Quand le Machine Learning se met à créer des malwares furtifs

Au même titre qu'Esope écrivait que la langue était la plus belle et la plus mauvaise des choses, l'intelligence artificielle peut aussi avoir ces deux facettes. A l'occasion de la Defcon, qui se déroule en ce moment à Las Vegas, le côté obscur de l'IA s'est dévoilé. La société de sécurité Endgame a révélé comment les outils d'apprentissage automatique peuvent servir à créer des malwares indétectables.

La démonstration a été réalisée par le directeur technique de la société, Hyrum Anderson, en s'appuyant sur le framework OpenAI, promu par Elon Musk. Concrètement, le spécialiste a d'abord créé, à partir de ce framework, un système d'entraînement pour éprouver les antivirus et détecter les malwares. Hyrum Anderson constate dans son analyse que « *l'ensemble des outils de Machine Learning ont une face cachée. En fonction des connaissances d'un pirate, ces tâches peuvent être exploitées* ».

Mettre en compétition les IA pour dévoiler les tâches cachées

Et c'est cette face sombre que l'équipe d'Endgame a réussi à utiliser en configurant un agent à base d'IA capable de concurrencer le détecteur de malware et de détecter les tâches cachées. Utilisant la méthode d'apprentissage par renforcement, l'agent a peaufiné des malwares dont le code a été modifié pour éviter leur détection par les antivirus. « *Dans un premier temps, nous nous sommes concentrés sur des malwares ciblant Windows, mais la méthode peut être généralisée à d'autres systèmes* », explique Hyrum Anderson.

Dans le cadre de leur POC, les chercheurs d'Endgame ont fait fonctionner l'agent pendant une quinzaine d'heures lui permettant d'obtenir 100 000 échantillons de code potentiellement indétectables par les antivirus. Pour parvenir, au final, à un taux de 60% de malwares créés capables de berner les systèmes de sécurité.

Hyrum Anderson se veut rassurant en expliquant que cette méthode est théorique. Et veut surtout mettre en exergue le manque de connaissances sur les moteurs de détection des antivirus et sur les modèles d'intelligence artificielle utilisés. Le dirigeant a précisé que l'agent capable de générer des malwares était disponible sur GitHub pour la communauté Open Source. Nul doute que les éditeurs de solutions de sécurité vont analyser avec soin cet agent.

A lire aussi :

Kaspersky veut concurrencer Windows Defender avec un antivirus gratuit

Microsoft admet désactiver les antivirus tiers, jugés incompatibles

Photo credit : Merrill College of Journalism Press Releases via Visual Hunt / CC BY-NC