Surveillance des attaques : ChatGPT, malvertising et supply chain en tant que vecteurs potentiels

Titre HTML : Les cinq techniques d’attaque les plus dangereuses selon l’Institut SANS

L’Institut SANS, une société qui offre des solutions de formation, certification et ressources en matière de cybersécurité, a présenté lors d’une session à la conférence RSA à San Francisco les cinq techniques d’attaque les plus dangereuses actuellement utilisées par les acteurs de la menace. Dans cet article, nous allons examiner chacune de ces techniques et les moyens de s’en prémunir.

Les IA adverses

Les acteurs de la menace se servent de l’Intelligence Artificielle (IA) pour augmenter la vitesse des campagnes de ransomware et identifier les vulnérabilités zero day. Pour répondre à cette menace, les entreprises doivent déployer un modèle de sécurité intégré de défense en profondeur qui automatise les actions critiques de détection et de réponse, et facilite les processus efficaces de traitement des incidents.

L’ingénierie sociale à la sauce GPT

L’ingénierie sociale alimentée par ChatGPT utilise l’IA générative pour exploiter les vulnérabilités humaines. Les utilisateurs sont aujourd’hui plus facilement attaquables que jamais, et un mauvais clic sur un fichier malveillant peut

mettre en danger non seulement une entreprise entière, mais aussi les moyens de subsistance des victimes. Les entreprises doivent encourager une culture de cyber-vigilance à tous les niveaux de l'entreprise.

Les attaques par supply chain

Les attaques qui passent par la chaîne d'approvisionnement des logiciels sont une technique sérieuse à prendre en compte. Les entreprises doivent travailler efficacement en tandem avec les développeurs de logiciels pour aligner les architectures de sécurité, partager les informations sur les menaces et naviguer dans les techniques d'attaque en constante évolution.

Le malvertising

Les attaques par référencement sont une autre méthode d'attaque dangereuse et émergente. Les cybercriminels exploitent des mots-clés SEO et des publicités payantes pour inciter les victimes à s'engager sur des sites Web falsifiés, à télécharger des fichiers malveillants et à autoriser l'accès d'utilisateurs à distance. Les entreprises doivent intégrer des programmes de formation de sensibilisation des utilisateurs évolutifs et adaptés aux nouvelles menaces.

Varier et diversifier les attaques pour mieux surprendre

Les attaques abordées dans cet article sont devenues de plus en plus fréquentes, sophistiquées et difficiles à détecter. Les pirates informatiques diversifient les techniques d'attaque afin de surprendre les entreprises. Les entreprises doivent rester à l'avant-garde et modifier sans cesse leur approche, quelle que soit la menace.

En conclusion, les entreprises doivent être très vigilantes sur plusieurs méthodes d'attaque émergentes et dangereuses. Elles doivent déployer un modèle de sécurité intégré de défense en profondeur qui automatise les actions critiques de détection et de réponse, et facilite les processus efficaces

de traitement des incidents. Il est vital que les entreprises encouragent une culture de cyber-vigilance à tous les niveaux de l’entreprise et modifient sans cesse leur approche, quelle que soit la menace.

Source : www.lemondeinformatique.fr

→ Accéder à CHAT GPT en cliquant dessus