Acronis Empleo del aprendizaje automático en la protección de los datos

Acronis Active Protection, introducida en enero de 2017, es una tecnología avanzada que utiliza sofisticados análisis para supervisar los sistemas con el fin de detectar comportamientos atribuibles al ransomware y detenerlos rápidamente. A pesar de los magníficos resultados obtenidos en las pruebas independientes y los elogios recibidos en los medios de comunicación, Acronis quería que su solución fuera aún más robusta. Para conseguirlo hemos empleado tecnologías de aprendizaje automático e inteligencia artificial.

CÓMO AYUDA EL APRENDIZAJE AUTOMÁTICO

El aprendizaje automático suele asociarse al big data, es decir, al análisis de ingentes volúmenes de datos para conseguir resultados que permitan actuar. Esta técnica se basa en la cantidad de datos y en los algoritmos elegidos, por lo que cuanto mayor sea la muestra de datos, mejores serán los resultados.

¿Y cómo utiliza Acronis esta tecnología? El primer paso es efectuar un análisis de volcados de pila que ofrece información sobre las subrutinas de los programas. Esta técnica se utiliza normalmente para ciertos tipos de depuración, ya que ayuda a los ingenieros de software a averiguar dónde se encuentra un problema o cómo funcionan juntas varias subrutinas durante la ejecución.

Acronis aplica este enfoque a los ataques de ransomware, utilizando el aprendizaje automático para detectar inyecciones de código malicioso.

CÓMO FUNCIONA EL APRENDIZAJE AUTOMÁTICO

Acronis ha analizado enormes volúmenes de datos limpios con sistemas Windows que ejecutan multitud de procesos legítimos. De esta forma, a partir de dichos procesos, hemos obtenido millones de volcados de pila legítimos y hemos generado distintos modelos de comportamiento "correcto" utilizando el aprendizaje basado en árboles de decisión. Además, hemos recopilado volcados de pila maliciosos de distintas fuentes con el fin de tener ejemplos del caso contrario.

Basándonos en estos millones de muestras de aprendizaje, hemos identificado patrones de comportamiento.

El aprendizaje basado árboles de decisión nos permite pasar de la observación a las conclusiones sobre su valor objetivo y crear un modelo que pueda predecir con precisión el valor de un nuevo elemento basándose en factores identificables. Los modelos permiten a Acronis construir respuestas adecuadas para los valores objetivo. En lugar de ralentizar la máquina cliente recopilando y enviando datos para su análisis, los modelos integrados ofrecen el mismo nivel de protección con una mayor eficacia.

CUÁNDO SE ACTIVA EL APRENDIZAJE AUTOMÁTICO

Como hemos dicho, Acronis Active Protection se basa en heurística de comportamientos. En la versión 2.0 añadimos nuevos procedimientos heurísticos para localizar procesos legítimos. Si Acronis Active Protection detecta un comportamiento sospechoso en un proceso legítimo, obtiene un volcado de pila y se lo envía al módulo de aprendizaje automático de Acronis. Allí el comportamiento se compara con modelos existentes de volcados de pila limpios e infectados con el fin de determinar si se trata de una amenaza.

Si se llega a la conclusión de que el comportamiento es de naturaleza maliciosa, el usuario recibe una alerta que le sugiere que bloquee el proceso.

UN NUEVO NIVEL DE DEFENSA ANTIRANSOMWARE

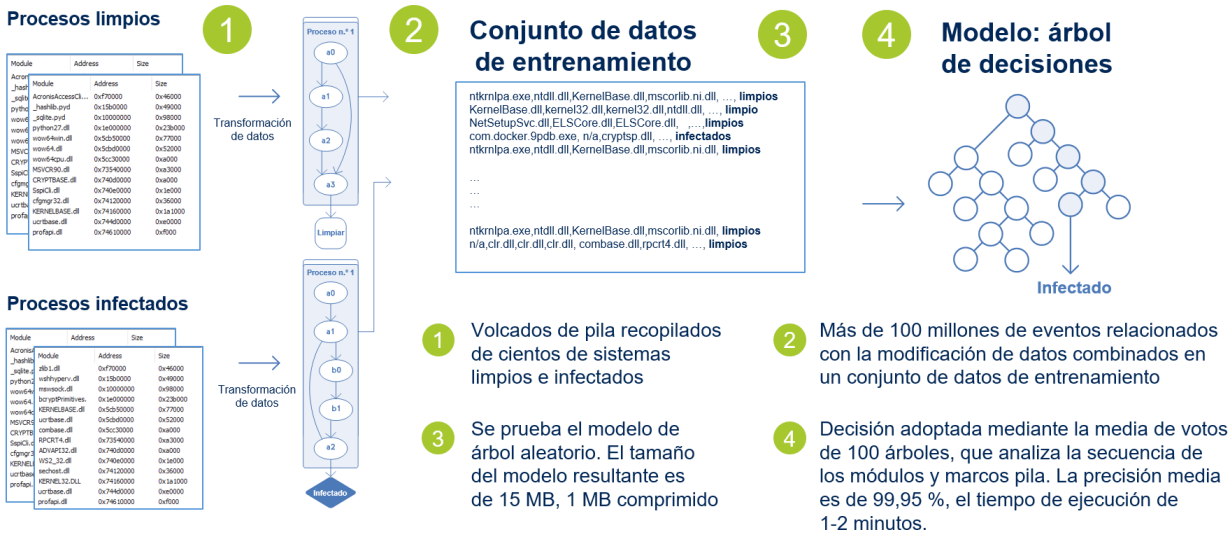
Todas estas tecnologías, y principalmente el aprendizaje automático, llevan a Acronis Active Protection a un nuevo nivel, especialmente en lo referente a la lucha contra amenazas de tipo día cero. Esta tecnología crea un modelo de procesos legítimos, de forma que aunque los ciberdelincuentes encuentren una nueva vulnerabilidad o forma de filtrarse en el sistema, el aprendizaje automático detectará los procesos de ransomware y los bloqueará.

La infraestructura de aprendizaje automático de Acronis se ha desarrollado de manera que se carguen con regularidad los nuevos datos de programas, anonimizados para su análisis. Esta infraestructura puede gestionar millones de solicitudes simultáneamente y, gracias al flujo constante de información, los nuevos modelos de comportamiento están listos mucho más rápidamente. Mientras tanto, las continuas actualizaciones de la heurística del producto incrementan aún más la seguridad. Este trabajo que se realiza entre bastidores en fracciones de segundo pasa desapercibido para los usuarios; ellos simplemente activan Acronis Active Protection y se olvidan de todo.

EL FUTURO

Acronis sigue ampliando el uso de esta tecnología aprovechando el aprendizaje automático para el análisis de código estático. Este análisis se realizará en la fase de preejecución, para que cuando el usuario descargue un archivo o lo copie en un disco duro, se compruebe su código inmediatamente para detectar anomalías. Si se descubre algo sospechoso, el proceso se puede bloquear antes de que un usuario o un script automático lo inicie.

De hecho, los modelos de aprendizaje automático se pueden utilizar para analizar scripts y Acronis ya está trabajando en esta dirección. Hay pruebas realizadas por NioGuard Security Lab que ponen de manifiesto que mientras la mayoría de las soluciones antivirus no consiguen detectar los ataques basados en scripts, Acronis Active Protection ofrece buenos resultados. Pero a pesar de ello, seguiremos mejorando aún más nuestras tecnologías antiransomware.



Para obtener más información, visite **www.acronis.com.**