Cybersécurité : Un demi-milliard d’e-mails destinés aux entreprises contiennent de potentielles cyberattaques

La 5e étude menée par Hornetsecurity à partir de l’analyse de plus de 55,6 milliards d’e-mails dans le monde met en lumière les risques croissants auxquels les entreprises sont confrontées par ce biais.

Temps de lecture : minute

14 janvier 2025

En 2024, dans le monde, un tiers de tous les e-mails reçus par les entreprises (36,9%) étaient indésirables et parmi eux, 2,3% contenaient un contenu malveillant, soit un total de 427,8 millions d’e-mails. C’est l’une des conclusions de la 5e étude sur les cybermenaces menée par Hornetsecurity, l'un des principaux fournisseurs mondiaux et européens de solutions de sécurité, de conformité, de sauvegarde et de sensibilisation à la sécurité nouvelle génération.

Si ce rapport fait état d’une baisse nette des attaques depuis 2023, les données démontrent que toutes les industries sont attaquées. « *Tout type d'entreprises dans tout type de secteur sont concernées, du fait notamment de la sophistication des attaques et leur démocratisation, qui permettent à des cybercriminels qui n'ont pas forcément des compétences techniques avancées de se saisir d'outils pour contourner l'authentification forte par exemple* » explique Romain Basset, directeur technique et stratégique d’Hornetsecurity.

De nouvelles formes d’attaques

L’étude révèle en effet que si le phishing reste la principale menace pour le courrier électronique, se développent de nouvelles formes d’attaques comme les URL malveillantes (22,7%) avec des pages de connexion factices qui piègent les utilisateurs pour capturer les identifiants en temps réel, rendant l'authentification à deux facteurs inefficace. Les cybercriminels exploitent d’ailleurs beaucoup plus des techniques d'ingénierie sociale.

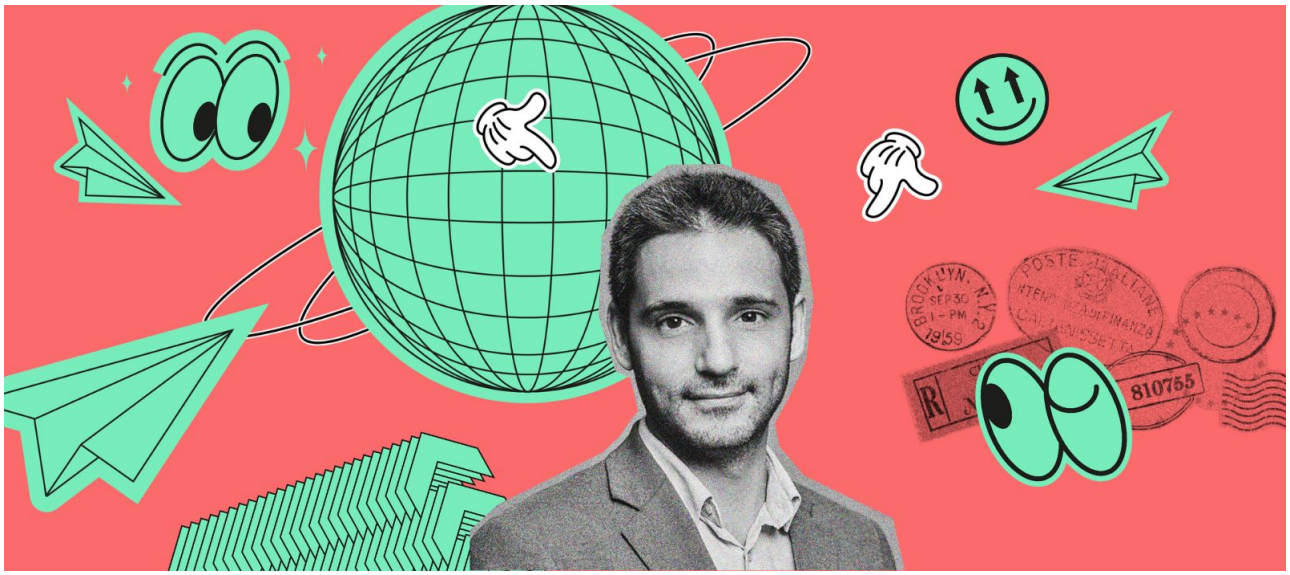
« *Finies ces attaques avec six fautes d'orthographe par phrase, elles vont désormais s'appuyer sur des éléments personnels collectées suite à des fuites de données à exploiter* » poursuit-il. C’est ce qu'on appelle du spear phishing avec des messages fortement personnalisés. « *Une tendance qui émerge actuellement, c'est l'arnaque à la fiche de paye, c’est-à-dire d’usurper l'identité d’un collaborateur pour demander aux RH de verser son salaire sur un autre compte suite à un prétendu changement de banque* » détaille Romain Basset.

Un état d'esprit Zero Trust

Hornetsecurity suit de près les menaces visant les mobiles, comme le smishing, une tentative d’hameçonnage par SMS. « *Une pratique particulièrement active en France, du fait de ses nombreux services publics comme la carte vitale ou la retraite* » souligne-t-il. En parallèle, les transporteurs, à l’image de DHL et de FedEx, sont les marques les plus usurpées en ligne avec une part de 7% du total des imitations de marques.

Selon Romain Basset, « *en 2025, les entreprises doivent adopter un état d'esprit* Zero Trust *et favoriser une forte culture de la sécurité avec une sensibilisation plus fine et adaptée au rôle de chacun* ». Cela passe aussi selon lui par une stratégie sur toute la chaîne de cybersécurité, de la

détection de plus en plus efficace grâce aux avancées de l’intelligence artificielle jusqu’au signalement pour agir quasi immédiatement et bloquer les futures évolutions d'une attaque.



À lire aussi
Cybersécurité : Filigran lève 35 millions pour devenir un acteur incontournable du secteur

Article écrit par Thibault Caudron