Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°281	Fecha: 24-11-2023
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Cibercriminales utilizan Telekopye Telegram Bot para crear estafas de phishing a gran escala		
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:**

   Han surgido más detalles sobre un bot malicioso de Telegram llamado Telekopye que utilizan los actores de amenazas para realizar estafas de phishing a gran escala.

   "Telekopye puede crear sitios web de phishing, correos electrónicos, mensajes SMS y más", dijo el investigador de seguridad de ESET Radek Jizba en un nuevo análisis.

2. **DETALLES:**

   Se sabe que los actores de amenazas detrás de la operación , cuyo nombre en código es Neandertal, dirigen la empresa criminal como una empresa legítima, generando una estructura jerárquica que abarca diferentes miembros que asumen diversos roles.

   Una vez que los aspirantes a neandertales son reclutados a través de anuncios en foros clandestinos, se les invita a unirse a los canales designados de Telegram que se utilizan para comunicarse con otros neandertales y realizar un seguimiento de los registros de transacciones.

   El objetivo final de la operación es realizar uno de los tres tipos de estafas: vendedor, comprador o reembolso.

   En el caso del primero, los neandertales se hacen pasar por vendedores e intentan atraer a mamuts desprevenidos para que compren un artículo inexistente. Las estafas a compradores implican que los neandertales se hagan pasar por compradores para engañar a los mamuts (es decir, comerciantes) para que introduzcan sus datos financieros y se deshagan de sus fondos.

   Otros escenarios entran en una categoría llamada estafas de reembolso, en la que los neandertales engañan a los mamuts por segunda vez con el pretexto de ofrecer un reembolso, sólo para deducir nuevamente la misma cantidad de dinero.

   También se ha observado que los neandertales usan VPN, proxys y TOR para permanecer en el anonimato, mientras exploran estafas inmobiliarias en las que crean sitios web falsos con listados de apartamentos y atraen a los mamuts para que paguen una tarifa de reserva haciendo clic en un enlace que apunta a un sitio web de phishing. .

   "Los neandertales escriben al propietario legítimo de un apartamento, fingiendo estar interesados y pidiéndole diversos detalles, como fotografías adicionales y qué tipo de vecinos tiene el apartamento", dijo Jizba.

   "Los neandertales toman toda esta información y crean su propio anuncio en otro sitio web, ofreciendo el apartamento en alquiler. Reducen el precio de mercado esperado en aproximadamente un 20%. El resto del escenario es idéntico al escenario de estafa del vendedor".

3. **RECOMENDACIONES:**

   - Verificar detalladamente las URLs que correspondan a sitios web oficiales.
   - Evitar abrir archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales.
   - Instalar y mantener actualizados los últimos parches de seguridad de su software.
   - Utilizar una solución antivirus licenciada con protección en tiempo real y que te permita eliminar troyanos.
   - Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2023/11/cybercriminals-using-telekopye-telegram.html