POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

Équipe 13

L'IA, le Dark Web et les Défis en Cybersécurité

- Saoussene Chaffai, 1959524
- Ilias Bettayeb, 2092408
- Heimanu Tepu, 2007764

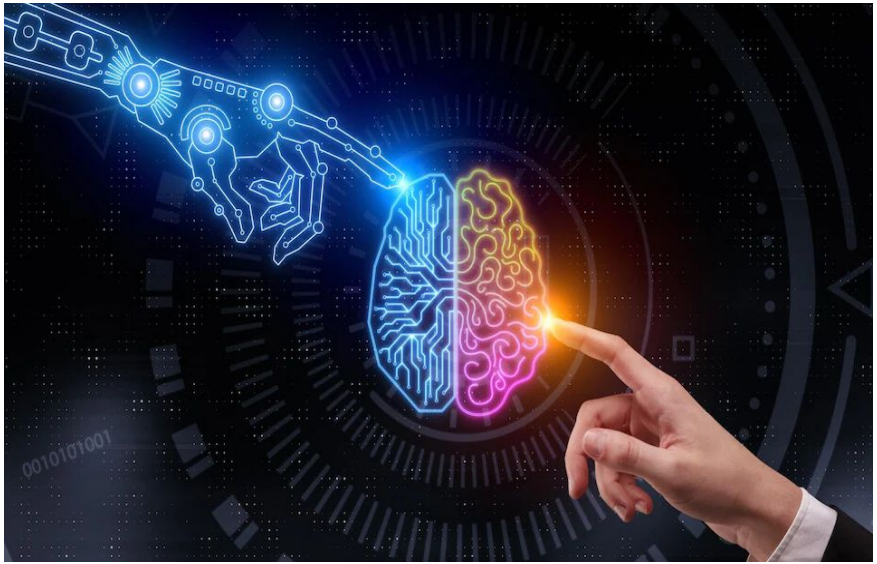
INF8108

2023-10-25

Introduction

Répondre à deux questions abordant les sujets suivants :

- L’apprentissage automatique adversaire
- L’IA et logiciels malveillants
- Les défis en cybersécurité



Plan

- Question 25
- Question 26

Question 25

Explorez le concept d'apprentissage automatique adversaire (adversarial machine learning) dans le contexte du Dark Web. Comment les acteurs malveillants peuvent-ils manipuler les systèmes d’IA pour échapper à la détection et améliorer leur anonymat ?

Réponse à la question 25

L’utilisation de l’Intelligence Artificielle permet de :

1. Contournement des systèmes de détection
2. Amélioration de l’anonymat
3. Contrefaçon de l’identité
4. Développement de Deep Fake
5. Augmente l’efficacité des mails d'hameçonnage et le “password guessing”
6. Possible d’utiliser IA pour développer des logiciels malveillants qui changent continuellement

Question 26

Pensez à l'utilisation potentielle de l'IA pour générer des logiciels malveillants sophistiqués et orchestrer des cyberattaques sur le Dark Web. En quoi les attaques basées sur l'IA peuvent-elles différer des méthodes traditionnelles, et quels défis cela pose-t-il aux professionnels de la cybersécurité ?

Réponse à la question 26

Les principales différences entre des attaques basées avec AI et des attaques traditionnelles:

- Découvrir des vulnérabilités devient autonome
- les IA peuvent traiter d'énormes volumes de données
- il y aura une adaptation plus rapide des attaquants grâce à l'AI
- Certaines attaques trop complexes pourront être exécuter à moindre coûts (coûts en temps)

Les défis pour les professionnels sont:

- Les méthodes de détection de vulnérabilité ne seront possiblement plus viable
- Gérer un plus grand nombre d'attaque
- s'adapter constamment aux nouvelles vulnérabilité trouver par l'AI
- Si le critère d'analyse d'une attaque est sa complexité il faudrait revoir la priorisation de certains actifs de l'entreprise à être protégés

Réponse à la question 26 (suite)

Quelques utilisations de l'AI possible par des professionnels de la cybersécurité:

- L'entraînement des AI pour détecter les malwares pour qu'il reconnaisse même les plus petits détails qui pourraient être une threat.
- Le monitoring et l'audit des systèmes peut être fait grâce à une AI entraîner pour détecter des comportements douteux.
- l'utilisation des AI pour une simulation d'attaque.

Merci!

Ressources

- Artificial Intelligence: Adversarial Machine Learning. https://www.nccoe.nist.gov/ai/adversarial-machine-learning
- Artificial Intelligence: Used for Attacks. https://www.csoonline.com/article/564321/6-ways-hackers-will-use-machine-learning-to-launch-attacks.html
- Artificial Intelligence: Playing a Bigger Role in Cybersecurity. https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html
- Artificial intelligence: Improve Scalability. https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/#:~:text=AI%20algorithms%20can%20process%20massive,%2C%20and%20zero-day%20vulnerabilities
- Artificielle intelligence: Detecting and Preventing Cybercrime. https://www.linkedin.com/pulse/use-ai-detecting-preventing-cybercrime-neil-sahota-%E8%90%A8%E5%86%A0%E5%86%9B-/