CybersÃ©curitÃ© : les tendances qui marqueront 2023.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 2/12/2022 13:00:00

A lâissue de cette annÃ©e 2022 riche pour le secteur de la cybersÃ©curitÃ©, les experts du Threat Labs de Netskope partagent leur vision sur les grandes tendances Ã suivre en 2023 en matiÃ¨re de supply chain, de phishing et de ransomwares.

Les opÃ©rations de phishing vont devenir de plus en plus sophistiquÃ©es pour contourner lâauthentification multifactorielle (MFA)

Â« Le phishing est une technique dâingÃ©nierie sociale, ce qui signifie que le cybercriminel doit Ã la fois trouver une victime qui ne soit pas mÃ©fiante, et la convaincre que son approche est lÃ©gitime pour quâelle lui transmette son mot de passe ou lâautorise Ã accÃ©der son compte.

Lâauthentification multifactorielle (MFA) a longuement Ã©tÃ© prÃ©sentÃ©e comme une solution fiable face aux attaques de phishing, mais elle ne fait que forcer les hackers Ã changer de tactique.

Entre les outils de phishing par proxy inverse faciles Ã dÃ©ployer et les techniques dâabus de flux dâautorisation OAuth, qui permettent de contourner la MFA et dâaccÃ©der directement aux applications cloud, il faut sâattendre Ã voir une augmentation de la sophistication des attaques de phishing ciblÃ©es pour la contourner. Â», Ray Canzanese, Director, Threat Research chez Netskope

La sÃ©curitÃ© de la supply chain logicielle sera une prioritÃ© pour les organisations

Â« Ces derniÃ¨res annÃ©es, les attaques contre la supply chain ont connu une forte augmentation. Dans la mesure oÃ¹ nous dÃ©couvrons de plus en plus de vulnÃ©rabilitÃ©s dans le code source des applications, en particulier des logiciels libres, nous nous attendons Ã ce que ce type dâattaque augmente.

Il est donc essentiel que les entreprises renforcent leurs mesures et leurs stratÃ©gies en matiÃ¨re de sÃ©curitÃ© de la supply chain. Â» Clive Fuentebella, ingÃ©nieur Threat Research chez Netskope

Les ransomwares ne vont pas disparaÃ®tre

Â« Les ransomwares sont lâune des cybermenaces les plus rÃ©pandues. Cette situation est exacerbÃ©e par lâintÃ©gration de multiples tactiques dâextorsion, telles que lâexfiltration de donnÃ©es et les attaques DDoS, par les cybercriminels, et cela ne va pas changer de sitÃ´t.

En rÃ©alitÃ©, nous verrons probablement davantage de groupes mener des attaques toujours plus dÃ©vastatrices, avec plus de membres impliquÃ©s. En outre, de nouvelles charges utiles et de nouveaux outils, ainsi que de nouveaux procÃ©dÃ©s, comme la collaboration directe avec des cybercriminels, Ã©mergeront certainement. Â» Dagmawi Mulugeta, ingÃ©nieur senior Threat Research chez Netskope

Lâexposition des donnÃ©es Ã la menace interne va sâaggraver avant de sâamÃ©liorer

Â« Les ajustements que les entreprises ont dÃ» mettre en place en rÃ©ponse Ã la pandÃ©mie et dÃ©sormais le travail Ã distance, requiÃ¨rent Ã©galement que les pratiques de sÃ©curitÃ© Ã©voluent.

Avec des collaborateurs qui se connectent Ã partir de rÃ©seaux distants et utilisent des services cloud, il est plus difficile que jamais dâidentifier de maniÃ¨re proactive les menaces internes. En 2023, nous verrons les organisations rÃ©aliser le peu de contrÃ´le quâelles ont sur leurs propres donnÃ©es. Â» Colin Estep, Principal Engineer chez Netskope

La menace des Ransomware-as-a-Service et des groupes dâextorsion va continuer de sâintensifier

Â« Les cyberattaques impliquant le chiffrement de donnÃ©es et le vol dâinformations confidentielles sont en hausse. Il y a une tendance croissante, qui devrait sâintensifier en 2023 et au sein de laquelle nous avons deux extrÃªmes : dâun cÃ´tÃ© il y a le tristement cÃ©lÃ¨bre Ransomware-as-a-Service, dans le cadre duquel les hackers sâintÃ©ressent Ã la fois au chiffrement et au vol de donnÃ©es sensibles.

Les groupes peuvent mÃªme se montrer trÃ¨s agressifs, tels que LockBit qui a mis en Åuvre le modÃ¨le de triple extorsion. Dâun autre cÃ´tÃ©, nous avons les groupes dâextorsion comme LAPSUS$ et RansomHouse, qui ne pÃ©nÃ¨trent dans les entreprises que pour exfiltrer des donnÃ©es sensibles, sans chiffrer aucun fichier.

Lâannée 2023 verra sÃ»rement une hausse des attaques de groupes RaaS et de groupes dâextorsion, voire mÃªme une intensification du modÃ¨le Extorsion-as-a-Service. Â» Gustavo Palazolo, Staff Threat Research Engineer chez Netskope