elDial.com
Contenidos Jurídicos

La inteligencia artificial, una aliada en la investigación informática forense

Por Pablo Rodríguez Romeo[(*)]

La inteligencia artificial (IA) está revolucionando todos los ámbitos, potenciando la forma en que trabajamos y generando nuevas oportunidades. Si bien, al mismo tiempo plantea desafíos éticos y sociales en cuanto al uso, manipulación y privacidad de los datos, que es imprescindible tener en cuenta por las consecuencias que su utilización puede generar.

En este artículo me propongo exponer las ventajas o beneficios que presenta para la investigación informática forense en cuanto a la recopilación y análisis de la evidencia digital en investigaciones legales y judiciales. Además, cómo es utilizada por los ciberdelincuentes para desarrollar ataques cada vez más sofisticados y difíciles de detectar o prevenir.

Es una realidad que hoy en día la IA no solo se utiliza para prevenir y detectar ciberdelitos, sino también para cometerlos. Los ciberdelincuentes están utilizando cada vez más la IA para desarrollar nuevas técnicas y herramientas que les permiten evadir las defensas de seguridad y llevar a cabo ataques cibernéticos más sofisticados.

Cómo protegerse de los ciberdelincuentes que utilizan inteligencia artificial para cometer ataques

A continuación, me propongo echar luz acerca de los ataques más frecuentes que encontramos en la actualidad, y las formas en que los delincuentes utilizan la IA para ejecutarlos. Pero también, cómo protegerse para prevenirlos.

Creación de malware: La IA puede ser utilizada para crear malware más sofisticado y difícil de detectar. Los ciberdelincuentes pueden usar algoritmos de aprendizaje automático para desarrollarlo y así que evada las defensas de seguridad y se propague rápidamente a través de redes y sistemas. También, para que se adapte y evolucione a medida que las defensas de seguridad cambien.

(*) Ing. Pablo Rodríguez Romeo (MP 2411 - MN 5117) – Perito Informático Forense, especialista en Seguridad - Socio del Estudio CySI de Informática Forense – www.cysi.com.ar

Ataques de phishing: Los ataques de phishing son uno de los métodos más comunes utilizados por los ciberdelincuentes para obtener información confidencial de las víctimas. La IA se puede utilizar para generar correos electrónicos de phishing más elaborados y personalizados que engañen a las víctimas y así revelen información confidencial, además de analizar y seleccionar las víctimas más vulnerables para los ataques.

Ataques de fuerza bruta: Los ataques de fuerza bruta son aquellos en los que los ciberdelincuentes intentan adivinar contraseñas y nombres de usuario mediante la utilización de algoritmos de IA que prueban todas las posibles combinaciones de datos hasta que se encuentra la correcta. La IA también puede ser utilizada para generar contraseñas más complejas y difíciles de adivinar.

Ataques de denegación de servicio (DDoS): Los ataques de denegación de servicio (DDoS) son aquellos en los que los ciberdelincuentes sobrecargan los servidores con tráfico falso para interrumpir el servicio. En este caso, la IA puede ser usada para llevar a cabo ataques más sofisticados que evadan las defensas de seguridad y causen más daño.

Fraude financiero: La IA puede ser utilizada para llevar a cabo fraudes financieros de mayor complejidad, como el robo de información de tarjetas de crédito o el fraude de cuentas bancarias. Además, para analizar y seleccionar a las víctimas más vulnerables y generar transacciones fraudulentas que parezcan legítimas.

Toda esta información, permite estar al tanto de las amenazas que existen y tomar medidas de seguridad adecuadas para protegerse. Por supuesto, la concientización del usuario es el primer paso, y fundamental, en esta tarea. Concientizar para que todos los usuarios sean responsables de las interacciones que tienen en internet y no brindar información personal o financiera confidencial a fuentes desconocidas.

Tan importante como esto es adoptar las medidas de seguridad habituales, como mantener los sistemas operativos y aplicaciones actualizadas, utilizar contraseñas seguras y complejas, evitar hacer clic en enlaces o archivos adjuntos sospechosos, y utilizar herramientas de seguridad confiables.

Insisto nuevamente, cualquiera sea el contexto es crucial educar a los usuarios sobre los riesgos asociados con el uso de la tecnología y cómo pueden protegerse a sí mismos y a sus dispositivos de posibles ataques cibernéticos.

Ventajas del uso de herramientas de IA para la investigación informática forense

A través de la utilización de herramientas de procesamiento de datos, machine learning y análisis de volúmenes masivos de evidencia digital, la IA puede ayudar a identificar, documentar e interpretar información relevante para una investigación. En las siguientes líneas detallaré las ventajas más sobresalientes

que presenta no solo en el análisis de la evidencia digital sino también en su recopilación.

Una de las principales ventajas de utilizar IA en la recolección de la evidencia digital es su capacidad para **procesar grandes cantidades de datos en poco tiempo**. Esto permite a los especialistas de la informática forense analizar rápidamente grandes volúmenes de información y encontrar patrones y conexiones que podrían ser difíciles de detectar manualmente. Por ejemplo, si se está investigando un caso de fraude financiero, la IA podría analizar rápidamente millones de transacciones para identificar patrones sospechosos o actividades inusuales.

Además, la IA también puede ayudar a mejorar la **precisión y confiabilidad de la evidencia digital recolectada**. Al utilizar algoritmos avanzados y técnicas de aprendizaje automático, se puede identificar y filtrar información irrelevante o engañosa, lo que ayuda a garantizar que solo se utilice evidencia precisa y confiable en una investigación. Esto es especialmente importante en casos donde la evidencia digital es crucial para resolver el caso, como en investigaciones de delitos informáticos.

Otra ventaja de utilizar IA en la recolección de evidencia digital es su capacidad para **aprender y mejorar con el tiempo**. A medida que se procesan más datos, los algoritmos de aprendizaje automático pueden mejorar su precisión y eficiencia, lo que permite a los investigadores obtener resultados más precisos y confiables con el tiempo.

De todos modos, y más allá de los beneficios que aporta a la investigación informática forense, es importante tener en cuenta que para el tratamiento de la evidencia digital se deben seguir los principales marcos de mejores prácticas existentes llevadas a cabo por profesionales forenses especializados en esta tarea, quienes se encuentran especialmente capacitados en el tema y conocen con exhaustividad las características que presenta la prueba digital.

No olvidemos que presenta especificidades propias que la hacen diferente a otros tipos de pruebas. Es muy frágil (puede ser fácilmente eliminada y modificada sin dejar rastros), reproducible (pueden hacerse copias de esa información y ser siempre original), y anónima (no se puede vincular a una persona, excepto que tenga firma digital incorporada al documento). Por lo cual seguir los lineamientos establecidos para una adecuada recopilación es imprescindible para poder asegurar inequívocamente que la información recabada como prueba es la misma en el tiempo y garantizar su cadena de custodia (esto es, quién la extrajo, por qué, a quién se la entregó, etc.).

¿Cómo se recopila la prueba digital?

Dadas sus características particulares, para que la prueba digital tenga validez en un proceso judicial o extrajudicial es fundamental no viciarla de nulidad. Una de las labores más trascendentes que tiene el perito informático forense justamente reside aquí. Y para que esto se realice con éxito es necesario llevar

a cabo un “paso a paso” riguroso y exhaustivo que permita brindar información valiosa que ayude a resolver el caso en cuestión.

Recopilar la evidencia digital en la escena requiere un conjunto específico de habilidades y técnicas para garantizar que su recopilación, preservación y conservación mantengan la integridad para un correcto análisis posterior. Este proceso requiere de habilidades diversas, unas en el momento de recolección de los dispositivos (en la escena) y otras en el momento del peritaje específicamente, donde interviene el profesional informático forense. Para lo cual se deberá cumplir con una correcta identificación y preservación de la evidencia. A continuación, detallo los pasos involucrados en la recopilación de evidencia digital:

Paso 1: Asegurar la escena. El primer paso para recolectar la evidencia digital es asegurar la escena. Esto significa que nadie puede entrar o salir del área hasta que se haya recopilado la evidencia digital. Además, se deben tomar medidas para asegurar que los dispositivos digitales no sufran ninguna adulteración, fundamental para garantizar la correcta preservación e iniciar la cadena de custodia (trazabilidad de la evidencia).

Paso 2: Identificar los dispositivos. Una vez que la escena está segura, el siguiente paso es identificar todos los dispositivos digitales que pueden contener evidencia relevante. Esto incluye teléfonos inteligentes, computadoras portátiles, tablets, cámaras y otros dispositivos digitales que pueden contener datos relacionados con el delito o el hecho que se desee analizar.

Paso 3: Documentar los dispositivos. Una vez identificados todos los dispositivos digitales, el siguiente paso es documentarlos. Esto incluye tomar notas detalladas sobre la marca y modelo de cada uno, su condición física y cualquier otra información relevante que pueda ser útil en la investigación.

Paso 4: Recopilar los dispositivos. Una vez que se han documentado los dispositivos, el siguiente paso es recolectarlos. Esto implica preservarlos; franjarlos; si no son equipos y son archivos los que se secuestran, hay que calcular el hash de cada uno de ellos; luego retirar con cuidado cada dispositivo de la escena y colocarlo en un contenedor seguro para su transporte; asegurar el inicio de la cadena de custodia y el correcto resguardo o franjado de los elementos.

Paso 5: Obtención de la evidencia. Una vez que se han recolectado los dispositivos, el siguiente paso es la obtención de la evidencia. Esto implica hacer una copia (forense) de los datos almacenados en los dispositivos y almacenarlos en un lugar seguro. Esto asegurará que los datos originales no se alteren o dañen de ninguna manera. Debido a la fragilidad de la prueba digital, lo que la hace fácilmente adulterable y eliminable, este paso es fundamental.

Paso 6: Analizar la evidencia. Una vez preservada la evidencia, el siguiente paso es analizarla. Esto implica revisar los datos almacenados en los dispositivos y buscar cualquier información relevante que pueda ayudar a resolver el caso.

En este camino, los profesionales informáticos forenses se valen de técnicas y softwares que permiten analizar gran cantidad de información en tiempo récord.

La tecnología cambia continuamente. Esto requiere de profesionales forenses altamente capacitados y actualizados para poder dar respuesta a los requerimientos que se presentan a diario. Una tarea compleja, pero mandatoria que no se aprende de libros únicamente, sino que también se investiga en el campo.

Conclusión

No caben dudas de que la inteligencia artificial está transformando todos los aspectos de nuestras vidas. Y el ámbito de la investigación informática forense no ha sido la excepción. Ha demostrado ventajas en la recopilación y análisis preciso y eficiente de la evidencia digital; aunque también ha colaborado para que los ciberdelincuentes aumenten la sofisticación de sus ataques, convirtiéndolos en cada vez más complejos y difíciles de detectar.

Por eso, se vuelve imprescindible la concientización y la educación acerca del uso que se hace de internet y los dispositivos. Los usuarios deben comprender los riesgos asociados con la tecnología y ser responsables en sus interacciones. De esta manera, disminuiremos la posibilidad de ser engañados y, por consiguiente, la posibilidad de que se ejecute un ciberdelito.

La inteligencia artificial ha brindado un nuevo enfoque en la investigación informática forense, permitiendo una mayor eficiencia y precisión en el análisis de la evidencia digital. Sin embargo, la colaboración entre la tecnología avanzada y la experiencia humana sigue siendo esencial para garantizar la justicia y la seguridad en un mundo cada vez más digitalizado y conectado.

Citar: elDial - DC32A5