Una avanzada plataforma de servicio de phishing conocida como Darcula ha fijado su objetivo en organizaciones de más de 100 países mediante el aprovechamiento de una extensa red de más de 20,000 dominios falsificados para ayudar a los delincuentes cibernéticos a llevar a cabo ataques a gran escala.

> *«La utilización de iMessage y RCS en lugar de SMS para enviar mensajes de texto tiene como consecuencia eludir los firewalls de SMS, lo cual se está utilizando con gran éxito para atacar al USPS junto con servicios postales y otras organizaciones establecidas en más de 100 países»,* indicó Netcraft.

Darcula ha sido utilizada en varios ataques de phishing de alto perfil durante el último año, donde los mensajes de smishing son enviados tanto a usuarios de Android como de iOS en el Reino Unido, además de aquellos que aprovechan señuelos de entrega de paquetes al hacerse pasar por servicios legítimos como USPS.

Un PhaaS en idioma chino, Darcula se promociona en Telegram y ofrece soporte para aproximadamente 200 plantillas que imitan marcas legítimas que los clientes pueden obtener por una tarifa mensual para configurar sitios de phishing y llevar a cabo sus actividades maliciosas.

La mayoría de las plantillas están diseñadas para simular servicios postales, pero también incluyen servicios públicos y privados, instituciones financieras, organismos gubernamentales (por ejemplo, departamentos de impuestos), aerolíneas y organizaciones de telecomunicaciones.

Los sitios de phishing están alojados en dominios registrados con propósito que suplantan los nombres de marca respectivos para agregar un aspecto de legitimidad. Estos dominios están respaldados por Cloudflare, Tencent, Quadranet y Multacom.

En total, se han detectado más de 20,000 dominios relacionados con Darcula en 11,000 direcciones IP, con un promedio de 120 nuevos dominios identificados por día desde el inicio

de 2024. Algunos aspectos del servicio PhaaS fueron divulgados en julio de 2023 por el investigador de seguridad israelí Oshri Kalfon.

Una de las características interesantes de Darcula es su capacidad para actualizar sitios de phishing con nuevas características y medidas anti-detección sin necesidad de eliminar y reinstalar el kit de phishing.

> *«En la página principal, los sitios de Darcula muestran una página falsa de venta/mantenimiento de dominios, probablemente como una forma de camuflaje para dificultar los esfuerzos de eliminación. En iteraciones anteriores, el mecanismo antimonitoreo de Darcula redirigiría a los visitantes que se creía que eran bots (en lugar de posibles víctimas) a búsquedas en Google de varias razas de gatos»*, señaló la empresa con sede en el Reino Unido.

Las tácticas de smishing de Darcula también merecen atención especial, ya que principalmente aprovechan Apple iMessage y el protocolo RCS (Servicios de Comunicación Enriquecida) utilizado en Mensajes de Google en lugar de SMS, evitando así algunos filtros implementados por los operadores de red para evitar que los mensajes fraudulentos lleguen a posibles víctimas.

> *«Aunque el cifrado de extremo a extremo en RCS e iMessage proporciona una valiosa privacidad para los usuarios finales, también permite a los delincuentes eludir los filtros requeridos por esta legislación al hacer que el contenido de los mensajes sea imposible de examinar para los operadores de red, dejando que la detección de spam en el dispositivo de Google y Apple y las aplicaciones de filtro de spam de terceros sean la principal línea de defensa para evitar que estos mensajes lleguen a las víctimas»*, agregó Netcraft.
>
> *«Además, no incurren en cargos por mensaje, que son típicos para SMS, lo que*

> *reduce el costo de entrega».*

Aparte del phishing basado en SMS tradicional, otro aspecto notable de los mensajes de smishing de Darcula es su astuto intento de evadir una medida de seguridad en iMessage que impide que los enlaces sean clicables a menos que el mensaje sea de un remitente conocido.

Esto implica instruir a la víctima a responder con un mensaje «Y» o «1» y luego volver a abrir la conversación para seguir el enlace. Un mensaje de este tipo publicado en el subreddit r/phishing muestra que los usuarios son persuadidos para hacer clic en el URL al afirmar que han proporcionado una dirección de entrega incompleta para el paquete de USPS.

Estos iMessages son enviados desde direcciones de correo electrónico como pl4396@gongmiaq.com y mb6367587@gmail.com, lo que indica que los actores de amenazas detrás de la operación están creando cuentas de correo electrónico falsas y registrándolas con Apple para enviar los mensajes.

Google, por su parte, recientemente anunció que está bloqueando la capacidad de enviar mensajes usando RCS en dispositivos Android con root para reducir el spam y el abuso.

El objetivo final de estos ataques es engañar a los destinatarios para que visiten sitios falsos y entreguen su información personal y financiera a los estafadores. Hay evidencia que sugiere que Darcula está dirigida hacia grupos de cibercriminales de habla china.

Los kits de phishing pueden tener consecuencias graves, ya que permiten a criminales menos hábiles automatizar muchos de los pasos necesarios para llevar a cabo un ataque, lo que reduce las barreras de entrada.

Este desarrollo se produce en medio de una nueva ola de ataques de phishing que aprovechan la función de restablecimiento de contraseña de Apple, bombardeando a los usuarios con lo que se llama un ataque de bombardeo de solicitudes (también conocido como

fatiga de MFA) con la esperanza de secuestrar sus cuentas.

Si suponemos que un usuario logra rechazar todas las solicitudes, *«los estafadores llamarán entonces a la víctima, falsificando el soporte de Apple en la identificación del llamante, informando que la cuenta del usuario está siendo atacada y que el soporte de Apple necesita 'verificar' un código de un solo uso»,* según informó el periodista de seguridad Brian Krebs.

Se ha observado que los estafadores de voz utilizan información sobre las víctimas obtenida de sitios web de búsqueda de personas para aumentar la probabilidad de éxito, y en última instancia *«activan el envío de un código de restablecimiento de ID de Apple al dispositivo del usuario»*, el cual, si se proporciona, permite a los atacantes restablecer la contraseña de la cuenta y bloquear al usuario.

Se sospecha que los responsables están explotando una debilidad en la página de restablecimiento de contraseña en iforgot.apple[.]com para enviar múltiples solicitudes de cambio de contraseña de una manera que evita las protecciones de limitación de velocidad.

Estos hallazgos también siguen a la investigación de F.A.C.C.T. que revela que los cambiadores de SIM están trasladando el número de teléfono de un usuario objetivo a su propio dispositivo con una SIM incorporada (eSIM) para obtener acceso no autorizado a los servicios en línea de la víctima. Se dice que esta práctica se ha llevado a cabo en la vida real durante al menos un año.

Esto se logra mediante la iniciación de una aplicación en el sitio web o la aplicación del operador para transferir el número desde una tarjeta SIM física a una eSIM haciéndose pasar por la víctima, lo que hace que el propietario legítimo pierda acceso al número tan pronto como se genere y active el código QR de la eSIM.

> *«Una vez que los ciberdelincuentes obtienen acceso al número de teléfono móvil de la víctima, pueden obtener códigos de acceso y autenticación de dos factores para varios servicios, incluidos bancos y aplicaciones de mensajería, lo que abre un*

> *abanico de oportunidades para que los delincuentes implementen esquemas fraudulentos*», comentó el investigador de seguridad Dmitry Dudkov.