de enlaces de Prolific Puma. El enlace acortado original (http://bwkd[.]me/ZFjfA3) redirige y termina por abrir una página de phishing diseñada para parecerse a un correo electrónico de Gmail.

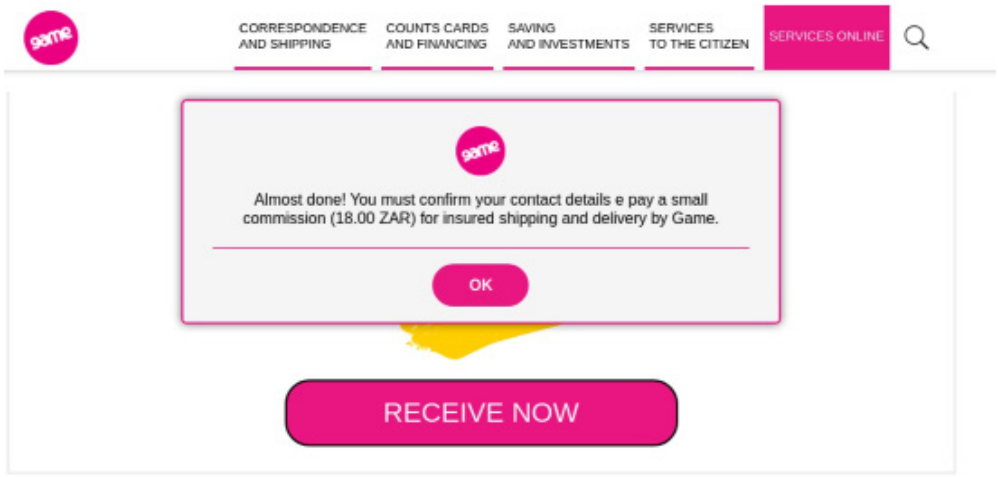


Figura 5.2. Paso de estafas y phishing en la campaña. Tras aceptar el iPhone gratis como se muestra en la Figura 5.1, se solicita al usuario que abone una cuota e introduzca su nombre y dirección.

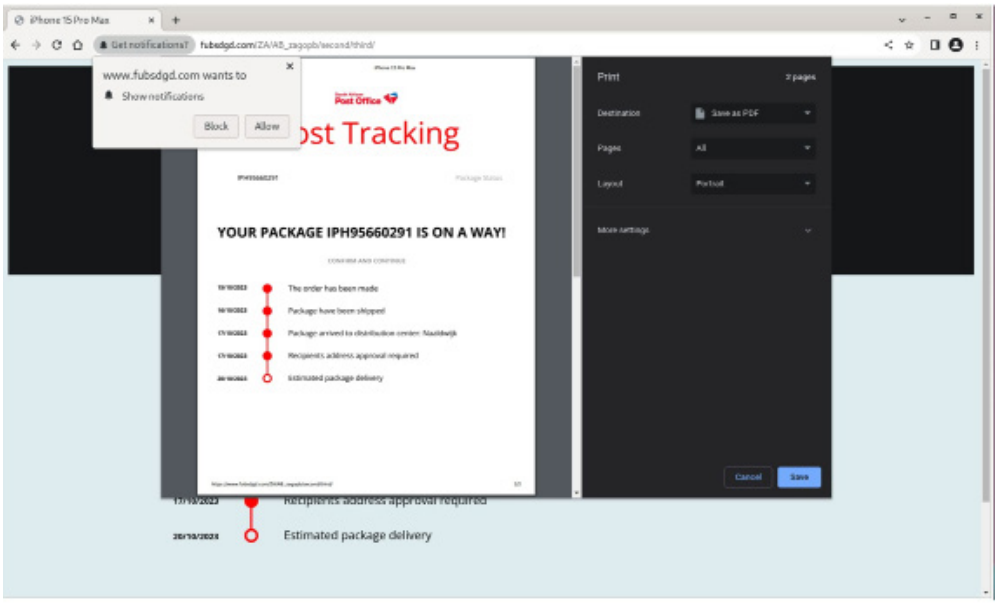


Figura 5.3. Paso de malware en la campaña. Una vez que la víctima abona la tarifa que se muestra en la Figura 5.2, recibe una notificación de envío del paquete y se le ofrece mostrarle notificaciones de fubsdgd[.]com. Si acepta las notificaciones, se envía el malware al dispositivo de la víctima.

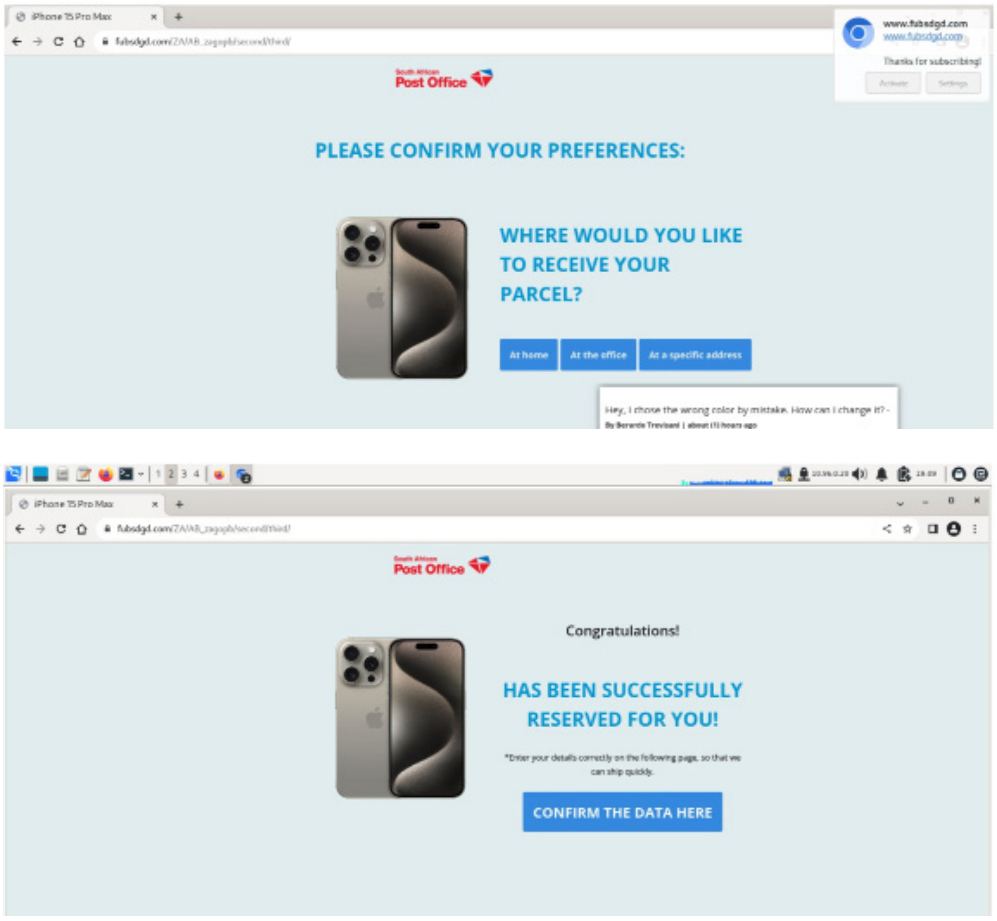


Figura 5.4a-b. Cuando el usuario acepta las notificaciones mostradas en la Figura 5.3, se le pide que especifique más datos y preferencias en una sucesión de pantallas.

CONCLUSIÓN

Prolific Puma demuestra cómo se puede abusar del DNS para respaldar actividades delictivas y pasar desapercibido durante años. Como parte de la cadena de suministro, este actor es más difícil de detectar y erradicar. Los sistemas de seguridad tradicionales protegen al usuario tomando como base la página de destino final de un enlace. Sin embargo, los sistemas de detección y respuesta del DNS pueden poner freno a Prolific Puma y a proveedores de servicios similares, derrotando así a todos los actores que cuentan con ellos para desarrollar actividades de phishing, estafas y malware. A través de un RDGA y registradores de dominios de bajo coste, Prolific Puma puede mantener y ampliar sus operaciones, pero, por otra parte, es posible detectar el uso de un RDGA en los DNS y los registros de dominios.

Prolific Puma es solo uno de los operadores de acortamiento de enlaces que ha descubierto Infoblox, y los acortadores de enlaces son solo uno de los tipos de servicio presentes en la economía sumergida. **Normalmente, primero descubrimos a los actores de amenazas del DNS a través de análisis que identifican dominios sospechosos recién registrados, configurados o consultados**. Incluso antes de correlacionar los dominios con actividades maliciosas, podemos usar otras características, como los TLD y la reputación del servidor de nombres, para marcar los dominios relacionados como sospechosos. Después, podemos conectar los dominios entre sí y aislar a un actor de amenazas. Al bloquear el acceso a los dominios sospechosos, las organizaciones pueden implementar una política de alta seguridad y eficacia sin lamentaciones para su red y sus usuarios.

INDICADORES DE ACTIVIDAD

A continuación se ofrece una pequeña selección de indicadores relacionados con Prolific Puma y las campañas que facilitan. Puede verse una lista más completa de indicadores recientes en nuestro repositorio abierto de GitHub aquí.

Indicador de actividad	Tipo de indicador
hygmi[.]com	Dominio del acortador de enlaces Prolific Puma
yyds[.]is	
0cq[.]us	
4cu[.]us	
regz[.]info	
u5s[.]us	
1jb[.]us	
jrbc[.]info	
uhje[.]me	
0md[.]us	
fh3[.]us	
0qa[.]us	
9jw[.]us	
iv0[.]us	
od9[.]us	
rpzp[.]me	

Indicador de actividad	Tipo de indicador
8fx[.]us	
3vb[.]us	
r1u[.]us	
zost[.]link	
9ow[.]us	
sf8i[.]us	
bu9[.]us	
ce2[.]us	
wf6[.]us	
v8z[.]us	
zj4[.]us	
rjvb[.]link	
fssu[.]link	
xbsf[.]link	
wqeh[.]link	

Indicador de actividad	Tipo de indicador
ymql[.]link 7tz[.]us w6q[.]us giqj[.]me u3q[.]us ke0[.]us v1u[.]us ti7[.]us 2zc[.]us gf6[.]us 6dr[.]us 6or[.]us kc0[.]us 0ty[.]us styi.info 6fe[.]us u8n[.]us d6s[.]us	
v8z[.]us zj4[.]us rjvb[.]link fssu[.]link xbsf[.]link wqeh[.]link ymql[.]link 7tz[.]us	IP de alojamiento del acortador de enlaces

Indicador de actividad	Tipo de indicador
bwkd[.]me ksaguna[.]com asdboloa[.]com game.co[.]za	Redirección y páginas de destino
fubsdgd[.]com	Dominios de malware en extensiones de navegador
blackpumaoct33@ukr[.]net	Correo electrónico de registro de Prolific Puma

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: 20241008v1