Cómo la inteligencia artificial está cambiando la cara de la seguridad cibernética

By Staff -

15/12/2016

0

¡Vamos a inyectar un virus en la nave extraterrestre atacante y vamos salvar a la Tierra! ¡Vamos a hackear el mainframe enemigo con seis pulsaciones de teclas y abortar el lanzamiento del torpedo! La ciberseguridad ha sido durante mucho tiempo un elemento básico de la ciencia ficción, ya sea en películas como “Independence Day” o programas de televisión como “Star Trek”. Sin embargo, en nuestro verdadero mundo del siglo XXI, la inteligencia artificial es la nueva cara de la ciberseguridad, incluso si no suena como Hal en “2001: Una odisea del espacio”.

El lugar más obvio para la inteligencia adicional es detectar si algún patrón de tráfico de red es benigno u hostil. Considere la posibilidad de enviar archivos por correo electrónico adjunto. ¿Contienen virus, troyanos u otros programas maliciosos? La tecnología pasada de moda examinaría los archivos buscando firmas, es decir, bits de código que se encontraron en ataques anteriores o documentados de otros archivos infectados con malware.

Las bases de datos de firmas, distribuidas por investigadores y empresas de antivirus / malware, son un método imperfecto por varias razones. A medida que aumenta el número de variantes de malware, aumenta el número de firmas, lo que requiere más tiempo para procesarlas. Además, las firmas son de uso limitado contra ataques de día cero que nadie ha visto antes.

Lo que se necesita son sistemas de autoaprendizaje que pueden detectar malware basándose en el hecho de que es malicioso, ya sea que tenga o no una firma, o si se ha encontrado anteriormente. Los sistemas de autoaprendizaje, también conocidos como aprendizaje automático, utilizan técnicas de IA para fomentar el reconocimiento de patrones, que es rápido y eficiente.

Otra área donde la IA está afectando a la seguridad cibernética es en la detección de cuando los hackers están tratando de violar contraseñas y permisos. Llamados "ataques de autenticación", los ciberdelincuentes exploran redes buscando vulnerabilidades, como dispositivos o servidores sin contraseña definida o una contraseña predeterminada conocida. Los sistemas basados en IA pueden supervisar el tráfico de la red y detectar cuándo una aplicación malintencionada está explorando la red en busca de tales vulnerabilidades, y elevar una alerta o iniciar contramedidas automáticamente. ¿Cómo lo sabe la IA? Debido a que ese tipo de tráfico de red no encaja en el patrón de uso normal del usuario final o de máquina a máquina, y el reconocimiento rápido de patrones es lo que muchos tipos de software de IA saben hacer mejor.

En estos y otros casos, la IA realiza su trabajo aplicando matemáticas al problema. De hecho, uno podría caracterizar todos los tipos de inteligencia artificial (y hay muchos) como matemáticas avanzadas. No se trata de comparar archivos o examinar firmas; El reto es resolver el problema matemático. AI ofrece poderosas técnicas y algoritmos para hacer exactamente eso.

Todos hemos visto que el software en Internet es muy, muy inteligente reconociendo imágenes. Facebook a menudo puede identificar automáticamente a nuestros amigos en las fotografías, y se ofrece a etiquetar para nosotros. Los algoritmos de Google pueden identificar videos de gato con una exactitud casi perfecta. Estos algoritmos de reconocimiento de imágenes no suelen llamarse IA, pero utilizan las mismas técnicas de aprendizaje de máquinas y redes neuronales, para llevar a cabo la misma tarea que un escáner de malware basado en IA, puede utilizar para detectar un archivo defectuoso o un ataque de autenticación.

La pregunta para malware basado en IA y escáneres de red es bastante fácil: ¿Es la cosa (sea lo que sea esta) segura o no segura? Esos escáneres están entrenados "mostrando", redes neuronales u otros sistemas de auto-aprendizaje, muchos ejemplos de cosas seguras e inseguras. Una vez que los algoritmos son entrenados, está listo para trabajar en el mundo real, y puede hacer una evaluación muy rápida y eficiente: El archivo está clasificado como 99% probablemente seguro y sólo 1% probablemente inseguro, así que permite que llegue al

usuario final. La solicitud de acceso a la aplicación está clasificada como 20% probablemente segura y 80% probablemente insegura, así que la bloquea.

Seguro. Inseguro. Esa es una llamada fácil de hacer, pero a veces los administradores o los usuarios finales quieren un poco más de información. ¿Por qué la IA clasifica una una hoja de cálculo de Excel como probablemente insegura? ¿Por qué bloquea el acceso a la aplicación? ¿Por qué el JavaScript de esa página web parecía, casi con toda seguridad, malicioso? Es difícil obtener respuestas de los sistemas de aprendizaje automático.

Piense en ello como un sistema de reconocimiento de imágenes diciendo que "esa imagen no es de un gato". ¿Por qué no se etiqueta como gato? Bueno, no parecía. Eso es lo mejor que puedes aprender. Tal vez eso es suficiente para una foto de gato, pero en una red de ordenadores de negocios, necesitamos saber más: ¿Por qué ese archivo está etiquetado como malware? En esos casos, el sistema de IA marcará el archivo y, a continuación, sistemas adicionales ejecutarán forenses para no sólo verificar la decisión inicial, sino también analizar el malware para obtener información adicional que puede ser útil para detectar y frustrar futuros ataques.

Casi todas las compañías de ciberseguridad están investigando la inteligencia artificial en cierta medida, no pueden permitirse no hacerlo. Tres compañías llevan una ventaja significativa con inteligencia artificial, y están apostando por ser los líderes en el aprovechamiento de IA para detectar y prevenir ataques: Cylance, Javelin Networks y Wedge Networks.

Cylance, con sede en Irvine, California, ha construido lo que se caracteriza como antivirus de próxima generación basado en IA. La especialidad de la compañía es la protección en el punto de final: Cylance detecta (y bloquea) malware, virus y bots conocidos y desconocidos, y hace que los futuros métodos de ataque sean inútiles.

Según Cylance, el núcleo de su capacidad de identificación de malware es una revolucionaria plataforma de máquina de aprendizaje de investigación que utiliza la ciencia algorítmica y la inteligencia artificial. Analiza y clasifica cientos de miles de características por archivo, dividiéndolos hasta un nivel atómico para discernir si un objeto es "bueno" o "malo" en tiempo real. Esas características no son las mismas que las firmas: son puntos de datos que deben ser examinados para cada archivo.

Piense otra vez sobre la identificación del gato: los gatos tienen ojos, oídos, narices y una forma de cabeza y una textura de la piel. Pero también lo hacen los perros, los ratones y los caballos. Se necesitan decenas de miles de puntos de datos para distinguir algo que es casi seguro que sea un gato, de algo que es casi seguro que no sea un gato. Lo mismo ocurre con distinguir un PDF seguro de un archivo PDF malicioso: no hay ningún indicador. La IA tiene que examinar un montón de datos con el fin de emitir un juicio seguro.

Stuart McClure, CEO, Presidente y Fundador de Cylance afirma: "Hemos agrietado el código. Hemos descubierto una manera de tomar un conjunto muy robusto de algoritmos y aplicarlos por primera vez a la seguridad cibernética. Estos algoritmos ya han sido probados durante más de 30 años en otras industrias como el comercio y seguros de alta frecuencia, incluso el mapeo del genoma y la secuenciación del genoma. Estos algoritmos toman los datos y entrenan al ordenador para reconocer patrones y predecir el futuro. Nos dio una rara

ventanta de oportunidades tomar esta nueva aplicación de IA y volar con ella, ya que la gente estaba harta de las soluciones antivirus existentes “.

El enfoque matemático de Cylance detiene la ejecución de código dañino sin tener conocimiento previo o empleando una técnica desconocida de ofuscación. Ningún otro producto anti-malware se compara con la precisión, facilidad de administración y eficacia de su producto, dice la compañía, especialmente aquellos que se basan en la comparación de archivos de firmas tradicionales.

Javelin Networks, con sede en Palo Alto, California, se centra en ataques de autenticación, donde un ciberdelincuente ha logrado penetrar en una red de negocios y está a punto de aprovechar su posición para robar activos corporativos. Lo que hace Javelin es usar el reconocimiento de patrones basado en IA para detectar instantáneamente que la red ha sido violada, por lo general reconociendo actividades realizadas sólo por atacantes, como escanear la red para detectar vulnerabilidades, cuentas de usuario fáciles de comprender, aplicaciones y servidores.

Cuando se detecta un ataque, Javelin entra en acción y realiza varias acciones simultáneamente.

- Se levanta una alerta, diciendo a los profesionales de seguridad corporativa y de TI que el ataque está sucediendo.
- Aisla secretamente el punto final comprometido (como el portátil de un usuario final) de acceso a activos corporativos reales, pero de una manera que el atacante no detectará.
- Y luego crea un universo de red ficticio pero real para el atacante, atrapándolo en un laberinto de cientos o miles de recursos atractivos pero simulados.

Mientras que el ciberdelincuente intenta penetrar aún más en esos recursos simulados, buscando propiedad intelectual, contraseñas de red, y otras golosinas, Javelin juega con el hacker como un salmón en una red de pesca. Javelin hace que el atacante pierda tiempo mientras que las herramientas forenses intentan reunir información sobre los propios ciberdelincuentes.

Greg Fitzgerald, COO y CMO de Javelin, afirma: “Javelin es una tecnología de detección de intrusión de próxima generación, adoptando un enfoque donde permite al atacante revelarse a través de sus acciones, de lo que hacen en una máquina en peligro. Javelin está cambiando el juego de cómo se encuentra un atacante en una organización y lo detiene, básicamente asumiendo que un ataque ocurrirá y una máquina se verá comprometida independientemente de si es malware o no lo es. Se ahorra una enorme cantidad de recursos, tanto financieros y humanos, en la recopilación de los datos y el análisis de la información y se acelera el tiempo en que se encuentra a un atacante. La investigación normal actual dice que se tarda entre 150 a 200 días en identificar a un atacante. Javelin ha podido demostrar que puede llevarlo de meses a minutos “.Javelin Networks explica que los ataques dirigidos se basan en el conocimiento de los atacantes de la topología de la red interna de las víctimas. Javelin aparta este conocimiento de ellos, al enmascarar toda la topología. En el momento en que los atacantes actúan sobre la topología enmascarada, son atrapados por el software de reconocimiento de patrones basado en IA, y después de eso, su juego acaba para los malos.

Wedge Networks, con sede en Calgary, Alberta, se centra en evitar que el malware y los ciberataques entren en una red corporativa (o en la casa de un cliente), escaneando el tráfico de Internet y la nube. La compañía utiliza muchas técnicas matemáticas para detectar y evitar que los usuarios de la red tengan virus y otros programas maliciosos, incluyendo ransomware. Debido a que los clientes conocen y confían en la seguridad basada en firmas, la plataforma de seguridad basada en la nube de Wedge emplea escáneres de firma de alta velocidad. Wedge también utiliza la tecnología IA para acelerar el proceso de reconocimiento de malware y se ha asociado con Cylance para aplicar el sistema de seguridad de punto final basado en IA de Cylance para funcionar como parte de la solución de seguridad basada en redes de Wedge.

Wedge Advanced Malware Blocker dirige la tecnología IA de Cylance y otras tecnologías para detectar y bloquear virus y malware avanzado, a nivel de red, para evitar que ingresen a redes empresariales. Orquestando la tecnología de hiper-inspección de Wedge con el motor de aprendizaje de máquina de Cylance y el análisis de amenazas WedgeAMB, ofrece una nueva tecnología innovadora en la prevención de malware, según la compañía.

Según explica Wedge, las amenazas se bloquean en tiempo real, eliminando el coste, la interrupción, el esfuerzo y la vergüenza asociadas con la lucha contra las amenazas después de que han penetrado en la red. También proporciona visibilidad en tiempo real del panorama de amenazas en toda la red, lo que permite al personal de seguridad identificar y centrarse primero en los riesgos más críticos.

James Hamilton, CEO de Wedge Networks afirma: "Tenemos un nuevo producto que combina la política tradicional de seguridad cibernética, que tiende a estar basada en firmas o basada en heurísticas, con algunas de las nuevas aplicaciones de aprendizaje automático de la IA. La combinación de los dos ha demostrado ser muy popular y muy potente. Con el aprendizaje de la máquina se puede entender la motivación del malware, lo que parece y cómo actúa. Usted no necesita saber exactamente lo que es, pero usted sabe cuáles son los atributos. Si puede saber qué está pasando en el punto final, puede entender el comportamiento del malware y bloquearlo. "WedgeAMB incluye WedgeIQ, un motor automatizado de inteligencia de amenazas que recoge datos de amenazas de los sistemas AMB de toda la empresa para caracterizar, correlacionar, analizar y visualizar el panorama de las amenazas en toda la red. El exhaustivo recurso de análisis de amenazas proporciona inteligencia de amenazas para eliminar aún más las amenazas en evolución en tiempo real.

El número de amenazas se está multiplicando a un ritmo espantoso. Según PandaLabs, más de 84 millones de nuevas muestras de malware fueron recogidas a lo largo de 2015, es decir, 230.000 nuevas muestras de malware por día. Así es: un cuarto de millón de nuevas cepas de malware detectadas cada día. La tasa está aumentando. No hay manera de que las tecnologías más antiguas, como el análisis basado en firmas, puedan realizar un seguimiento. La lucha contra el malware y la ciberdelincuencia requiere inteligencia, inteligencia artificial. Cada empresa de ciberseguridad está explorando la IA como una herramienta esencial para ayudar a los clientes a proteger sus redes y puntos finales; Cylance, Javelin Networks y Wedge Networks están por delante de la curva. Esa es una buena noticia para sus clientes y una mala noticia para los ciberdelincuentes.