Le machine learning, nouvelle porte d'entrée pour les attaquants d'objets connectés

Émilie Bout, Valeria Loscri

Le machine learning, nouvelle porte d'entrée pour les attaquants d'objets connectés

theconversation.com/le-machine-learning-nouvelle-porte-dentree-pour-les-attaquants-dobjets-connectes-160427

Émilie Bout, Valeria Loscri

Au cours des dernières années, les appareils connectés IoT (Internet des objets) ont continué de croître de manière exponentielle dans des domaines variés. D'après le rapport annuel de Cisco, le nombre de connexions de ces dispositifs devrait représenter 50 % des 14,7 milliards de connexions prévues en 2023.

Présents dans de nombreux domaines tels que la médecine avec les pompes insulines connectées, l'industrie ou encore le transport avec les voitures connectées, ces dispositifs sont peu à peu devenus une véritable aire de jeu pour les cyberattaquants.

À mesure que ces appareils évoluent, ils embarquent par ailleurs avec eux de nouvelles technologies, et intègrent notamment des algorithmes de *machine learning*. Une avancée qui résout certains problèmes mais ouvre aussi de nouvelles perspectives pour les attaquants.

L'IoT dopé par le *machine learning*

Avec l'avancée de la technologie, les appareils IoT sont désormais bien plus que de simples capteurs aptes à récupérer des données. Une nouvelle aire combinant l'IoT et le *machine learning* commence à donner le jour à des dispositifs de plus en plus intelligents, capables de répondre à des besoins spécifiques pour chaque utilisateur.

Le business des objets connectés | Internet de tout et n'importe quoi (½) (Arte, 19 mai 2020).

C'est par exemple le cas de l'Amazon echo, qui intègre avec elle des composants supportant le *machine learning* et répond à des requêtes telles qu'allumer une lumière ou jouer une musique. Les voitures autonomes en sont une autre illustration : partant des données récoltées en temps réel, elles arrivent à analyser le trafic et à adapter leur comportement.

Le *machine learning* répond aussi à de nombreux problèmes liés aux appareils en eux-mêmes, en optimisant par exemple leur consommation énergétique ou en adaptant leur connectivité.

Des algorithmes de machines learning peuvent ainsi être utilisés dans les téléphones intelligents afin d'économiser leur énergie. En récupérant des données comme la fréquence et la durée d'utilisation d'une application, il est alors possible de déduire des informations et d'adapter certains éléments en fonction, tels que la luminosité, et ainsi réduire la consommation énergétique de l'appareil.

Machine learning et cybersécurité

Le développement de solutions de *machine learning* dédiées à la détection d'attaques peut par ailleurs améliorer la sécurité de l'IoT.

Les algorithmes d'apprentissage automatique constituent en effet de véritables assistants dans différents domaines de la sécurité.

Ils servent par exemple à repérer des menaces sur un réseau en surveillant en continu le comportement de ce dernier, permettant de traiter une quantité de données en temps quasi réel. Ils représentent également un soutien essentiel pour les utilisateurs en déduisant et informant les utilisateurs des « mauvais comportements » d'un site web ou d'un mail.

Enfin, ils sont aussi capables de nous permettre de protéger nos données stockées en ligne, par l'analyse des activités de connexion suspectes aux applications Cloud, en se fondant sur les anomalies de localisation ou d'adresse IP.

Dans le cas de l'IoT, l'effet est néanmoins contrebalancé par la complexité et la variété croissantes des appareils connectés présents sur le marché, qui laissent encore place, au sein des algorithmes de *machine learning*, à de nombreux vecteurs d'attaques qu'Europol appréhende comme une menace réelle et importante.

Concevoir un algorithme de *machine learning*

Avant de comprendre comment les attaquants s'y prennent pour déjouer un algorithme de *machine learning*, il est essentiel d'appréhender le fonctionnement de ce dernier.

> Intelligence artificielle : les défis de l'apprentissage profond https://t.co/9sBL2eTLjs pic.twitter.com/w5galCOeh1
>
> — The Conversation France (@FR_Conversation) April 23, 2019

Dans la plupart des cas, la création se fait en plusieurs phases. La première consiste à entraîner un modèle de *machine learning* à partir de données prétraitées en amont. Vient ensuite la phase d'utilisation, qui ne commence réellement que lorsque le modèle est fiable. Celui-ci est alors utilisé avec de nouvelles données, dont la provenance dépend du problème à résoudre. Dans le cas d'Amazon Echo, par exemple, il s'agit des instructions fournies par l'utilisateur.

Cet éclaircissement fait, penchons-nous sur les trois principales types d'attaques visant le *machine learning* et applicables sur nos objets de l'IoT.

Attaque, mode d'emploi

La première est nommée « l'empoisonnement » : elle a pour but de modifier le comportement de base de l'algorithme. L'attaquant cherche alors à altérer les données utilisées lors de la phase d'apprentissage.

Une autre attaque particulièrement répandue est « l'évasion » : il s'agit ici de jouer sur les données d'entrée du *machine learning* afin d'obtenir une décision différente de celle normalement attendue par l'application. Le but est d'introduire une donnée légèrement modifiée afin d'obtenir une décision différente tout en restant indétectable. L'attaquant tâche de créer l'équivalent d'une illusion d'optique pour l'algorithme.

> Plusieurs organismes ont été sujettes à des demandes de rançon par kidnapping de données. Comment les assaillants procèdent-ils et comment s'en prémunir ?
> https://t.co/jOYVluBBMz
>
> — The Conversation France (@FR_Conversation) February 22, 2021

Les voitures autonomes constituent une cible de choix pour ce type d'attaques. Censées reconnaître, entre autres, les panneaux de signalisation routière, elles peuvent être trompées si une modification en apparence anodine pour l'homme est introduite. Une étude a ainsi montré que le simple ajout d'un autocollant sur un panneau « STOP » pouvait mettre l'algorithme en échec, approuvant alors à 97 % qu'il s'agissait d'un panneau de limitation de vitesse.

Enfin, il existe l'attaque par « inférence », le but ici étant de déduire le type d'algorithme utilisé, ainsi que les données. Un attaquant teste alors successivement différentes requêtes sur l'application et étudie l'évolution de son comportement afin de le déduire – il s'agit dans ce cas d'un vol de données.

Cette dernière attaque apparaît particulièrement efficace pour déterminer le comportement d'un système de détection fondé sur du *machine learning* dans les réseaux IoT.

L'attaque, toujours la meilleure des défenses

Face à leur augmentation constante et inexorable, la clé reste de découvrir et d'étudier en amont les différentes attaques possibles. Les entreprises, la recherche et l'innovation sont ainsi forcées d'anticiper les actions et d'utiliser les mêmes outils et les mêmes techniques que les attaquants afin d'évaluer la sécurité de leurs systèmes IoT ou d'y trouver de nouvelles vulnérabilités.

Se mettre à la place du hacker permet aussi de mieux comprendre le fonctionnement des appareils IoT, en les détournant de leur fonctionnalité première. L'un des objectifs est d'identifier les zones à risques les plus visibles afin de pouvoir créer des solutions le plus rapidement possible.

D'ailleurs, créer des attaques en laboratoire ne sert pas uniquement à prouver qu'elles sont réalisables. Cela donne aussi l'occasion de tester les solutions de sécurité existantes, de les améliorer et d'en concevoir de nouvelles.

Si la sécurisation des réseaux IoT est possible, ceux-ci présentent néanmoins encore d'importantes faiblesses, alors que le secteur est amené à occuper une place de plus en plus importante dans nos vies. À mesure que ces objets se développent, de nouvelles failles apparaissent et avec elles les menaces d'attaques, alertant toujours plus sur la nécessité de développer les recherches dans le domaine.