EL MERCURIO
innovación

Fecha: 24/10/2024 Audiencia: 320.543 Sección: ACTUALIDAD
Vpe: $11.065.628 Tirada: 126.654 Frecuencia: SEMANAL
Vpe pág: $18.442.944 Difusión: 126.654
Vpe portada: $18.442.944 Ocupación: 60%

AFP

Esta herramienta puede ser usada para generar engaños o para extorsionar a personas. En la foto, cuentas falsas de redes sociales creadas con inteligencia artificial.

ESPECIALISTAS SE REUNIERON EN UN SEMINARIO INTERNACIONAL:

La IA puede ayudar a cibercriminales, pero también da herramientas para combatir el delito

OBJETIVOS DE DESARROLLO SOSTENIBLE

Los 17 Objetivos de Desarrollo Sostenible (ODS) son un llamado de Naciones Unidas a los gobiernos, las empresas y la sociedad civil para erradicar la pobreza, proteger el planeta y asegurar la prosperidad para todos al año 2030.

Permite que los ataques sean más sofisticados o darle acceso a crear códigos maliciosos a inexpertos. Pero, por otro lado, ayuda a analizar gran cantidad de datos para combatir el crimen organizado o prevenir ataques digitales en empresas. **ALEXIS IBARRA O.**

Un grupo de *hackers* especializados que generan ataques a escala mundial hasta inexpertos ciberdelincuentes se benefician del uso de la IA en sus operaciones delictivas. Unos para mejorar sus sofisticados ataques; los otros para crear códigos maliciosos sin tener siquiera conocimientos de programación.

Dmitry Bestuzhev, consultor independiente en temas de seguridad informática —que fue invitado al Séptimo Seminario Internacional de Ciberseguridad: La era de la inteligencia artificial, organizado por la PDI y la U. Técnica Federico Santa María, y que se realizó hace unos días—, señaló que la Oficina 121 es un grupo de *hackers* de elite de Norcorea y que han sido reclutados meticulosamente. "Este no es un simple grupo cibercrimimal, sino una operación liderada por el líder supremo", dijo.

Según Bestuzhev, estos *hackers* han desarrollado casi todas las formas de ataque: desde la creación de *malware* (código malicioso), robo de criptomonedas; fueron los responsables de WannaCry y otros ataques de *ransomware*. Además, explica, son responsables de ataques a entidades bancarias en América Latina, incluido Chile. Con IA, dice, logran infiltrarse en la sociedad. "Con el uso de la inteligencia artificial generativa, ya no solo usan mensajes de texto para engañar, sino que pueden enviar mensajes de audio, en cualquier idioma, simulando el acento local", aclara.

Así como estos sofisticados *hackers* usan la IA para el engaño, otros menos avezados pueden usarla en sus primeros pasos en el ciberdelito.

"La IA automatiza el desarrollo de código. Podría tomar de unos 15 a 20 minutos desarrollar una herramienta para penetrar una red pública no muy complicada", dijo en el seminario Cyril Delaere, director de la Unidad de Ciberseguridad en Entel.

Agregó que el cibercrimen ya es una industria en la que ciberdelincuentes acceden a servicios que ofrecen otros ciberdelincuentes, como la creación de código malicioso. "En 2030 el cibercrimen producirá tantos recursos que sería la tercera economía mundial, tras EE.UU. y China".

INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURA

Garantizar la seguridad de las tecnologías digitales y la protección de datos es crucial para el desarrollo sostenible, plantea este objetivo.

ALEXIS IBARRA

Un seminario, organizado por la PDI y la USM este mes, se centró en ciberseguridad en la era de la inteligencia artificial.

David Nieto, *country manager* de Telefónica Tech, dice que al año, a nivel mundial, se detectan 20 mil millones de amenazas y hay 200 mil vulnerabilidades conocidas.

"¿Por qué es importante la IA?", se preguntaba. "Porque las empresas y las personas tenemos que ser efectivas el 100% de las veces que nos ataquen; los atacantes solo necesitan ser efectivos una sola vez. Simple". De ahí, que se necesite la colaboración de herramientas automatizadas.

La IA también se usa para la extorsión por medios digitales. "Ahora se hacen llamadas telefónicas, suplantan voces, simulan promociones bancarias, hacen llamadas fraudulentas y hasta alteran imágenes utilizando inteligencia artificial. Este es el nuevo reto que enfrentamos", dice Óscar Rojas, director para Sudamérica de Celebrite, empresa israelí de *softwares* para hacer análisis forense en dispositivos.

EVIDENCIA **VIRTUAL**

Pero así como la IA puede ayudar a cometer delitos, también es usada por las policías para combatirlo. Y no solo crímenes digitales, sino de toda índole.

En Fortinet, empresa de seguridad informática, dicen que ayudará a los profesionales de seguridad informática a ser más eficientes. "Un asistente virtual nos puede mostrar las estaciones de trabajo que tengan un comportamiento sospechoso en las últimas horas y nos entrega una lista con dispositivos que pueden estar comprometidos en su seguridad dado su comportamiento", dice Leandro Reyes, vicepresidente de Ingeniería en Fortinet.

"El uso de la IA por parte de los investigadores es esencial, ya que la mayoría de los delitos incluyen al menos un dispositivo digital", dice Rojas.

El especialista cuenta que a un perito podría tomarle catorce días hacer el análisis del contenido de un teléfono: fotos, videos, audios, ubicaciones, búsquedas en páginas *web*, uso de diferentes medios de mensajería (WhatsApp, Signal, Telegram), etc.

En un solo teléfono puede haber 60 mil mensajes, 30 mil imágenes y mil videos. "Al desarticular una organización criminal capturamos como evidencia digital 15 teléfonos y dos computadoras con información en la nube. Aquí es donde entran los beneficios de la inteligencia artificial: velocidad, fiabilidad, eficiencia, una lista unificada, optimización de recursos y, sobre todo, un ahorro de tiempo para el investigador", dice Rojas.

Se le puede usar para bandas delictuales asociadas al ciberdelito, al tráfico de drogas o para redes de pornografía infantil. "Por ejemplo, se puede pedir que identifique y filtre las imágenes que contengan desnudos para detectar a las víctimas. En un caso logramos recabar como evidencia 20 videos de pornografía y 17 mil fotos de imágenes eróticas infantiles", aclara.