Un individuo amenazante conocido como *«Prolific Puma»* ha mantenido un perfil discreto y opera un servicio de acortamiento de enlaces clandestino que ofrece a otros individuos amenazantes durante al menos los últimos cuatro años.

> *«Prolific Puma crea nombres de dominio utilizando un algoritmo de generación de dominio registrado (RDGA) y emplea estos dominios para proporcionar un servicio de acortamiento de enlaces a otros actores maliciosos, lo que les ayuda a eludir la detección mientras distribuyen ataques de phishing, estafas y software malicioso»,* según un análisis reciente de Infoblox basado en el análisis del Sistema de Nombres de Dominio (DNS).

Dado que se sabe que los actores maliciosos utilizan acortadores de enlaces para llevar a cabo ataques de phishing, este adversario desempeña un papel significativo en la cadena de suministro del cibercrimen, habiendo registrado entre 35,000 y 75,000 nombres de dominio únicos desde abril de 2022. «Prolific Puma» también es un actor amenazante de DNS que hace uso de la infraestructura de DNS con propósitos perniciosos.

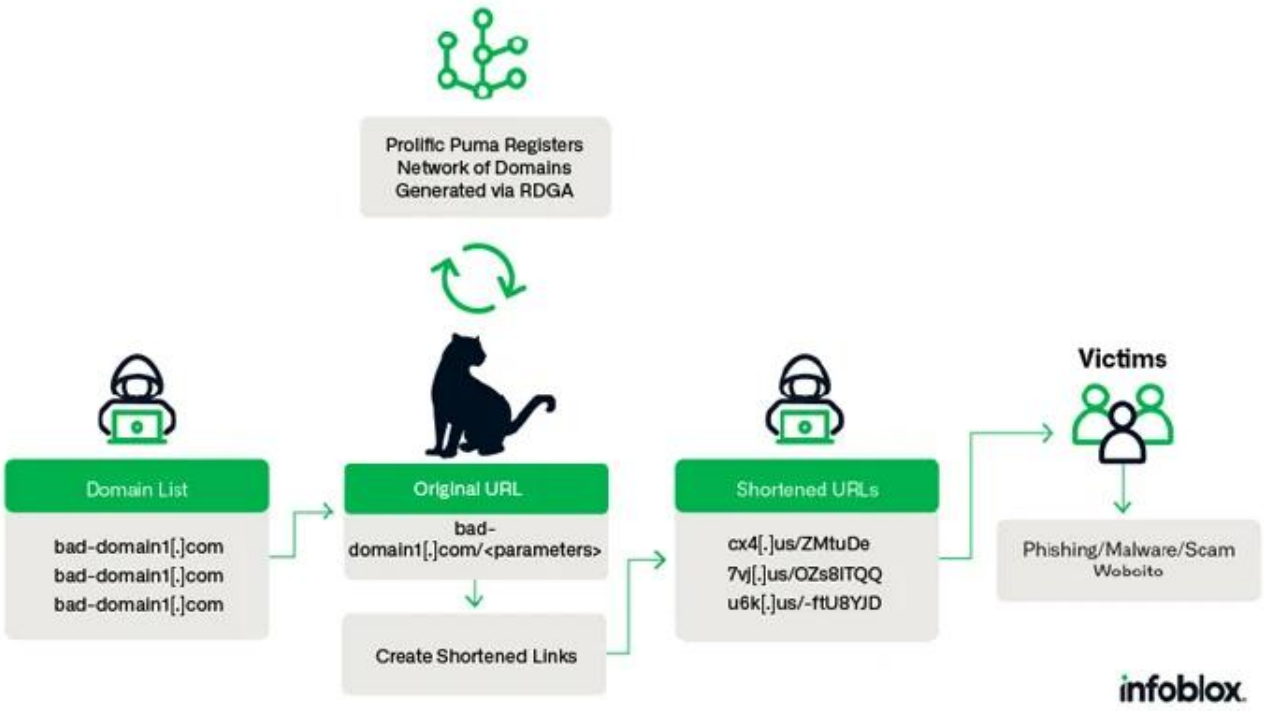
Un aspecto destacado de las operaciones del actor amenazante es el uso de una compañía estadounidense registradora de dominios y de alojamiento web llamada NameSilo para el registro y los servidores de nombres, debido a su accesibilidad y a una interfaz de programación de aplicaciones (API) que facilita el registro en masa.

«Prolific Puma», que no publicita su servicio de acortamiento de enlaces en mercados clandestinos, también ha sido observado empleando el envejecimiento estratégico para aparcar dominios registrados durante varias semanas antes de alojar su servicio con proveedores anónimos.

> *«Los dominios de Prolific Puma son alfanuméricos, pseudoaleatorios, con longitud variable, generalmente de 3 o 4 caracteres de largo, pero también se han observado etiquetas de segundo nivel (SLD) de hasta 7 caracteres»*, explicó

> Infoblox.

Además, el actor amenazante ha registrado miles de dominios en el dominio de nivel superior de EE. UU. (usTLD) desde mayo de 2023, utilizando repetidamente una dirección de correo electrónico que hace referencia a la canción «OCT 33» de una banda de soul psicodélico llamada Black Pumas: blackpumaoct33@ukr[.]net.




La verdadera identidad y el origen de «Prolific Puma» siguen siendo desconocidos hasta el momento. Sin embargo, se informa que varios actores amenazantes están utilizando esta oferta para dirigir a visitantes hacia sitios de phishing y estafas, desafíos CAPTCHA e incluso a otros enlaces acortados creados por un servicio distinto.

En una instancia de un ataque de phishing y malware documentado por Infoblox, las víctimas

que hacen clic en un enlace acortado son llevadas a una página de aterrizaje que les solicita proporcionar información personal y realizar un pago, infectando en última instancia sus sistemas con malware de complemento del navegador.

Esta revelación se produce semanas después de que la empresa expusiera a otro actor amenazante persistente de DNS, apodado «Open Tangle», que utiliza una gran infraestructura de dominios parecidos a los de instituciones financieras legítimas para dirigirse a consumidores en ataques de phishing y smishing.

> *«Prolific Puma demuestra cómo el DNS puede ser utilizado de forma perjudicial para respaldar actividades criminales y pasar desapercibido durante años»,* concluyó Infoblox.

## La herramienta de hackeo Kopeechka inunda plataformas en línea con cuentas falsas

Este desarrollo se produce tras la publicación de un nuevo informe de Trend Micro que revela que ciberdelincuentes con habilidades limitadas están empleando una herramienta recién creada llamada Kopeechka (que significa «penique» en ruso) para automatizar la creación de cientos de cuentas de redes sociales falsas en cuestión de segundos.

> Según el investigador de seguridad Cedric Pernet, *«este servicio ha estado operativo desde principios de 2019 y ofrece una manera sencilla de registrar cuentas en redes sociales populares, incluyendo Instagram, Telegram, Facebook y X (anteriormente conocido como Twitter)».*

Kopeechka ofrece dos tipos de direcciones de correo electrónico diferentes para facilitar el proceso de registro masivo: direcciones de correo electrónico alojadas en 39 dominios

propiedad del actor de amenazas y aquellas que se alojan en servicios de correo electrónico más ampliamente utilizados como Gmail, Hotmail, Outlook, Rambler y Zoho Mail.

> Pernet explicó que *«Kopeechka en realidad no proporciona acceso a las casillas de correo reales. Cuando los usuarios solicitan casillas de correo para crear cuentas en redes sociales, solo obtienen una referencia de la dirección de correo electrónico y el correo específico que contiene el código de confirmación o la URL».*

Existe la sospecha de que estas direcciones de correo electrónico son o bien comprometidas o creadas por los mismos actores de Kopeechka.

Dado que muchos servicios en línea requieren la verificación de números de teléfono para completar el proceso de registro, Kopeechka permite a sus clientes elegir entre 16 servicios de SMS en línea diferentes, la mayoría de los cuales tienen su origen en Rusia.

Además de acelerar las actividades del cibercrimen y proporcionar a los actores de amenazas la capacidad de llevar a cabo operaciones a gran escala, estas herramientas, concebidas dentro del modelo de negocio «como servicio», ponen de manifiesto la creciente profesionalización del ecosistema criminal.

> En palabras de Pernet, *«los servicios ofrecidos por Kopeechka pueden facilitar una forma sencilla y económica de crear cuentas en línea en gran cantidad, lo cual puede resultar de utilidad para los ciberdelincuentes».*

> Asimismo, señaló que *«aunque Kopeechka se utiliza principalmente para crear múltiples cuentas, también puede resultar útil para aquellos ciberdelincuentes que desean agregar un grado de anonimato a sus actividades, ya que no necesitan emplear sus propias direcciones de correo electrónico para crear cuentas en*

> *plataformas de redes sociales».*