Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°009	Fecha: 10-01-2024
		Página: 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ciberdelincuentes atacarán Telegram en 2024		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Con el avance de ChatGPT y otras aplicaciones de inteligencia artificial, los ciberdelincuentes estarán más 'capacitados' que nunca, y atacarán apps de mensajería como Telegram.

Varios laboratorios de firmas de ciberseguridad, como ESET Latinoamérica, ya analizaron las amenazas que más impacto tendrán en 2024 y destacan que el cibercrimen posará su mirada en los chats de los usuarios, hará campañas de espionaje y mejorará sus troyanos bancarios.

En el vertiginoso paisaje digital de América Latina, será un año desafiante para la seguridad informática. Mientras la tecnología avanza, también lo hacen las amenazas cibernéticas", comenta el jefe del Laboratorio de Investigación de ESET Latinoamérica, Camilo Gutiérrez.

2. DETALLES:

Algunas de las principales tendencias de ciberseguridad a tomar en cuenta, y detalla cómo protegerse.

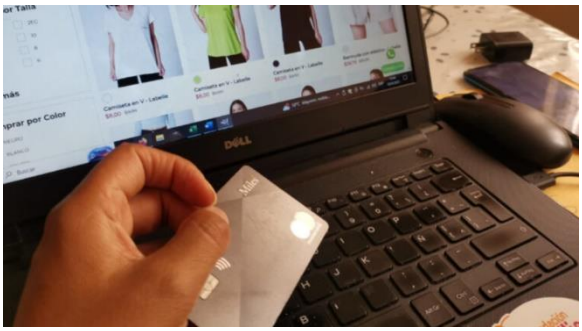
A. Cibercrimen en aplicaciones de mensajería

Firmas como ESET esperan que los ciberdelincuentes apuntarán sus actividades de estafa en aplicaciones como Telegram y plataformas similares. También se espera que una vez 'secuestrados' los datos de los usuarios, estos se vendan libremente en la Dark Web, aquel espacio de la internet oscura que se presta para ilícitos. “El principal reto radicará en encontrar un enfoque que logre armonizar la seguridad digital con la preservación de la libertad individual, dice Gutiérrez Amaya de ESET. ¿Cómo atacarán los hackers en Telegram o WhatsApp? Básicamente, utilizarán mensajes falsos de ingeniería social, sobre millonarios premios o loterías de visas; y también llamadas engañosas de números extranjeros y con contactos que no existen, o creados con inteligencia artificial.

B. La IA en escena

Con el avance de ChatGPT y otras aplicaciones que incorporan tecnologías de inteligencia artificial generativa, se abre una ventana de oportunidades y peligros. Por un lado, las empresas pueden implementar modelos de lenguaje avanzados para detectar amenazas. Pero por el otro, actores malintencionados pueden orquestar ataques basados en la ingeniería social aún más sofisticados. Con las herramientas de inteligencia artificial generativa, algunas hasta gratuitas, se ha demostrado lo sencillo que puede ser generar correos electrónicos, mensajes o llamadas automatizadas que imiten de manera convincente a usuarios legítimos. Así que en 2024 dude de casi todo lo que recibe, como una fotografía inverosímil del papa Francisco pidiendo ayuda en su iglesia, o de una hermosa modelo invitándolo a un evento.

C. Troyanos bancarios



Troyanos bancarios Compras en línea con tarjeta de crédito. Foto referencial del 18 de septiembre de 2023. PRIMICIAS Los cambios identificados durante este año en la forma de propagarse y el diseño de los troyanos bancarios indican que este tipo de amenazas seguirán vigentes y evolucionarán. Desde ESET esperan una mayor sofisticación en técnicas de evasión, como el uso de técnicas de camuflaje y la exploración de vulnerabilidades

específicas de la región. ¿Qué es un troyano bancario? Técnicamente, es un tipo de virus o archivo malicioso que infecta un sistema y su fin es robar datos de la banca en línea, sistemas de pago electrónico y tarjetas de débito o crédito. Por ello, las empresas de ciberseguridad resaltan que la primera línea de defensa es el usuario o cliente, quien debe tener buenas prácticas de ingreso al sistema, es decir, una clave robusta y estar alerta a engaños que lleguen en correos electrónicos.

D. Ojo a los cascos virtuales

El "desenfrenado" uso de códigos QR y los cascos y gafas de realidad virtual y mixta serán otro de los focos de la ciberseguridad. La firma de ciberseguridad Panda señala en su web que en 2024 "veremos cómo un investigador o un pirata informático malintencionado encuentra la manera de recopilar o acceder a los datos de los sensores de los auriculares y recrear el entorno en el que juegan los usuarios". Estos cascos ofrecen una gran cantidad de información nueva y personal que puede ser robada, monetizada y utilizada como arma por los malhechores, por ejemplo, el diseño o ubicación exacta del hogar.

3. RECOMENDACIONES:

- Siempre cerrar las sesiones de las apps de mensajería que se hayan iniciado en el computador.
- Nunca dar clic a ningún enlace de un contacto desconocido, que lo lleve a otra App externa, como una red social.
- No contestar llamadas por WhatsApp de números extranjeros, a menos que espere dicha llamada.
- Desconfiar de todo anuncio exagerado como las promociones imperdibles que puedan llevarlo a descargar malware o virus.
- Nunca ingresar a portales bancarios ni colocar datos confidenciales desde una conexión gratuita de Wifi, por ejemplo, en una cafetería o restaurante.

Fuente de Información:	• hxxps://www.primicias.ec/noticias/entretenimiento/tecnologia/ciberdelincuentes-telegram-apps-virus/