Aumentan estafas en WhatsApp con venta de dólares como anzuelo

Los ataques y fraudes online que utilizan la suplantación de identidad continúan en aumento. En gran parte, esto se debe a la mayor presencia de usuarios en medios virtuales, donde la identidad de una persona se convierte en un perfil fácil de duplicar.

Sumado a esto se encuentra la falta de conciencia que tiene el usuario promedio sobre la cantidad de información personal que está pública en Internet y los riesgos que esto supone. Desde 2020 a esta parte los ataques que involucraron el robo de identidad aumentaron de manera desmedida y desde entonces la cantidad de denuncias no disminuyó.

ESET, compañía especializada en detección proactiva de amenazas, advierte sobre un nuevo ataque que utiliza la venta de dólares como anzuelo, un engaño vía WhatsApp que comienza con un phishing.

Todo comienza al recibir un mensaje vía WhatsApp desde un número desconocido en el que se hacen pasar por una persona cercana. Si bien el número de teléfono es diferente, el perfil es una copia del legítimo, incluyendo fotografía y nombre de cuenta. Además, pueden llegar a dirigirse por un apodo familiar para dar más veracidad a la comunicación.

Luego de mantener una conversación mínima, llega un mensaje fuera de lo común, tanto por los mensajes que se intercambian, así como por la relación que se puede tener con la persona cuya identidad fue suplantada: Se pregunta por personas interesadas en comprar dólares estadounidenses.

Lo que se debería hacer inmediatamente después de recibir un mensaje sospechoso es comunicarse con el contacto original -ahora víctima- por teléfono. Ese usuario está siendo blanco de un ataque de suplantación de identidad.

Gracias al mensaje de advertencia que envió el usuario a todos sus contactos en su teléfono real, descubrió que la mayoría de sus contactos de WhatsApp habían recibido mensajes similares desde el mismo número.

El delincuente que se hace pasar por este usuario se contacta a

través de un número distinto y utilizando una cuenta de WhatsApp diferente, con lo cual no se trata de un caso de SIM swapping ni de robo de la cuenta de la aplicación.

El equipo de investigación de ESET, realizó el análisis de posibles orígenes del ataque: ¿De dónde habían robado la fotografía y nombre completo? ¿Cómo poseían todos los contactos? ¿Por qué habían elegido una aplicación como WhatsApp? ¿Qué objetivo tenía este ataque en particular?

“En primer lugar, notamos que la cuenta usada para llevar a cabo el engaño posiblemente haya sido robada, ya que se trataba de una cuenta de WhatsApp Business que pertenecía a una compañía del rubro automotor. Además, tras revisar sus redes sociales y perfiles en distintas aplicaciones, nos dimos cuenta de que el usuario usaba la misma fotografía y nombre de perfil en otros servicios públicos. Esto podría significar que su cuenta de WhatsApp no fue comprometida y que los estafadores suplantaron su identidad utilizando otra cuenta robada de la red social de mensajería”, comenta Martina Lopez, Investigadora de Seguridad Informática de ESET Latinoamérica.

Teniendo en cuenta la cantidad de contactos que habían sido contactados, desde ESET comprendieron que probablemente el estafador obtuvo una copia de seguridad de los contactos de alguna manera. Con esto en mente, puso el foco en un perfil que combinara todas las piezas robadas: una copia de su lista de contactos, fotografía y nombre completo.

Sabiendo que el phishing es la modalidad de ataque más utilizada por los cibercriminales para robar cuentas de correo electrónico, el equipo de ESET realizó junto al usuario una búsqueda dentro de los correos para encontrar alguno sospechoso en donde haya ingresado.

El resultado fue que hace algunos meses el usuario había sido víctima de un correo de phishing en el que se suplantaba la identidad de Microsoft y en el cual le solicitaban las credenciales utilizando como excusa una supuesta actividad inusual en la cuenta de la víctima. Un clásico engaño de ingeniería social.

Para evitar este tipo de estafas desde ESET comparten algunas recomendaciones que son tan simples como importantes:

– Tener cuidado con aquellas comunicaciones que soliciten credenciales, ya que no suele ser un método que utilicen las aplicaciones. Además, es importante saber cómo identificar un

engaño de phishing para no caer la trampa, sobre todo teniendo en cuenta que es una modalidad muy común.

Con información de BancayNegocios