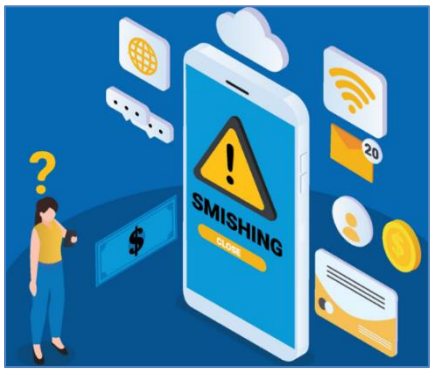
Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°207	Fecha: 03-09-2023
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nueva campaña de smishing dirigida que ataca a ciudadanos estadounidenses para robar datos de pago		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:



El smishing (también conocido como SMS Phishing) es un tipo de ataque cibernético en el que los atacantes utilizan SMS (mensajes de texto) para engañar a las personas para que revelen el siguiente tipo de información o datos personales y financieros: Contraseñas, números de tarjetas de crédito, números de tarjeta de débito, credenciales bancarias, o hacer descargar software malicioso. En ataques como este, los actores de amenazas imitan a agencias gubernamentales, bancarias o postales como USPS para parecer legítimos, engañando a las víctimas para que compartan información de pago a cambio de tarifas falsas.

Recientemente, los investigadores de ciberseguridad de RSecurity descubrieron una nueva y extensa campaña de smishing denominada "Smishing Triad", en la que los actores de amenazas se dirigen activamente a los ciudadanos de los Estados Unidos, haciéndose pasar hábilmente por servicios líderes de correo/entrega como Royal Mail o USPS para atrapar a ciudadanos estadounidenses desprevenidos.

Además de Estados Unidos, los investigadores también revelaron que, en incidentes anteriores, los actores de amenazas atacaron a víctimas de varios otros países: El Reino Unido, Polonia, Suecia, Italia, Indonesia y Japón.

2. DETALLES:

El grupo generalmente explota el servicio iMessage para enviar estafas de seguimiento de paquetes y roba PII (información de identificación personal) y datos financieros (como detalles de tarjetas de pago o credenciales bancarias) para realizar fraudes con tarjetas de crédito y robo de identidad.

Esta vez, Smishing Triad ha cambiado ligeramente su estrategia y explota los mensajes de cuentas comprometidas de Apple iCloud para engañar a los usuarios. Su kit de smishing también está a la venta en grupos de mensajería instantánea de Telegram para crear una red de fraude como servicio extensa y bien organizada.

El equipo de inteligencia sobre amenazas de Resecurity accedió y realizó ingeniería inversa en uno de esos kits y descubrió una vulnerabilidad de inyección SQL a través de la cual pudieron recuperar datos confidenciales de más de 108.000 víctimas y les advirtieron sobre la probabilidad de robo de identidad.

A. Entidades imitadas:

- The Royal Mail (Reino Unido)
- New Zealand Postal Service (Servicio Postal de Nueva Zelanda)
- Correos (España)
- Postnord (Suecia)
- Poste Italiane and the Italian Revenue Service (Agencia Tributaria Italiana)
- J&T Express (Indonesia)
- Poczta Polska (Polonia)

Estos perpetradores también están suministrando a otros ciberdelincuentes 'kits de smishing' hechos a medida, disponibles para su compra a través de un grupo en Telegram, a partir de 200 dólares al mes. Los suscriptores reciben códigos de activación y scripts de implementación para los siguientes marcos:

- ThinkPHP
- Laravel
- VueJS
- React
- Uniapp

B. Indicadores de compromiso (IOC):

- wangduoyu[.]me
- wangduoyu[.]shop
- wangduoyu[.]site
- poczta-polska[.]cc
- ususmx[.]top
- ususmx[.]top
- ususnb[.]top
- ususgs[.]top
- ususcgh[.]top
- uspoddp[.]top
- uspsjh[.]top
- ususnu[.]top
- usushk[.]top
- ususcsa[.]top
- uspoky[.]top
- usplve[.]top
- ususcac[.]top
- uspshhg[.]top
- uspodad[.]top
- uspogumb[.]top
- uspsuiu[.]top
- uspshhg[.]top
- uspsuiu[.]top
- uspskkq[.]top
- ususuua[.]top
- uspodaa[.]top

- uspoadc[.]top
- uspshhg[.]top
- usplve[.]top
- usushk[.]top
- uspshhg[.]top
- ususcgh[.]top
- ususnu[.]top
- ususnb[.]top
- uspoddp[.]top
- usususua[.]top

"Es complicado interrumpir la actividad cibercriminal cometida por actores ubicados en jurisdicciones extranjeras como China sin una armonización regulatoria adecuada y asistencia legal mutua en el extranjero", indicó Resecurity.

3. RECOMENDACIONES:

- Verificar siempre la identidad del remitente antes de responder a cualquier mensaje SMS, especialmente aquellos que solicitan información personal o financiera.
- Evitar hacer clic en enlaces o descargar archivos adjuntos en mensajes de texto, especialmente si no esperaba recibir dicho mensaje.
- Nunca compartir información personal o financiera a través de mensajes de texto, como números de Seguro Social, detalles de tarjetas de crédito o credenciales de inicio de sesión. Las organizaciones legítimas no solicitarán datos tan confidenciales a través de SMS.
- Utilizar fuentes confiables o comunicarse con la organización directamente, utilizando un número de teléfono o un sitio web confiable, para verificar la autenticidad del mensaje.
- Utilizar software antivirus y antimalware licenciados en su dispositivo móvil.
- Mantener actualizados el sistema operativo y las aplicaciones de su teléfono.
- Usar contraseñas seguras y únicas para sus cuentas y habilitar la autenticación de dos factores, siempre que sea posible.

Fuente de Información:	• hxxps://gbhackers.com/smishing-campaign-attacking-us-citizens-steal-payment-data/ • hxxps://www.hackread.com/chinese-smishing-triad-us-users-cybercrime-attack/