Les pirates utiliseront-ils davantage l'IA dans les attaques par rançongiciel en 2025 ?

Réponse courte : Oui. Les attaquants devraient continuer à élargir leur utilisation de l'intelligence artificielle, en particulier des grands modèles de langage, pour usurper l'identité de personnes de confiance et manipuler les victimes afin qu'elles accordent un accès ou leur confiance.

Pourquoi l'IA est devenue une favorite des pirates

Les résultats de recherche, les fils d'actualités et les conversations quotidiennes sont désormais saturés de références à l'IA, et cet engouement s'est également emparé des cybercriminels. Lorsque la plupart des gens mentionnent l'IA, ils font généralement référence à des grands modèles de langage comme ceux qui alimentent ChatGPT et des outils similaires capables d'imiter de manière convaincante la communication humaine. Les attaquants ont reconnu que cette capacité est extrêmement utile pour l'ingénierie sociale. Plutôt que de s'appuyer sur des e-mails de phishing génériques, ils peuvent générer des messages, des voix ou des conversations qui ressemblent étroitement à un vrai collègue, fournisseur ou figure d'autorité, ce qui rend beaucoup plus facile de gagner la confiance d'une cible avant de frapper.

Attendez-vous à des tactiques d'usurpation d'identité plus raffinées

La tendance à l'approche de 2025 n'est pas que les attaques pilotées par l'IA soient totalement nouvelles, mais qu'elles deviennent plus soignées et professionnelles. De la même manière que les entreprises légitimes déploient des agents de vente pilotés par l'IA et des outils de prospection automatisés, les attaquants affinent leurs propres techniques d'usurpation d'identité basées sur l'IA. Cela signifie des messages plus convaincants imitant des patrons, des collègues ou des partenaires de confiance, tous conçus pour exploiter les relations de travail dont dépendent les gens au quotidien. Le danger est qu'une conversation qui semble personnelle et légitime puisse en réalité provenir d'un système d'IA hautement performant conçu pour manipuler, et non pour aider.

Ce que cela signifie pour la défense

À mesure que ces tactiques d'usurpation d'identité se perfectionnent, les organisations doivent partir du principe que les attaques basées sur la confiance deviendront plus difficiles à repérer par instinct seul. Vérifier les demandes par des canaux indépendants, plutôt que de faire confiance à un message ou à un appel sur la seule apparence, devient de plus en plus important. Étant donné que ces attaques sont conçues pour contourner le jugement humain, disposer de capacités de détection et de réponse automatisées, telles que celles intégrées dans FortressAI de Cyber Crucible, offre une couche de protection supplémentaire lorsque l'ingénierie sociale parvient à déjouer les défenses d'une personne.

https://player.vimeo.com/video/1046827321

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #1
Created 2026-07-24 07:28:26 UTC by Dennis Underwood
Updated 2026-07-24 07:28:26 UTC by Dennis Underwood