En otra señal más de que Telegram se está convirtiendo cada vez más en un centro próspero para el delito cibernético, los investigadores descubrieron que los hackers están usando la plataforma de mensajería para vender kits de phishing y ayudar a configurar campañas de phishing.

> *«Para promocionar sus bienes, los phishers crean canales de Telegram a través de los cuales educan a su audiencia sobre el phishing y entretienen a los suscriptores con encuestas como '¿Qué tipo de datos personales prefieres?'»,* dijo Olga Svistunova, analista de contenido web de Kaspersky.

Los enlaces a estos canales de Telegram se distribuyen a través de YouTube, GitHub y los kits de phishing que desarrollan los propios ciberdelincuentes. La compañía rusa de seguridad cibernética dijo que detectó más de 2.5 millones de URL maliciosas generadas con kits de phishing en los últimos seis meses.

Uno de los servicios destacados que se ofrecen es proporcionar a los hackers bots de Telegram que automatizan el proceso de generación de páginas de phishing y recopilación de datos de usuarios.

Aunque es responsabilidad el estafador distribuir las páginas de inicio de sesión falsas a los objetivos de interés, las credenciales capturadas en esas páginas se envían de vuelta por medio de otro bot de Telegram.

Otros servicios de bots van un paso más allá al anunciar opciones para generar páginas de phishing que imitan un servicio legítimo, que después se usan para atraer a posibles víctimas con el pretexto de regalar likes en los servicios de redes sociales.

> *«Los canales de Telegram operados por estafadores a veces publican lo que parecen ser ofertas excepcionalmente generosas, por ejemplo, conjuntos comprimidos de kits de phishing listos para usar que se dirigen a una gran cantidad*

> *de marcas globales y locales»,* dijo Svistunova.

En algunos casos, también se observa que los phishers comparten datos personales de los usuarios con otros suscriptores de forma gratuita con la esperanza de atraer a aspirantes a delincuentes, solo para vender kits pagos a quienes desean realizar más ataques de este tipo. Los estafadores ofrecen también enseñar *«cómo hacer phishing para obtener dinero en efectivo».*

El uso de propuestas gratuitas también es una forma de en la que los estafadores engañan a los delincuentes novatos y con problemas de liquidez para que utilicen sus kits de phishing, lo que resulta en un doble robo, donde los datos robados también se envían al creador sin su conocimiento.

Los servicios de pago, por otro lado, incluyen kits avanzados que cuentan con un diseño atractivo y características como detección anti-bot, encriptación de URL y geobloqueo que los hackers podrían usar para cometer esquemas de ingeniería social más avanzados. Dichas páginas cuestan entre 10 y 280 dólares.

Otra categoría de pago implica la venta de datos personales, con credenciales de cuentas bancarias anunciadas a distintas tasas según el saldo. Por ejemplo, una cuenta con un saldo de $49,000 dólares, se colocó en 700 dólares.

Además, los servicios de phishing se comercializan por medio de Telegram por suscripción (es decir, phishing como servicio o PhaaS), donde los desarrolladores alquilan los kits por una tarifa mensual a cambio de proporcionar actualizaciones periódicas.

También se promociona como suscripción un bot de contraseña de un solo uso (OTP) que llama a los usuarios y los convence de ingresar el código de autenticación de dos factores en sus teléfonos para ayudar a eludir las protecciones de la cuenta.

La configuración de estos servicios es relativamente sencilla. Lo que es más difícil es ganarse

la confianza y lealtad de los clientes. Algunos proveedores hacen lo posible para garantizar que toda la información esté encriptada para que ningún tercero, incluidos ellos mismos, pueda leerla.

Los hallazgos también siguen a un aviso de Cofense a inicios de enero, que reveló un aumento del 800% año tras año en el uso de bots de Telegram como destino de exfiltración para información de phishing.

> *«Los aspirantes a phishers solían necesitar encontrar una forma de ingresar a la web oscura, estudiar los foros allí y hacer otras cosas para comenzar. El umbral para unirse a la comunidad de phishers se redujo una vez que los actores maliciosos migraron a Telegram y ahora comparten ideas y conocimientos, por lo general de forma gratuita, allí mismo en el popular servicio de mensajería».*