LITORALPRESS

Fecha: 24-07-2024
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: Catálogo con las nuevas estafas y engaños que usan los ciberdelincuentes

Pág. : 11
Cm2: 739,3
VPE: $ 4.065.577

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

Especial Educación financiera

Juan Pablo Arias es gerente de ingeniería de Fortinet Chile.

DAVID VELÁSQUEZ

"Generan textos, imágenes o videos bastante elaborados que pueden engañar incluso a los más desconfiados", explica Juan Pablo Arias, gerente de ingeniería de Fortinet Chile.

Uso de la inteligencia artificial mejora la verosimilitud de los mensajes falsos

Catálogo con las nuevas estafas y engaños que usan los ciberdelincuentes

JOAQUÍN RIVEROS

El glosario de estafas que apuntan a clientes bancarios y público en general mediante el uso de nuevas tecnologías cada día suma nuevas estrategias. Si bien el contexto del engaño sigue siendo parecido como poner, por ejemplo, en apremio a la víctima mediante algún problema que debe ser resuelto con urgencia o atraerlo con algún beneficio o premio, la aplicación de nuevas tecnologías hace mucho más verosímil la historia. "Si bien este tipo de estrategia no es nueva, hoy en día su uso ha evolucionado gracias a la inteligencia artificial generativa. De esta forma, se generan textos, imágenes o videos bastante elaborados que pueden engañar incluso a los más desconfiados", explica Juan Pablo Arias, gerente de ingeniería de Fortinet Chile, multinacional experta en ciberseguridad.

CEDIDA

Paola Sánchez, de Inform.

El comisario Juan Valdenegro, de la Brigada del Cibercrimen, ratifica el punto: "Hemos detectado un uso creciente de Inteligencia Artificial en este tipo de estafas. Los ciberdelincuentes modifican videos de personajes públicos, de modo que estos aparecen llamando a hacer determinadas inversiones, en moneda nacional o criptomonedas. Estas estafas se ligan al historial de búsqueda de los usuarios, en base a sus archivos temporales. De ese modo saben que tiene un perfil que calza con el engaño", indica.

Los nuevos ataques envían mensajes por diferentes tecnologías y plataformas. "Un formato es el envío de campañas, que pueden ir desde promociones hasta la entrega de ayudas gubernamentales. Para ello, mandan links falsos de los bancos (phishing) por correo electrónico, mensajes por WhatsApp y hasta llamadas pregrabadas con el formato de call centers, de modo que se refuerza la verosimilitud de la estafa", explica Pedro Huichalaf, docente del Centro de Ciberseguridad de la Universidad Mayor.

El contenido de las historias que usan los ciberdelincuentes lo obtienen de las redes sociales. "Se aprovechan de la información disponible en ellas sobre los amigos, familia y hábitos de una persona para elaborar engaños tremendamente sofisticados", explica Arias.

Password spraying: "Consiste en capturar la password de un usuario y probarla en múltiples sitios. Las personas usualmente reutilizan sus contraseñas en distintos servicios ya que es difícil memorizar muchas contraseñas largas. Este tipo de estrategia se ha potenciado por el uso de la IA", cuenta Arias.

Side-channel attack: Se captura el sonido de las teclas usando el mismo micrófono del dispositivo para adivinar la password mediante el análisis de la señal auditiva mediante el uso de IA.

Llamada del banco por clave: Un estafador bloquea la clave bancaria de una persona mediante intentos fallidos de ingreso. Luego, llama a la víctima haciéndose pasar por un ejecutivo de fraude del banco, informando sobre un supuesto bloqueo de cuenta por una compra grande. El estafador pide a la víctima verificar el bloqueo en la página del banco y, una vez confirmado, solicita realizar una recuperación de clave usando la autenticación de doble factor en el celular. De esta forma, el estafador roba la nueva clave bancaria de la víctima.

Plataformas de Inversión en criptomonedas: Es un ámbito usado para nuevas estafas. La atracción de inversiones con muy buenos rendimientos es un gancho para articular engaños. "Las plataformas para hacer transacciones de criptomonedas atraen a la gente por lo novedoso y pueden ser engañadas por falta de conocimiento en el tema.

Redes WiFi: Ocurre en lugares con red WiFi públicas. "Los ciberatacantes pueden levantar redes inalámbricas abiertas para engañar a las personas y robar información", cuenta Arias.

Carga de celulares en sitios públicos: En los terminales aéreos, buses o en cafés, los delincuentes intervenen los terminales USB de carga de celulares o notebooks, remplazándolos por dispositivos que inyectan malwares a dichos dispositivos los que permiten capturar claves.

Phishing: Es el envío de mails o mensajes por otros soportes en que se hacen promociones comerciales, campañas o requerimientos personales, supuestamente de bancos u otras instituciones. Estos mensajes contienen links que llevan a sitios web fraudulentos diseñados para robar contraseñas y números de tarjetas de crédito.

Malware: "Es una técnica que infecta a los dispositivos móviles y ordenadores, capturando datos sensibles cuando los usuarios acceden", explica Paola Sánchez, Business Developer de RiskShield en Inform para Latinoamérica. El ataque incluso puede tomar el control del dispositivo. Opera al infectar computadoras a través de descargas engañosas, correos electrónicos o vulnerabilidades de seguridad.

Atacas de Ingeniería social: "Ocurre cuando los estafadores manipulan psicológicamente a los usuarios para obtener información confidencial, haciéndose pasar por representantes de soporte técnico o amigos que necesitan ayuda financiera", explica Sánchez.