Acronis

DOCUMENTO TÉCNICO

Uso de la inteligencia artificial para detectar documentos y scripts maliciosos

Consiga una sólida protección multicapa con la ayuda de la inteligencia automática

Los ataques maliciosos aumentan sin cesar y los ciberdelincuentes emplean técnicas de ingeniería social por correo electrónico y otros canales de comunicación como principal vector de ataque. Es muy habitual que los mensajes de correo electrónico fraudulentos contengan archivos adjuntos que, cuando se abren, desencadenan la ejecución de un malware que aprovecha una vulnerabilidad para realizar acciones maliciosas. También se pueden descargar documentos maliciosos mediante un enlace que recibe el usuario a través de los canales de comunicación.

Según los expertos de Acronis, a mediados de 2022 se utilizaban documentos fraudulentos o con carga maliciosa, por ejemplo, archivos de Microsoft Office o PDF de Adobe, en aproximadamente uno de cada tres ataques. Este dato coincide con los observados por otras empresas del sector. El malware suele estar incrustado en un archivo, aunque la cadena de ejecución puede variar. Por ejemplo, puede comenzar por aprovechar una vulnerabilidad, elevar los privilegios y, a continuación, descargar y ejecutar el malware. Hace años que se usan archivos de Office y PDF en ciberataques, ya que este tipo de documentos pueden contener macros incrustadas, códigos shell, código JavaScript e incluso archivos completos. Sin embargo, el problema se ha agravado en los últimos años, ya que, en la actualidad, los hackers utilizan la optimización en los motores de búsqueda (o SEO) para posicionar mejor en los resultados de las búsquedas los archivos maliciosos, en especial, los PDF.

Ocurre algo parecido con los scripts maliciosos ejecutados por herramientas legítimas, como PowerShell. Como en el caso de los documentos maliciosos, el número de ataques que usan scripts maliciosos sigue aumentando, año tras año. En concreto en este tipo de ataques, los expertos de Acronis han observado que el aumento casi se ha duplicado en los dos últimos años. El objetivo de los scripts maliciosos es el mismo: infiltrarse en el sistema, elevar los privilegios, descargar la carga útil y, posteriormente, ejecutarla.

Para las empresas de ciberseguridad, los dos problemas descritos son idénticos, ya que requieren que el usuario distinga cuáles son los documentos o scripts legítimos y cuáles son maliciosos. Afortunadamente hay una forma mucho más eficaz de resolverlos, mediante el uso de aprendizaje automático (ML) e inteligencia artificial (IA), o, como consideramos en Acronis, con la inteligencia automática.

Uso de inteligencia automática en la detección de amenazas

Acronis comenzó a utilizar aprendizaje automático ya en 2017, con nuestra tecnología antiransomware Active Protection. Poco después, creamos un motor de detección estática totalmente basado en IA, que actualmente se utiliza en el producto más emblemático de Acronis: Acronis Cyber Protect.

Este motor se actualiza continuamente y, con cada nuevo modelo de aprendizaje automático introducido, mejora en cuanto a rendimiento y a tasa de detección. Por ejemplo, al principio, se empleaba para analizar los registros de seguimiento de la pila de procesos ejecutados y posteriormente, para analizar archivos y bibliotecas completas, con el propósito de detectar elementos maliciosos. En la actualidad, es capaz de analizar cadenas extraídas de archivos ejecutables y procesar imágenes. Observar la frecuencia de algunos cientos de palabras seleccionadas en las cadenas extraídas ha aportado una mejora de más del 3 % a la tasa de detección.

Lógicamente, se puede aplicar un enfoque similar para detectar documentos y scripts maliciosos. Comencemos con los documentos de Microsoft Office. Aunque Microsoft ha anunciado y comenzado a aplicar esta estrategia, con la desactivación predeterminada de las macros en los documentos que se transfieren por Internet, desafortunadamente esto no resuelve todos los problemas.

Windows agrega el atributo de marca de web (MOTW) a los archivos procedentes de fuentes poco fiables, como Internet o las zonas restringidas; por ejemplo, las descargas del navegador o los adjuntos de mensajes de correo electrónico. Sin embargo, este atributo solo se aplica a los archivos guardados en sistemas de archivos NTFS y no a los que se guardan en dispositivos con formato FAT32. ¿Y qué ocurre cuando el archivo procede de una dirección de correo electrónico de empresa legítima? Además, esto no necesariamente funcionará en entornos en los que el empleo de macros es esencial, por ejemplo, en contabilidad. Sin embargo, se mejora la protección de este tipo de entorno basado en políticas y, en algunos casos, se consiguen evitar típicos ataques de phishing, como los empleados en las campañas de Emotet. Por desgracia, como hemos explicado, esto no basta y crea otras complicaciones para muchas empresas. Por eso los especialistas en IA de Acronis han mejorado nuestro motor de detección con el objetivo de que, gracias al aprendizaje automático, pueda detectar documentos maliciosos.

¿Cuándo considerar que un script de macro es malicioso? Cuando realiza una o varias de las siguientes acciones:

- Crear procesos
- Ejecutar scripts en PowerShell, VBA, etc.
- Descargar archivos de servidores remotos
- Incrustarse en otros archivos o plantillas de Office

Pero lógicamente, la detección real no es tan simple; existen muchos otros parámetros que se deben tener en cuenta. Por ejemplo, el modelo de aprendizaje automático de Acronis verifica los siguientes atributos de los archivos DOCX para llegar a una conclusión:

- Diferentes características del texto y el funcionamiento de VBA
- Datos de proporción, como comentarios, código, etc.
- La entropía de la propia macro, su código y sus comentarios
- Si hay algún elemento oculto y qué es
- Parámetros de indicadores de compromiso (IoC) conocidos, como las URL, los ejecutables, etc.

Aunque no se trata de una lista exhaustiva, sirve para ilustrar cómo muchos aspectos se analizan en un gran conjunto de datos, que se revisa y se actualiza constantemente. Como resultado, estamos alcanzando una excelente tasa de detección, con un tamaño de modelo comprimido de menos de 1 MB. Sin la inteligencia artificial y el aprendizaje automático, sería prácticamente imposible conseguir estos resultados. Además, hay que tener en cuenta que esto es solo una parte de una robusta protección multicapa y que solo se pondrá en práctica si otras tecnologías, como los motores de análisis de seguridad del correo electrónico, los entornos aislados o el filtrado de URL, no detectan antes la amenaza.

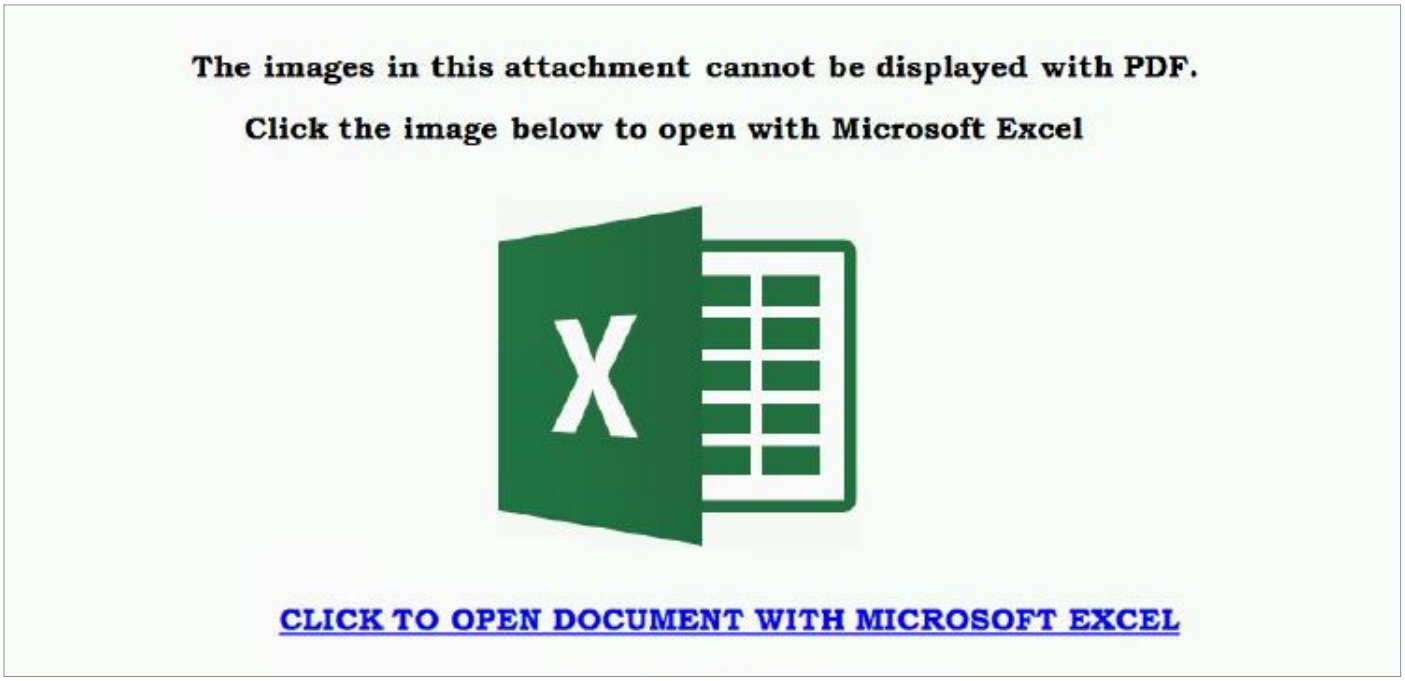
Hace poco, los expertos de Acronis aplicaron una estrategia similar para detectar scripts de AutoIT maliciosos, que suelen usarse en entornos de proveedores de servicios. Con un diminuto modelo de aproximadamente 0,6 MB, ya conseguimos una tasa de detección del 92 %; al igual que en el caso de los archivos DOCX, en los que el modelo se mejora de forma continua.

Eliminación de la amenaza de archivos PDF con carga maliciosa

Además de los documentos Word de Microsoft Office, los archivos PDF de Adobe son también muy populares entre los ciberdelincuentes para comprometer sistemas o introducir malware en la máquina de un usuario. Los archivos PDF, que se basan en el lenguaje PostScript, pueden contener abundante información, como texto, hiperenlaces, componentes multimedia, imágenes, archivos adjuntos, metadatos, etc., lo que los convierte en un formato que ofrece multitud de posibilidades. El formato PDF tiene una función de "acciones" que permite abrir un archivo o un enlace web, ejecutar código JavaScript y realizar muchas otras operaciones que, como es de imaginar, pueden tener fines malintencionados.

Los documentos PDF se pueden visualizar con navegadores y con diferentes programas de software, y todos ellos pueden tener, o de hecho tienen, vulnerabilidades que los ciberdelincuentes pueden aprovechar, por ejemplo, las de ejecución de código arbitrario, desbordamiento de búfer, corrupción de memoria o lectura fuera de los límites, entre muchas otras. En la actualidad, existen cientos de vulnerabilidades y riesgos comunes (CVE) para programas de lectura de PDF (se conocen casi 300 vulnerabilidades para Adobe Acrobat Reader solamente). Los investigadores de seguridad y los ciberdelincuentes descubren casi a diario nuevos exploits relacionados con los PDF.

Este es un ejemplo de una vulnerabilidad CVE-2021-28550 que se observó en circulación: las versiones de Acrobat Reader DC 2021.001.20150 (y anteriores); 2020.001.30020 (y anteriores); y 2017.011.30194 (y anteriores) sufren una vulnerabilidad UAF (Use Afer Free). Un atacante no autenticado puede aprovechar esta vulnerabilidad para la ejecución de código arbitrario en el contexto del usuario actual. Para ello, se requiere de la interacción del usuario, ya que es necesario que la víctima abra un archivo malicioso.



Ejemplo de phishing con un enlace malicioso incrustado en un archivo de PDF.

El modelo de Acronis basado en el aprendizaje automático para la detección de PDF maliciosos, al igual que con otros tipos de archivos descritos, comprueba distintos parámetros para llegar a la conclusión correcta:

- Entropía
- Número total de caracteres
- Número de palabras clave especiales
- Número de líneas; líneas de asignaciones especiales
- Etc.

Como resultado, se consigue una tasa de detección idéntica y muy eficaz, como se ha descrito anteriormente.

La formación para concienciar sobre ciberseguridad puede ser de gran ayuda

Lógicamente, es fundamental integrar este tipo de modelo de detección en una solución de ciberprotección. Pero además, la postura de seguridad global de las empresas y las personas mejorará considerablemente si los usuarios son conscientes de las amenazas y saben cómo se presentan y cómo reaccionar de manera adecuada, ya que, en la mayoría de los casos, para que un documento o un script malicioso se ejecute, se necesita la intervención del usuario. Y sin esta intervención, tampoco habrá amenaza.

Esta formación para concienciar en seguridad exige que se cumplan las archiconocidas reglas básicas de la comunidad de seguridad:

- Verificar siempre de dónde viene un mensaje de correo electrónico o un enlace ¿Conoce al remitente? ¿Estaba esperando este archivo? Comprobar la dirección de correo electrónico real del remitente, y no solo el nombre o el alias.
- Si el usuario ya ha hecho clic en el archivo y un mensaje indica alguna clase de incompatibilidad, pide que se active algo, muestra algún enlace o un código captcha falso, o algo similar, debe cerrarse y eliminarse inmediatamente, e informar al equipo de seguridad.
- Si al hacer clic en el archivo, no se abre nada, también es mala señal. Si ha abierto un archivo y el resultado no es el esperado, es posible que ya haya caído en la trampa. Debe informar de inmediato al equipo de seguridad.

Por lo tanto, en resumen, la mejor regla es no abrir archivos adjuntos ni hacer clic en enlaces sin pensarlo dos veces. Debe comprobarse todo y, si aun así se tienen dudas, solicitar ayuda del equipo de seguridad. No baje la guardia y protéjase.