Cybercriminalité : comment tirer parti de l'IA

La dernière tendance dans cette course actuelle aux cyberarmes est l'utilisation de l'automatisation, de l'apprentissage automatique (Machine Learning) et, en fin de compte, de l'intelligence artificielle (IA).

Ce n'est pas que de la science-fiction. Un rapport récent de Nokia, par exemple, a montré que les botnets alimentés par l'intelligence artificielle sont utilisés pour trouver des vulnérabilités spécifiques dans les appareils Android et ensuite exploiter ces vulnérabilités en chargeant des logiciels malveillants de vol de données qui sont généralement détectés seulement après que le dommage soit réalisé.

Le défi de la transformation numérique pour les entreprises

La transformation numérique (DX) a réussi à bouleverser complètement des années de stratégie de sécurité pour les professionnels de la cybersécurité. Or aujourd'hui, en raison de l'élargissement du déficit de compétences en matière de cybersécurité, les organisations ne peuvent pas se permettre d'étendre leur infrastructure de sécurité pour faire face à la surface croissante de leurs attaques.

Pour relever ce défi, il faut confier les décisions d'ordre inférieur et les processus fastidieux à des systèmes automatisés qui exigent moins d'yeux et de mains. En parallèle, les dispositifs de sécurité en place, traditionnellement isolés, doivent non seulement être remplacés par des systèmes intégrés qui étendent la visibilité et le contrôle dans tous les environnements réseau, mais ils doivent également inclure des éléments tels que le Machine Learning et l'IA pour combler les lacunes, corréler les renseignements sur les menaces et coordonner les réponses à des vitesses numériques.

L'opportunité de la transformation numérique pour les cybercriminels

La transformation numérique a été l'une des plus grandes aubaines pour la communauté cybercriminelle en multipliant la surface d'attaque potentielle de manière exponentielle. L'intelligence artificielle et le Machine Learning sont tout aussi utiles ici qu'ils le sont pour les réseaux d'entreprise.

Comme pour leurs victimes, le maintien du retour sur investissement d'une entreprise cybercriminelle passe par une diminution du nombre de personnes entendues tout en augmentant

l'efficacité et l'efficience des outils conçus pour pénétrer les systèmes de défense.

Par exemple, les logiciels malveillants (Malwares) intégrés qui peuvent fonctionner sur une différents périphériques et environnements, et fournir une variété d'exploits et de charges utiles peuvent être très efficaces.

Cependant, en tirant parti de l'automatisation et du machine learning, ces malwares peuvent déterminer de manière autonome quelles charges utiles (payloads) seront les plus efficaces sans s'exposer par des communications constantes avec son serveur C2. Il en résulte des tentatives de vol de données plus efficaces sans augmenter les frais généraux.

L'IA passe à la vitesse supérieure

Les attaques qui exploitent les technologies d'auto-apprentissage peuvent rapidement évaluer les vulnérabilités, sélectionner ou adapter les logiciels malveillants (malwares) et contrer activement les efforts de sécurité pour les arrêter.

La combinaison de l'IA avec des menaces émergentes comme les swarmbots permettra de décomposer une attaque en ses éléments fonctionnels, de les assigner à différents membres d'un essaim et d'utiliser des communications interactives à travers l'essaim pour accélérer la vitesse à laquelle une attaque peut survenir.

La seule défense efficace contre de telles stratégies d'attaques renforcées par l'IA sont les solutions qui utilisent ces mêmes stratégies. L'intelligence artificielle permettra aux entreprises de déployer une solution de sécurité capable de détecter les menaces, de combler les lacunes, de reconfigurer les dispositifs et de réagir aux menaces sans intervention humaine.

Parce que tant de fournisseurs voient les revenus potentiels associés à l'intelligence artificielle, beaucoup sont prêts à annoncer des fonctionnalités d'intelligence artificielle là où elles n'existent pas réellement, ce qui peut laisser les entreprises qui cherchent à « combattre le feu par le feu » dans un dilemme quant aux solutions qu'elles doivent choisir.

Pour dissiper cette confusion, les équipes informatiques doivent poser quelques questions en amont aux fournisseurs afin de déterminer si leur solution d'IA vaut la peine d'être envisagée :

 Combien d'années avez-vous passé à développer cette IA ? L'IA exige des années d'entraînement minutieux. Tout fournisseur qui n'a pas utilisé de formation basée sur des normes au cours des années pour former son système d'IA offre une solution loin d'être idéale.

 Combien de nœuds sont utilisés pour traiter les données et prendre des décisions ? D'une manière générale, la véritable IA nécessite des millions de nœuds combinés à des quantités massives de données pour générer des solutions de défense précises.

 Quelle est la qualité des données que vous fournissez à votre IA ? Nourrir une IA avec de bonnes données est plus difficile qu'il n'y paraît. Des ensembles de données massifs de données fiables et constamment disponibles sont absolument nécessaires pour une IA efficace.

Les moteurs d'une prise de décision basés sur les risques qui sont suffisamment intelligents pour sortir les humains de la boucle doivent non seulement être capables d'exécuter la « boucle OODA » (Observer, Orienter, Décider et Agir) pour la grande majorité des situations qu'ils rencontrent, mais aussi suggérer des pistes d'action lorsqu'un problème est découvert au lieu de se baser simplement sur des situations prédéfinies.

Trouver les outils qui peuvent répondre à cette norme exige du temps et une analyse minutieuse. Ce n'est qu'à ce moment-là que l'entreprise, en toute confiance, pourra abandonner les processus de sécurité critiques afin que ses précieux experts en cybersécurité puissent se concentrer sur les décisions difficiles où la cognition et l'intervention humaines sont les plus nécessaires.