Les cybercriminels surfent sur la vague de l'IA
Internet
PostÃ© par : JerryG
PubliÃ©e le : 15/1/2024 13:00:00

Netskope, un leader sur le marchÃ© du SASE (Secure Access Service Edge), publie une nouvelle Ã©tude selon laquelle plus de 10â□□% des employÃ©s utilisent au moins une application dâ□□intelligence artificielle (IA) gÃ©nÃ©rative chaque mois, contre seulement 2â□□% un an plus tÃ´t.

AnnoncÃ©s dans le cadre de lâ□□Ã©tude annuelle Cloud and Threat Report de Netskope, ces rÃ©sultats soulignent la croissance rapide de lâ□□adoption des applications dâ□□IA gÃ©nÃ©rative au sein des organisations, ainsi que lâ□□Ã©mergence de nouveaux risques pour la cybersÃ©curitÃ©.

Lâ□□Ã©tude annuelle Cloud and Threat Report de Netskope fait le point sur les principales tendances qui ont marquÃ© lâ□□annÃ©e 2023 sur le plan de la cybersÃ©curitÃ© du cloud, et anticipe la faÃ§on dont lâ□□adoption du cloud, et la surface dâ□□attaque qui en dÃ©coulera, continueront dâ□□Ã©voluer en 2024.

2023 : lâ□□annÃ©e de lâ□□IA gÃ©nÃ©rative

Selon lâ□□Ã©tude de Netskope, plus de 10â□□% de lâ□□ensemble des utilisateurs en entreprise accÃ¨dent Ã au moins une application dâ□□IA gÃ©nÃ©rative par mois, contre seulement 2â□□% un an plus tÃ´t. En 2023, ChatGPT sâ□□est imposÃ©e comme lâ□□application dâ□□IA gÃ©nÃ©rative la plus populaire du marchÃ©, reprÃ©sentant 7â□□% des utilisations dâ□□IA gÃ©nÃ©rative en entreprise.

Tandis que Netskope prÃ©voit une hausse continue et modÃ©rÃ©e du nombre total de collaborateurs qui accÃ¨deront Ã des applications dâ□□IA au cours de lâ□□annÃ©e 2024, il apparaÃ®t quâ□□un groupe Ã©mergent dâ□□utilisateurs chevronnÃ©s a recours de faÃ§on croissante Ã ces applications.

ParallÃ¨lement Ã lâ□□augmentation exponentielle de cette utilisation, les 25â□□% dâ□□utilisateurs qui reprÃ©sentent les plus importants consommateurs dâ□□IA gÃ©nÃ©rative devraient accroÃ®tre de faÃ§on significative leur activitÃ© en 2024, imaginant de nouvelles faÃ§ons dâ□□intÃ©grer la technologie Ã leur activitÃ© quotidienne.

Â«â□□Compte tenu de lâ□□utilisation croissante des applications dâ□□IA, les employÃ©s sont davantage susceptibles dâ□□exposer des donnÃ©es sensibles, quâ□□il sâ□□agisse dâ□□identifiants, dâ□□informations personnelles ou de propriÃ©tÃ© intellectuelle, observe Ray Canzanese, Threat Research Director, Netskope Threat Labs. Pour que les applications dâ□□IA soient utilisÃ©es en toute sÃ©curitÃ©, les entreprises doivent mettre en Å□uvre des moyens de contrÃ´le raisonnables, ainsi que des outils avancÃ©s de sÃ©curitÃ© des donnÃ©es, tout en se concentrant sur la faÃ§on dont leurs employÃ©s peuvent utiliser lâ□□IA de maniÃ¨re productive.â□□Â»

Hausse de lâ□□utilisation des applications Cloud
Â
De maniÃ¨re gÃ©nÃ©rale, lâ□□adoption des applications cloud a continuÃ© dâ□□augmenter tout au long de lâ□□annÃ©e Ã©coulÃ©e, les collaborateurs essayant rÃ©guliÃ¨rement de nouvelles applications, tout en augmentant leur utilisation de celles les plus prisÃ©es.

Principaux enseignements de cette Ã©tudeâ□□

â□¢ Le nombre dâ□□applications Cloud auxquelles les collaborateurs ont accÃ©dÃ© a progressÃ© en moyenne de 19â□□% par an, passant de 14 Ã 20 applications diffÃ©rentes en lâ□□espace de seulement deux ans ;

â□¢ La moitiÃ© des utilisateurs en entreprise interagit chaque mois avec entre 11 Ã 33 applications cloud, les 1 % les plus performants utilisant plus de 96 applications par mois. Lâ□□utilisation de ces applications cloud augmente Ã un rythme encore plus soutenu, passant dâ□□un peu plus de 1 000 interactions par mois il y a deux ans Ã prÃ¨s de 2 000 aujourdâ□□hui ;

â□¢ La plupart des collaborateurs gÃ©nÃ¨rent entre 600 et 5 000 interactions par mois, tandis que les 1 % d'utilisateurs les plus expÃ©rimentÃ©s gÃ©nÃ¨rent plus de 50 000 activitÃ©s par mois.

Les attaques par ingÃ©nierie sociale en premiÃ¨re ligne

En 2023, lâ□□ingÃ©nierie sociale sâ□□est imposÃ©e comme la mÃ©thode la plus couramment utilisÃ©e par les cyberattaquants pour obtenir un accÃ¨s initial ; câ□□est en effet le moyen le plus simple de se frayer un chemin au cÅ□ur de systÃ¨mes dont les failles de sÃ©curitÃ© connues sont rapidement corrigÃ©es et qui limitent lâ□□accÃ¨s Ã distance.

Au cours de lâ□□annÃ©e Ã©coulÃ©e, les techniques les plus rÃ©pandues se sont appuyÃ©es sur des mÃ©thodes telles que le phishing pour subtiliser des identifiants, et les chevaux de Troie pour inciter les victimes Ã tÃ©lÃ©charger et Ã installer des malwares.

Les utilisateurs sont tombÃ©s dans le piÃ¨ge du phishing trois fois plus souvent quâ□□ils ont tÃ©lÃ©chargÃ© des chevaux de Troie, 29 collaborateurs en entreprise sur 10â□□000 en moyenne ayant cliquÃ© sur un lien dâ□□hameÃ§onnage une fois par mois en 2023.

Les applications cloud et les sites dâ□□achat en ligne ont figurÃ© parmi les principales cibles dâ□□un bout Ã lâ□□autre de lâ□□annÃ©e, tandis que les portails bancaires, les rÃ©seaux sociaux et les cibles gouvernementales enregistraient eux aussi une augmentation sensible.

Les cheveux de Troie sont le deuxiÃ¨me vecteur dâ□□attaque le plus courant, les utilisateurs en ayant tÃ©lÃ©chargÃ©s en moyenne 11 par mois pour 10â□□000 utilisateurs. En dâ□□autres termes, dans une entreprise qui emploie 10 000 personnes, 132â□□chevaux de Troie ont en moyenne Ã©tÃ© tÃ©lÃ©chargÃ©s au cours de lâ□□annÃ©e.

Acteurs de la menace et activitÃ©s malveillantes

En 2023, la majoritÃ© des activitÃ©s malveillantes visant des clients de Netskope ont Ã©tÃ© motivÃ©es par la criminalitÃ©, les cyberattaquants gÃ©opolitiques les plus actifs intervenant en Asie et en AmÃ©rique latine. Netskope a constatÃ© quâ□□en 2023, les principaux groupes de cybercriminels Ã©taient basÃ©s en Russie, tandis que les auteurs de menaces gÃ©opolitiques opÃ©raient Ã partir de la Chine, ciblant essentiellement des victimes situÃ©es en Asie, et tout particuliÃ¨rement Ã Singapour.

De nombreux groupes se sont largement appuyÃ©s sur le logiciel Cobalt Strike pour maintenir leur prÃ©sence et dÃ©ployer des applications malveillantes (ransomwares, infostealers, wipers et autres malwares) en vue dâ□□extorquer leurs victimes. Dans son Ã©tude, le Threat Labs de Netskope prÃ©sente le profil des cinq principaux adversaires observÃ©s au cours de lâ□□annÃ©e Ã©coulÃ©e, ainsi que les campagnes et activitÃ©s observÃ©es pour chaque groupe.

Â«â□□En 2023, nombre de cyberadversaires ont tirÃ© parti de lâ□□adoption croissante des applications cloud dans les environnements dâ□□entreprise, notamment par le biais dâ□□astuces

liÃ©es Ã lâ□□ingÃ©nierie sociale. Cette tendance devrait se poursuivre en 2024â□□Â», ajoute Ray Canzanese.

Principaux enseignements pour les entreprises

Netskope recommande aux entreprises de prendre les mesures suivantes afin de lutter efficacement contre ces tendances :

â□¢ Limiter exclusivement lâ□□accÃ¨s aux applications qui rÃ©pondent Ã un objectif professionnel lÃ©gitime ; crÃ©er un processus dâ□□analyse et dâ□□approbation pour les nouvelles applications ; et mettre en Å□uvre un processus de surveillance continue qui informera les opÃ©rateurs de sÃ©curitÃ© quâ□□une application est utilisÃ©e Ã des fins malveillantes ou a Ã©tÃ© compromise ;

â□¢ Le dÃ©ploiement et lâ□□adoption dâ□□applications dâ□□IA en toute sÃ©curitÃ© doivent constituer une prioritÃ© majeure pour la plupart des entreprises, notamment en identifiant les applications autorisÃ©es et en mettant en Å□uvre des contrÃ´les permettant aux collaborateurs de les utiliser au maximum de leurs possibilitÃ©s, tout en protÃ©geant lâ□□entreprise contre les risques ;

â□¢ Les entreprises doivent continuer dâ□□investir en vue de rÃ©duire les risques dâ□□ingÃ©nierie sociale, notamment par le biais de formations Ã la cyber-sensibilisation et aux technologies anti-phishing.

Pour ***tÃ©lÃ©chargez*** lâ□□intÃ©gralitÃ© de lâ□□Ã©tude Cloud and Threat: 2024.