Acronis L'apprentissage automatique au service de la sécurité des données

Introduite en janvier 2017, Acronis Active Protection est une technologie de pointe qui a recours à une méthodologie sophistiquée d'analyse et de surveillance des systèmes, dans le but de détecter les comportements associés aux ransomwares et de les bloquer rapidement. Elle a obtenu d'excellents résultats lors de tests indépendants et a été largement saluée par les médias. Pourtant, Acronis voulait encore améliorer la robustesse de la solution. Nous y sommes parvenus en faisant appel à l'apprentissage automatique et à l'intelligence artificielle.

ATOUTS DE L'APPRENTISSAGE AUTOMATIQUE

Le concept d'apprentissage automatique (machine learning) est souvent associé au Big Data, c'est-à-dire l'analyse d'énormes volumes de données visant à produire des résultats exploitables. Comme l'apprentissage automatique repose sur le volume de données et les algorithmes choisis, plus l'échantillon de données est important, meilleurs sont les résultats.

Comment Acronis utilise-t-il cette technologie? La première étape consiste à effectuer une analyse de la trace de pile, qui rend compte des appels du programme concerné. Cette technique est couramment utilisée pour certains types de débogage, car elle permet aux développeurs de logiciels de déterminer l'origine d'un problème ou comment diverses sous-routines interagissent pendant l'exécution.

Acronis applique cette approche aux attaques par ransomware, en utilisant l'apprentissage automatique pour détecter les injections de code malveillant.

FONCTIONNEMENT DE L'APPRENTISSAGE **AUTOMATIQUE**

Acronis a analysé d'énormes volumes de données saines à l'aide de systèmes Windows qui exécutent une multitude de processus légitimes. Nous avons ensuite extrait plusieurs millions de traces de pile légitimes de ces processus et construit différents modèles de comportement « correct » à l'aide de l'apprentissage par arbre de décision. Nous avons également recueilli des traces de pile malveillantes provenant de diverses sources afin de fournir des contre-exemples.

Des modèles de comportement sont alors identifiés sur la base de ces millions d'échantillons d'apprentissage.

L'apprentissage par arbre de décision nous permet de passer de l'observation d'un élément à la formulation de conclusions sur sa valeur cible, puis à la création d'un modèle qui prédit correctement la valeur d'un nouvel élément en fonction de facteurs identifiables. Les modèles permettent à Acronis d'intégrer des réponses appropriées aux valeurs cibles. Au lieu de ralentir la machine cliente en collectant et transmettant les données à analyser, les modèles intégrés offrent le même niveau de protection avec une plus grande efficacité.

QUAND L'APPRENTISSAGE AUTOMATIQUE EST-IL ACTIVÉ?

Comme expliqué ci-dessus, Acronis Active Protection repose sur l'analyse heuristique comportementale. Dans la version 2.0, nous avons ajouté plusieurs nouvelles règles heuristiques qui recherchent les processus légitimes. Si Acronis Active Protection détecte un comportement étrange dans un processus légitime, il prélève une trace de pile et l'envoie au module d'apprentissage automatique d'Acronis. Là, le comportement est comparé aux modèles existants de traces de pile saines et infectées, pour déterminer s'il s'agit ou non d'une menace.

Si le comportement est identifié comme étant de nature malveillante, l'utilisateur reçoit une alerte lui suggérant de bloquer le processus.

NOUVEAU NIVEAU DE PROTECTION **CONTRE LES RANSOMWARES**

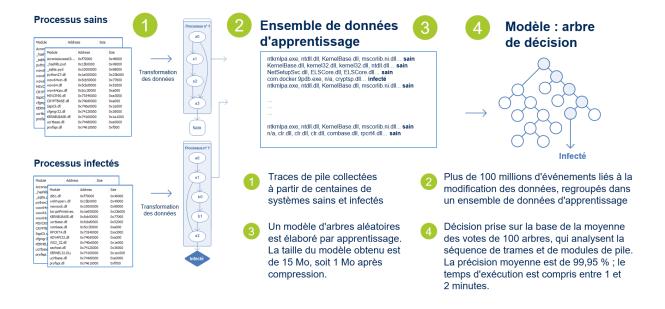
Toutes ces technologies, l'apprentissage automatique en tête, améliorent considérablement l'efficacité d'Acronis Active Protection, en particulier lorsqu'il s'agit de contrer les menaces jour zéro. Acronis Active Protection crée un modèle pour les processus légitimes pour que, même si des pirates trouvent une nouvelle vulnérabilité ou un nouveau mécanisme, l'apprentissage automatique puisse détecter les processus du ransomware et les arrêter.

L'infrastructure d'apprentissage automatique d'Acronis est conçue de sorte que les nouvelles données de programme anonymisées soient téléchargées régulièrement pour analyse. Elle peut gérer plusieurs millions de requêtes simultanément et, grâce au flux constant d'informations, les nouveaux modèles de comportement sont prêts beaucoup plus rapidement. Pendant ce temps, des mises à jour constantes des règles d'analyse heuristique du produit renforcent encore la sécurité. Rien de tout ce travail en coulisses n'est perceptible pour les utilisateurs ; ceux-ci peuvent simplement activer Acronis Active Protection et se consacrer à leurs activités sans plus y penser.

LES PROJETS D'AVENIR D'ACRONIS

Acronis continue d'étendre l'utilisation de cette technologie en appliquant l'apprentissage automatique à l'analyse de code statique. Cette analyse sera effectuée à l'étape de préexécution, si bien que lors du téléchargement ou de la copie d'un fichier sur un disque dur, son code sera instantanément vérifié fin de détecter les anomalies éventuelles. En cas d'élément suspect, le processus peut être bloqué avant même d'être lancé par un utilisateur ou un script automatisé.

En effet, les modèles d'apprentissage automatiques peuvent être utilisés pour analyser les scripts et Acronis travaille déjà dans ce sens. En fait, les tests effectués par NioGuard Security Lab ont montré que si la plupart des solutions antivirus sont incapables de détecter une attaque basée sur des scripts, Acronis Active Protection offre quant à lui des performances satisfaisantes. Malgré ce succès, nous continuons de tout mettre en œuvre pour améliorer continuellement nos technologies anti-ransomware.





Pour plus d'informations, visitez notre site : **www.acronis.com**.