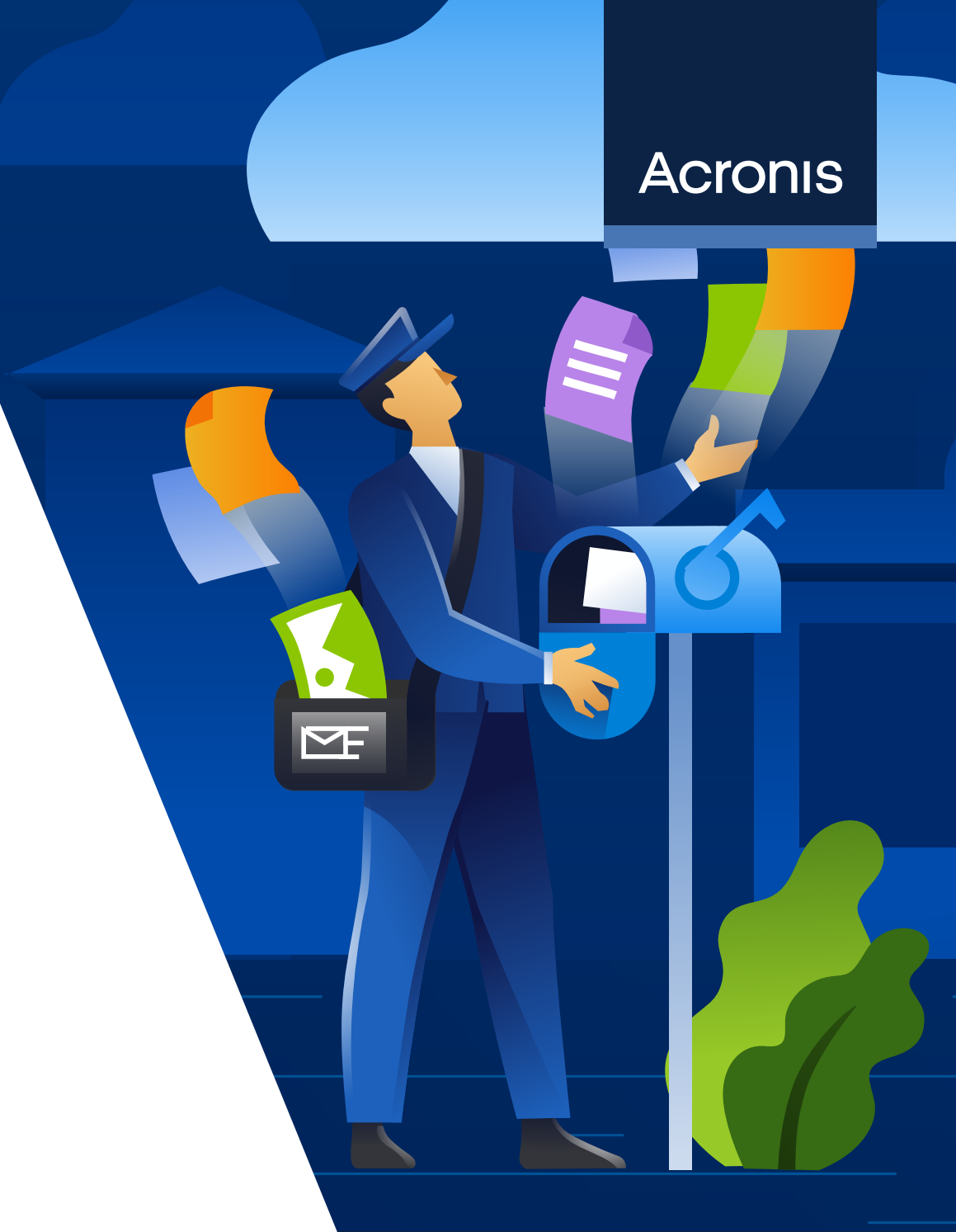
Acronis



DOCUMENTO TÉCNICO

Uso de inteligencia artificial para detectar documentos y scripts maliciosos

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

Con los ataques maliciosos en constante aumento, son cada vez más los ciberdelincuentes que emplean la ingeniería social por medio del correo electrónico y otros canales de comunicación como el vector principal y más importante de los ataques. Con mucha frecuencia, se reciben correos electrónicos engañosos con archivos adjuntos que, al abrirlos, desencadenan la ejecución de un malware que aprovecha una vulnerabilidad para realizar acciones maliciosas. También es posible que se descargue un documento malicioso 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 maliciosos o engañosos, por ejemplo, archivos de Microsoft Office o PDF de Adobe, en aproximadamente una tercera parte de todos los ataques. Otros actores de la industria han enfrentado un panorama similar. Por lo general, el malware está incrustado en un archivo, aunque la cadena de su ejecución puede variar. Por ejemplo, en un principio, se aprovecha una vulnerabilidad, se elevan los privilegios y, luego, el malware se descarga y ejecuta. Los archivos de Office y PDF se utilizan desde hace años en los ciberataques, ya que pueden contener macros incrustadas, shellcodes, código JavaScript y hasta archivos enteros dentro de ellos. Sin embargo, el problema se agravó en los últimos años, ya que, en la actualidad, los hackers utilizan la optimización en motores de búsqueda (SEO) para posicionar mejor los archivos maliciosos, en especial, los PDF, en los resultados que se obtienen.

Otro problema similar ocurre con los scripts maliciosos que ejecutan herramientas legítimas, como PowerShell. Como sucede con los documentos maliciosos, la cantidad de ataques que utilizan scripts maliciosos crece de manera incesante año a año. En particular, los expertos de Acronis observaron casi el doble de crecimiento en esa clase de ataques durante los últimos dos años. El objetivo de los scripts maliciosos es el mismo: infiltrarse en el sistema, elevar los privilegios, descargar la carga útil y, luego, ejecutarla.

Para las empresas de ciberseguridad, los dos problemas detallados anteriormente son idénticos, ya que requieren que el usuario distinga entre los documentos o scripts legítimos y maliciosos. La buena noticia es que el problema puede resolverse de forma mucho más eficaz mediante el uso del aprendizaje automático (AA) y la inteligencia artificial (IA), o, como consideramos en Acronis, con la inteligencia automática.

El uso de la inteligencia automática en la detección de amenazas

En Acronis, empezamos a utilizar el aprendizaje automático en 2017, al introducir nuestra tecnología de ransomware Active Protection. Poco tiempo después, creamos un motor de detección estática basado por completo en la IA, que se utiliza actualmente en el producto más emblemático de Acronis: Acronis Cyber Protect.

Este motor se actualiza de forma constante y, con cada modelo de aprendizaje automático que se introduce, mejora un poco más en cuanto a su rendimiento y tasa de detección. Por ejemplo, al principio, se utilizaba para analizar los registros de seguimiento de la pila de los procesos ejecutados y posteriormente, para analizar archivos y bibliotecas completas, con el propósito de detectar los que fueran 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 generó una mejora de más del 3 % en la tasa de detección.

Como se imaginará, se puede utilizar un enfoque similar para detectar documentos y scripts maliciosos. Comencemos con los documentos de Microsoft Office. Si bien, hace poco tiempo, cuando las macros se desactivaron por defecto en los documentos transmitidos por Internet, Microsoft anunció y comenzó a aplicar esta estrategia, por desgracia, esto no resuelve todos los problemas. Windows agrega el atributo de marca de web (MOTW) a los archivos que provienen de ubicaciones poco confiables, como Internet o una zona restringida; por ejemplo, las descargas del navegador o los adjuntos de los correos electrónicos. Sin embargo, el atributo solo se aplica a los archivos guardados en un sistema de archivos NTFS y no a los que se guardan en dispositivos con formato FAT32. ¿Y qué sucede cuando el archivo proviene de una dirección de correo electrónico de Office legítima? Por no hablar de entornos en los que el trabajo dependa en gran medida de las macros, por ejemplo, en el ámbito de la contabilidad. Sin embargo, este entorno basado en políticas se vuelve más seguro y, en algunos casos habituales de ataques de phishing, como en las campañas de Emotet, pueden prevenirse exitosamente. Por desgracia, como dijimos antes, esto no alcanza y genera otras complicaciones para muchas empresas. Es por eso que los especialistas en IA de Acronis mejoraron nuestro motor de detección, para que tenga la capacidad de detectar documentos maliciosos, gracias al poder del aprendizaje automático.

¿Qué script de macro puede percibirse como malicioso? Aquel que 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 u otras 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 un veredicto:

- Diferentes textos y características de 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 esta no es una lista exhaustiva, ayuda a explicar que muchos aspectos se analizan en el marco de un gran conjunto de datos, el cual se revisa y actualiza de forma constante. Como resultado, alcanzamos una tasa de detección excelente, con un tamaño de modelo comprimido de menos de 1 MB. Sin la IA y el AA, alcanzar estos resultados es casi imposible. Además, debe tener en cuenta que esta es apenas una parte de una sólida protección multicapa que solo se activará si otras tecnologías, como los motores de análisis de seguridad del correo electrónico y de entornos aislados, o el filtrado de URL, no detectan la amenaza antes.

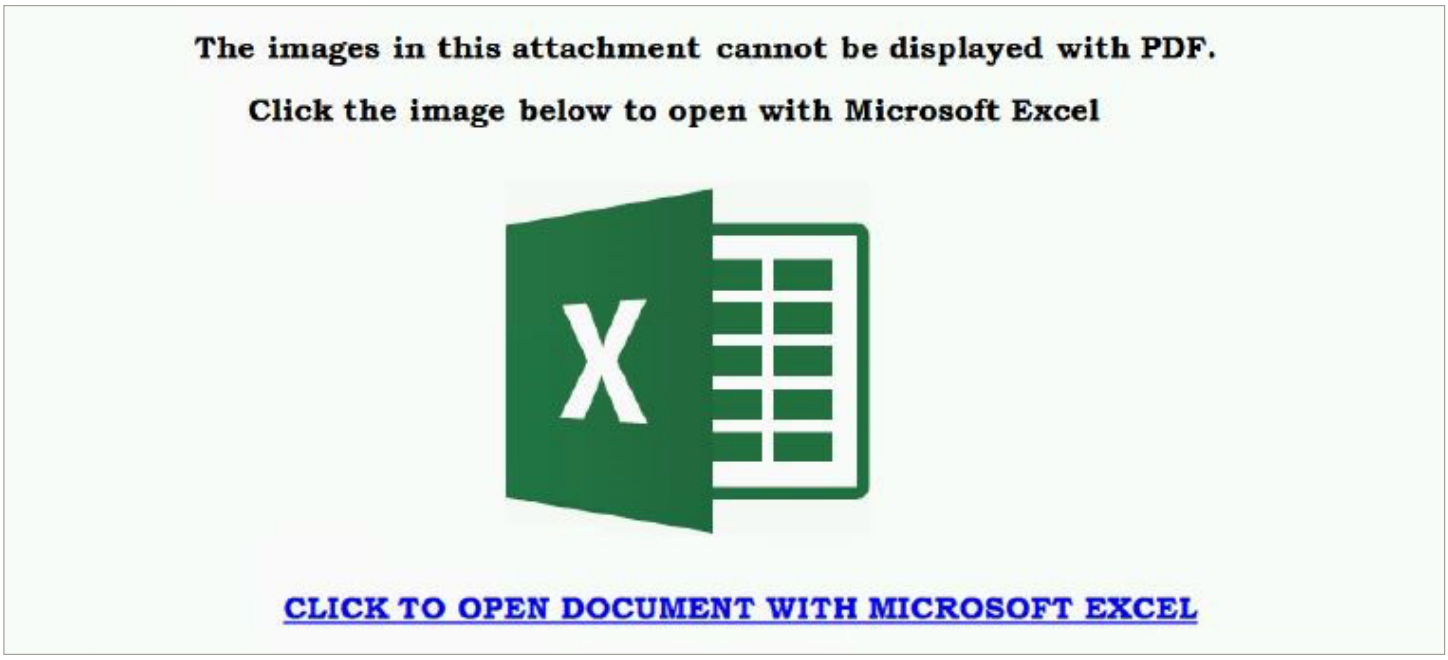
Hace poco tiempo, los expertos de Acronis pusieron en marcha una estrategia similar para detectar scripts de AutoIT maliciosos, que se utilizan con mucha frecuencia en el entorno de los proveedores de servicios. Con un modelo diminuto de unos 0,6 MB, ya podemos proveer una tasa de detección del 92 %; lo mismo sucede con los archivos DOCX, en los que el modelo mejora de forma continua.

Eliminación de la amenaza de archivos PDF con carga maliciosa

Además de los documentos de Microsoft Office Word, los archivos PDF de Adobe son una herramienta muy utilizada entre los ciberdelincuentes para poner en riesgo un sistema o introducir malware en la máquina de un usuario. Los archivos PDF, que se basan en el lenguaje PostScript, pueden contener mucha información, como texto, hiperenlaces, componentes multimedia, imágenes, archivos adjuntos, metadatos, etc., lo que los convierte en un formato muy poderoso. El formato de PDF tiene una función de "acciones" que permite abrir un archivo o un enlace web, ejecutar un código JavaScript y realizar muchas otras operaciones que, como es de imaginar, pueden ser malintencionadas.

Los documentos PDF se pueden visualizar con navegadores y con diferentes programas de software de lectura, y todos ellos pueden tener o tienen vulnerabilidades que los ciberdelincuentes pueden aprovechar, como la ejecución de código arbitrario, el desbordamiento de búfer, la corrupción de memoria, la lectura fuera de los límites y muchas otras. En la actualidad, existen cientos de vulnerabilidades y riesgos comunes (CVE) para programas de lectura de PDF; por ejemplo, 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) se ven afectadas por una vulnerabilidad UAF (Use Afer Free). Un atacante no autenticado puede aprovechar esta vulnerabilidad para realizar una 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 de detección de PDF maliciosos, basado en el aprendizaje automático, al igual que con otras clases de archivos mencionadas previamente, comprueba una variedad de parámetros para llegar al veredicto correcto:

- Entropía
- Conteo de caracteres totales
- Conteo de palabras clave especiales
- Cantidad de líneas; líneas de asignaciones especiales
- Etc.

Como resultado, se alcanza una tasa de detección idéntica y muy eficaz, tal como se detalló anteriormente.

Capacitar a las personas en ciberseguridad puede ser de gran ayuda

Es fundamental integrar esta clase de modelo de detección en una solución de ciberprotección. Sin embargo, los niveles de seguridad de las empresas y las personas en general pueden mejorar considerablemente si los usuarios saben cuáles son las amenazas y cómo se presentan, y reaccionan de la manera correcta, ya que, en la mayoría de los casos, interactuar con un documento o un script malicioso requiere de la intervención del usuario. Esto quiere decir que, si no existe tal intervención, tampoco habrá amenaza.

Para esta capacitación, es necesario cumplir las archiconocidas reglas básicas de la comunidad de seguridad:

- Verifique siempre el origen de un correo electrónico o enlace. ¿Conoce al remitente? ¿Estaba esperando este archivo? Asegúrese de comprobar la dirección de correo electrónico real de la que proviene y no solo el nombre o el alias.
- Si el usuario ya hizo clic en el archivo y se indicó alguna clase de incompatibilidad, se pidió que se habilitara algo, se mostró un enlace o código captcha falso, o bien algún otro mensaje similar, el archivo debe cerrarse y eliminarse de inmediato, y se debe informar sin demoras al equipo de seguridad.
- Si al hacer clic en el archivo, no se abrió nada, esto también es una mala señal. Si se abrió un archivo y no es lo que esperaba, es posible que ya haya caído en la trampa, por lo que debe informar de inmediato al equipo de seguridad.

En pocas palabras, la mejor regla es no abrir archivos adjuntos ni hacer clic en enlaces de inmediato. Verifique todo dos veces y, si aún tiene dudas, comuníquese con un equipo de seguridad. Manténgase alerta para mantenerse a salvo.

Acronis

Encontrará más información en www.acronis.com