LITORALPRESS

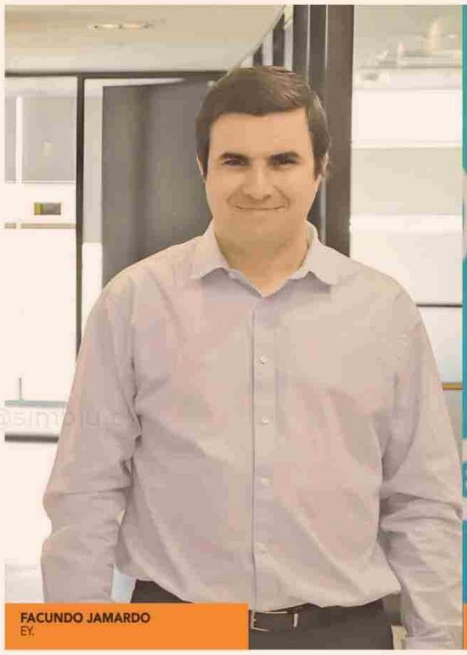
Fecha: 16-12-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Ciberataques potenciados por IA generativa redefinirán la ciberseguridad**

Pág. : 38
Cm2: 243,1
VPE: $ 2.153.856

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Ciberataques potenciados por IA generativa redefinirán la ciberseguridad

- Surgirán nuevas amenazas como suplantación de identidad con deepfake en tiempo real y envenenamiento de códigos en sistemas de inteligencia artificial, y los blancos se amplían.



FACUNDO JAMARDO
EY.

MARTINA LÓPEZ
ESET LATINOAMÉRICA

POR MARCO ZECCHETTO

El avance acelerado de las nuevas tecnologías, como la inteligencia artificial (IA) generativa están redefiniendo tanto el escenario actual como el futuro de la ciberseguridad. Desde ataques de *deepfake* -videos, imágenes o audios generados que imitan la apariencia y el sonido de una persona- en tiempo real, hasta correos maliciosos con capacidad de retroalimentación, son algunas de las modalidades de ciberataques esperadas para 2025.

La investigadora de seguridad informática de ESET Latinoamérica, Martina López, proyectó que el *phishing* -técnicas de engaño con suplantación de identidad- mantendrá una tendencia cercana a los 2 millones de detecciones mensuales para el próximo ejercicio, la que podría verse potenciada por la IA generativa, con campañas a través de correos maliciosos.

"Seguimos teniendo al *phishing* como la amenaza más detectada en toda Latinoamérica, y lo seguirá siendo probablemente. Y en este sentido, la IA generativa será bastante auxiliar en esto", afirmó.

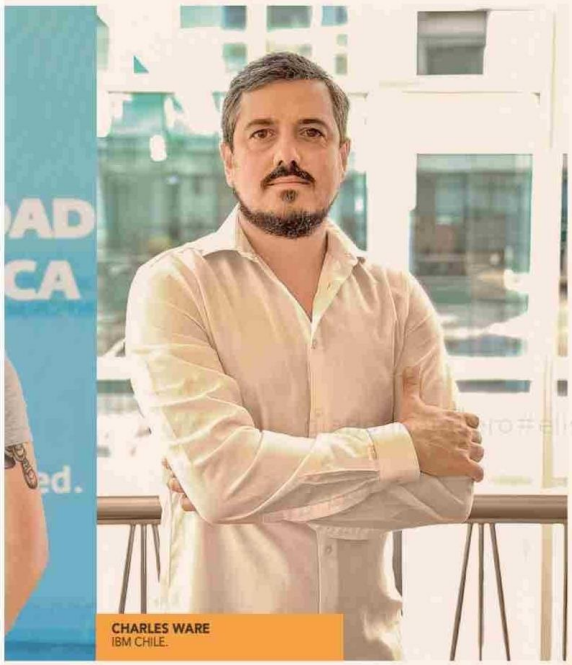
Comentó también que este año detectaron casi 430 mil archivos únicos asociados a códigos maliciosos como troyanos, *exploits* (aprovechan una vulnerabilidad informática) y códigos espía, y se espera que las detecciones únicas mensuales aumenten en 10% y

LITORALPRESS

Fecha: 16-12-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Ciberataques potenciados por IA generativa redefinirán la ciberseguridad**

Pág. : 39
Cm2: 241,7
VPE: $ 2.141.275

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida



CHARLES WARE
IBM CHILE.

que se vean potenciados por IA generativa.

López indicó que la tendencia en el manera de operar de los ciberatacantes se centrará principalmente en campañas dirigidas a organizaciones específicas, más que ataques en forma masiva; las que se potenciarán con el uso de inteligencia artificial.

Nuevas ciberamenazas

Según López, algunas de las tendencias para el próximo año serán los correos maliciosos con capacidad de aprender del comportamiento de sus víctimas.

"Es como si fuese una especie de modelo aprendido, como ChatGPT. Podríamos llegar a ver campañas vía email que aprenden y se vayan perfeccionando de acuerdo al comportamiento de las víctimas, si *clickean* o no en los enlaces, por ejemplo", advirtió.

También se espera un aumento en la proliferación de *deepfakes* sofisticados en video, y que la dificultad para detectarlos "va a ser mucho más grande".

En tanto, el socio líder de ciberseguridad de EY, Facundo Jamardo, dijo que la inteligencia artificial y la IA generativa continuarán "multiplicando las superficies a proteger" en las empresas, desde los segmentos operativos, la cadena de suministro, hasta las áreas de TI.

Entre los nuevos ataques, destacó que el *zoombombing* -intrusión no autorizada de personas en una reunión virtual- se verá potenciado por *deepfakes* en tiempo real, suplantando la identidad, voz y gestos de trabajadores o ejecutivos de organizaciones, durante videoconferencias.

El *security client executive* de IBM Chile, Charles Ware, advirtió que otra tendencia en 2025 será el "shadow AI" (IA en las sombras), es decir, el uso de modelos de IA que los trabajadores o áreas de una compañía encuentran en internet, pero que no están bajo la gobernanza de la organización, lo que podría exponer datos de la empresa en la web.

"Los ciberdelincuentes se están dando cuenta de que es más fácil buscar estos modelos y tomar los datos que las propias empresas están sacando para afuera, que tratar de entrar en la compañía y tomar los datos de adentro", afirmó.

Agregó que también se observará un aumento en los envenenamientos de código a grandes modelos de lenguaje (códigos dañinos para manipular sus datos de entrenamiento y alterar el comportamiento del modelo) y en la generación de códigos maliciosos que permitirían, por ejemplo, crear agentes de IA capaces de automatizar ataques.

Se amplían los blancos

Jamardo de EY señaló que la industria financiera seguirá siendo "el atractivo principal" de los ciberatacantes, pero también comenzarán a verse ataques con mayor frecuencia en los sectores productivos.

"Particularmente en Chile, se verán en la industria minera, la manufactura avanzada y también en la industria de energía", afirmó.

Ante los perfiles de empresas objetivo en la región, López de ESET Latinoamérica, agregó que los atacantes se enfocarán en "buscar un balance" entre la cantidad de información sensible que puede llegar a poseer una compañía, la cantidad de dinero que dispone "para un posible chantaje, y la valoración y confianza de esta ante el público en general".

Se viene la encriptación postcuántica

Facundo Jamardo de EY comentó que el avance de la computación cuántica, capaz de vulnerar los sistemas de encriptación tradicionales, ya tiene a las empresas de software trabajando para desarrollar sistemas de criptografía postcuántica -basada en algoritmos matemáticos complejos y otras tecnologías- los que estima podrían salir al mercado el año que viene.
No obstante, si bien hay avances en esta tecnología, todavía no existen computadores cuánticos de uso masivo, por lo tanto, aún es difícil que el próximo año se vean ataques realizados desde ordenadores cuánticos, pero sí se verán algunas empresas interesadas en adoptar los nuevos métodos de encriptación postcuánticos.