Acronis

LIVRE BLANC

Détection des documents et scripts malveillants grâce à l'IA

Adopter une protection multiniveau hors pair avec l'aide de l'intelligence artificielle

Avec l'essor des attaques malveillantes, de plus en plus de cybercriminels utilisent l'ingénierie sociale comme principal vecteur d'attaques déployées via e-mail ou d'autres canaux de communication. Très souvent, ces e-mails frauduleux contiennent des pièces jointes malveillantes qui, une fois ouvertes, déclenchent l'exploitation par malware d'une vulnérabilité dans le but d'exécuter des actions illicites. Il arrive aussi qu'un document malveillant soit associé à un lien reçu par un utilisateur sur divers canaux de communication.

Selon les experts Acronis, à la mi-2022, des documents malveillants ou dangereux tels que des fichiers Microsoft Office ou Adobe PDF étaient utilisés dans un tiers des attaques environ. D'autres protagonistes du secteur font le même constat. Les malwares sont généralement incorporés dans un fichier, même si la chaîne d'exécution peut varier. Par exemple, l'attaque commence par l'exploitation d'une vulnérabilité, le cybercriminel effectue ensuite une élévation des privilèges et, enfin, un malware est téléchargé et exécuté. Les fichiers Office et PDF sont utilisés depuis des années dans le cadre de cyberattaques, car ils permettent d'incorporer des macros, des shellcodes, du code JavaScript et même des fichiers entiers. Cependant, le problème s'est aggravé dernièrement, et les pirates utilisent désormais des techniques d'optimisation SEO (Search Engine Optimization) afin de placer les fichiers malveillants, en particulier les PDF, en haut des classements de résultats des moteurs de recherche.

Une technique similaire consiste à utiliser des scripts malveillants exécutés au moyen d'outils légitimes tels que PowerShell. Le nombre d'attaques employant des scripts malveillants, ou des documents malveillants, est en augmentation constante année après année. En outre, les experts Acronis ont observé que la croissance de ces attaques a pratiquement doublé au cours des deux dernières années. Dans le cas des scripts malveillants, l'objectif est le même : infiltrer le système, augmenter le niveau de privilèges, télécharger, puis exécuter la charge active.

Du point de vue des entreprises de cybersécurité, les deux problèmes décrits ci-dessus sont identiques, car ils exigent de l'utilisateur qu'il puisse faire la différence entre des documents et scripts dangereux ou légitimes. La bonne nouvelle, c'est que ce problème peut être résolu bien plus efficacement en recourant à deux technologies critiques : l'apprentissage automatique (machine learning, ML) et l'intelligence artificielle (IA).

Détection des menaces basée sur l'apprentissage automatique et l'intelligence artificielle

Acronis a commencé à recourir à l'apprentissage automatique en 2017 déjà, époque où l'entreprise a introduit la technologie antiransomware Active Protection. Peu de temps après, nous avons créé un moteur de détection statique basé sur l'IA, actuellement utilisé dans notre solution phare Acronis Cyber Protect.

Ce moteur est constamment mis à jour et, avec l'introduction de chaque nouveau modèle d'apprentissage automatique, il gagne en performances et en taux de détection. Ainsi, il a été initialement utilisé pour analyser des traces de pile de processus exécutés, passant ensuite à l'analyse de fichiers et de bibliothèques entiers afin de détecter les éléments malveillants. À l'heure actuelle, ce moteur est capable d'analyser des chaînes extraites de fichiers exécutables et des images de processus. Nous avons obtenu une amélioration de plus de 3 % du taux de détection en extrayant quelques centaines de mots dans des chaînes en tant que caractéristiques supplémentaires, puis en les analysant afin d'en déterminer la fréquence.

Comme vous l'imaginez sans doute, une approche similaire peut servir à détecter des documents et scripts malveillants. Commençons par les documents Microsoft Office. Même si Microsoft a récemment annoncé son intention de suivre une approche similaire, et commencé à appliquer la mesure, par exemple en désactivant par défaut les macros dans les documents qui transitent par Internet, cela ne peut malheureusement pas tout résoudre.

L'attribut MOTW (Mark Of The Web) est ajouté par Windows aux fichiers provenant d'un emplacement non approuvé, comme Internet ou une zone soumise à restrictions, par exemple des téléchargements de navigateur ou des pièces jointes d'e-mail. Cela étant, l'attribut ne s'applique qu'aux fichiers enregistrés sur un système de fichiers NTFS, et pas sur des équipements en FAT32. Qu'en est-il si le fichier provient d'un e-mail professionnel légitime ? De surcroît, la stratégie ne fonctionnera pas nécessairement dans un environnement qui repose en grande partie sur les macros, comme la comptabilité. Toutefois, un environnement doté de politiques de sécurité de ce type est plus sécurisé, et permet de prévenir certaines attaques de phishing courantes telles que celles des campagnes Emotet. Mais comme nous l'avons déjà mentionné, la mesure n'est malheureusement pas suffisante et peut entraîner des complications pour de nombreuses entreprises. Voilà pourquoi les spécialistes de l'IA Acronis ont optimisé notre moteur de détection pour permettre l'identification de documents malveillants, grâce à la puissance de l'apprentissage automatique.

Quel script de macro peut être perçu comme malveillant ? Celui qui exécute au moins l'une des opérations suivantes :

- Création de processus
- Exécution de scripts PowerShell, VBA, etc.
- Téléchargement de fichiers depuis des serveurs distants
- Incorporation dans d'autres fichiers ou modèles de fichiers Office

Or, de toute évidence, la détection n'est pas si simple, car il est nécessaire de prendre en compte de nombreux autres paramètres. Par exemple, le modèle d'apprentissage automatique Acronis vérifie les attributs suivants des fichiers DOCX pour parvenir à un verdict :

- Diverses fonctions texte et VBA
- Données de ratio telles que commentaires, code, etc.
- Entropie d'une macro elle-même, son code et ses commentaires
- Mesures d'obfuscation présentes et éléments obfusqués
- Paramètres d'indicateurs de compromission connus tels qu'URL, fichiers exécutables, etc.

La liste n'est bien entendu pas exhaustive, mais elle illustre comment de nombreux éléments sont analysés dans un grand ensemble de données, lui-même constamment révisé et mis à jour. Par conséquent, nous atteignons un excellent taux de détection, avec un modèle de petite taille représentant moins de 1 Mo avec compression. Sans intelligence artificielle et apprentissage automatique, il est pratiquement impossible d'obtenir de tels résultats. Gardez également à l'esprit qu'il ne s'agit que d'une partie de la protection multiniveau robuste qui ne sera déclenchée que si la menace n'est pas détectée par les autres technologies en amont, comme les moteurs d'analyse des e-mails ou les analyses en sandbox, ou encore le filtrage d'URL.

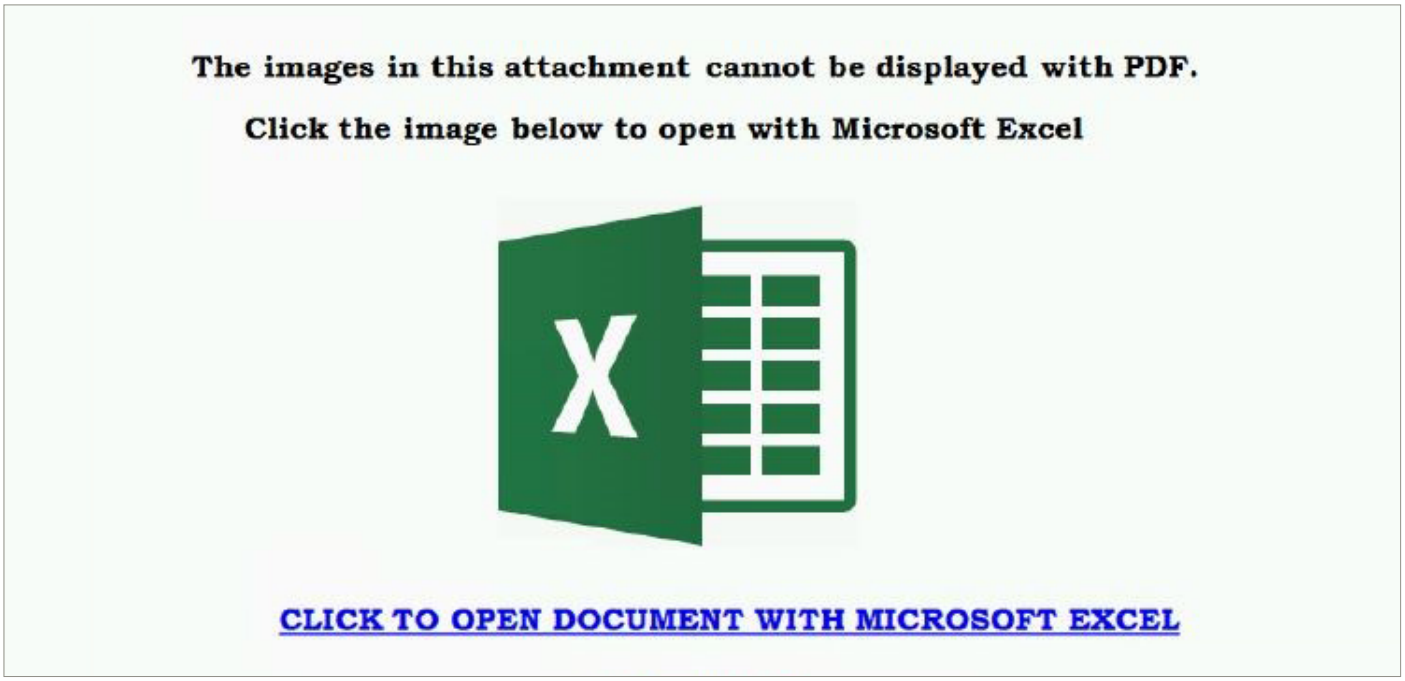
Une approche très similaire a récemment été adoptée par les experts Acronis pour détecter les scripts AutoIT malveillants, souvent utilisés dans les environnements de fournisseurs de services. Avec un modèle de faible encombrement d'environ 0,6 Mo, nous pouvons déjà offrir un taux de détection de 92 %. Il en va de même pour les fichiers DOCX, pour lesquels le modèle enregistre constamment des améliorations.

Élimination de la menace représentée par les PDF dangereux

À l'instar des documents Word de la suite Microsoft Office, le format de document PDF (Portable Document Format) d'Adobe est un outil très prisé par les cybercriminels pour compromettre un système ou déposer un malware sur l'ordinateur d'un utilisateur. Basé sur le langage PostScript, un fichier PDF peut contenir énormément d'informations, dont du texte, des liens hypertextes, des contenus multimédias, des images, des pièces jointes, des métadonnées, etc. — ce qui rend ce format particulièrement efficace. Les fichiers PDF peuvent également être associés à une fonctionnalité d'« action » permettant d'ouvrir un lien web ou un fichier, d'exécuter du code JavaScript ainsi que de nombreuses autres opérations qui, comme vous l'imaginez, peuvent être utilisées à des fins malveillantes.

Les documents PDF peuvent être consultés à l'aide de navigateurs et d'une large gamme de logiciels de lecture, qui peuvent tous contenir des vulnérabilités susceptibles d'être exploitées par des cybercriminels. Parmi elles, on peut citer l'exécution arbitraire de code, les dépassements de mémoire tampon, la corruption de mémoire et les lectures hors limites. On dénombre actuellement des centaines de vulnérabilités CVE pour les lecteurs PDF, avec près de 300 vulnérabilités connues rien que pour Adobe Acrobat Reader. Les chercheurs en sécurité et les cybercriminels découvrent de nouveaux exploits visant les PDF pratiquement chaque jour.

Voici un exemple de vulnérabilité CVE-2021-28550 dont on a observé l'exploitation en environnement réel : Acrobat Reader DC versions 2021.001.20150 (et antérieures) ; 2020.001.30020 (et antérieures) ; et 2017.011.30194 (et antérieures) sont affectés par une vulnérabilité de type « Use After Free ». Un attaquant non authentifié pourrait exploiter cette vulnérabilité pour effectuer une exécution de code arbitraire dans le contexte de l'utilisateur actuel. L'exploitation nécessite une intervention de l'utilisateur, dans le sens où la victime doit ouvrir un fichier malveillant.



Exemple de phishing avec un lien malveillant intégré dans un fichier PDF

Le modèle de détection des fichiers malveillants d'Acronis basé sur l'apprentissage automatique, qu'il s'applique aux PDF ou aux autres types de fichiers évoqués précédemment, vérifie une série de paramètres pour parvenir au verdict correct :

- Entropie
- Nombre total de caractères
- Nombre de mots clés spéciaux
- Nombre de lignes, lignes d'affectation spéciales
- Etc.

Cette stratégie permet d'enregistrer un taux de détection identique et très efficace, comme décrit plus haut.

Une formation de sensibilisation à la cybersécurité à l'intention des utilisateurs est un atout

Certes, l'intégration de ce type de modèle de détection dans une bonne solution de cyberprotection est une mesure essentielle. Il n'en reste pas moins que le niveau de sécurité global tant des individus que de l'entreprise en général peut être significativement renforcé si les utilisateurs sont conscients des menaces et de l'importance de leur comportement, et s'ils adoptent les réactions adéquates. En effet, dans la plupart des cas, un document ou script malveillant nécessite une interaction avec un utilisateur pour produire ses effets. Sans interaction, la menace est inopérante.

Une sensibilisation à la sécurité exige de respecter des règles de sécurité de base bien connues :

- Vérifiez toujours l'origine d'un e-mail ou d'un lien. Connaissez-vous l'expéditeur ? Vous attendiez-vous à recevoir ce fichier ? Contrôlez l'adresse qui a effectivement envoyé le message, pas seulement le nom et l'alias.
- Si vous avez déjà cliqué sur le fichier, et qu'un message annonce un problème de compatibilité quelconque, vous demande d'activer quoi que ce soit, affiche des liens ou un faux CAPTCHA, ou toute autre communication du même type, ce fichier doit être immédiatement fermé et supprimé, et vous devez prévenir l'équipe de sécurité sans tarder.
- Si vous avez cliqué sur le fichier, mais que rien ne s'ouvre, c'est également mauvais signe. Si le fichier qui s'ouvre n'est pas ce à quoi vous vous attendiez, vous êtes peut-être déjà tombé dans le piège du cybercriminel et devez tout de suite informer une équipe de sécurité.

En résumé, la première règle à respecter est de ne pas ouvrir les pièces jointes et de ne pas cliquer immédiatement sur les liens. Vérifiez tout, et si vous avez le moindre doute, adressez-les à une équipe sécurité. Restez vigilant et prudent.