MAILINBLACK

Communiqué de presse
Marseille, le 13 décembre 2021

Mailinblack dévoile sa nouvelle fonctionnalité de simulations d'attaques par ransomware

Mailinblack, la pépite française qui rend la cybersécurité accessible à toutes les organisations, intègre des simulations d'attaque par ransomware à Cyber Coach (anciennement Phishing Coach), son outil de sensibilisation et de formation aux cyberattaques. Il est désormais possible d'envoyer des campagnes d'emailing par ransomware personnalisées aux collaborateurs pour mieux connaître et identifier les comportements à risque face aux attaques. Les collaborateurs qui tombent dans le piège sont dirigés vers une page de sensibilisation ciblée selon le sujet choisi (facture impayée, règlement RGPD, paiement encaissé, livraison, etc.).

Les signalements d'attaques par ransomware ont augmenté de 255% entre 2019 et 2020 d'après l'ANSSI. Menace numéro 1 en France en 2021, le ransomware constitue 60% des attaques observées par le CERT-Wavestone. Dans 56% des cas, les victimes n'avaient pas anticipé être la cible potentielle d'une cyberattaque et dans 90% des cas, des données ont été perdues irrémédiablement. La formation des collaborateurs est plus que jamais nécessaire à la pérennité des organisations et Mailinblack répond à ce besoin grâce à des exercices réguliers en conditions réelles pour les entraîner à repérer les messages dangereux et adopter de bons réflexes.

"Le coût moyen des rançons est estimé à 250 000€ et les coûts indirects d'une attaque générés par une interruption de l'activité sont 5 à 10 fois plus élevés que la rançon. En moins d'un an, le coût moyen total de reprise d'activité après une attaque par ransomware a plus que doublé. Intégrer un module de formation aux attaques par ransomware à notre outil Cyber Coach était pour nous une évidence au regard de l'augmentation de ce type d'attaques et des risques encourus par les organisations," **explique Thomas Kerjean, Directeur Général chez Mailinblack.**

L’humain : cible numéro 1 des cyber attaquants

Le ransomware, également connu sous le nom de rançongiciel, est un logiciel malveillant qui bloque l'accès aux équipements numériques en les chiffrant et demande le règlement d’une rançon en échange d’une clé de décryptage. Ce type de virus, véhiculé majoritairement par email, se cache dans une pièce-jointe vérolée ou derrière un lien malveillant. Les pirates informatiques exploitent des failles technologiques et humaines telles que le manque de connaissance en cybersécurité des collaborateurs. Ils misent également sur la détresse des victimes pour obtenir le paiement de la rançon.

Avec plus de 80% des attaques qui transitent par email, l’approche pédagogique de Mailinblack se fonde sur la sensibilisation et la formation des collaborateurs. Cyber Coach replace l’humain au cœur de la cybersécurité et s'appuie sur une véritable collaboration entre équipes R&D, clients et neuroscientifiques.

Les messageries professionnelles représentent une porte d'entrée de choix pour les hackers et dans 99 % des cas (Harvard Business Review), l'humain reste la cible prioritaire. Des simulations d'attaques permettent donc de se tester, d’apprendre et de prendre conscience des conséquences potentielles sur son organisation.

Les plus petites d’entre elles sont souvent les plus vulnérables et ne peuvent sous-estimer ce risque et la nécessité de former leurs collaborateurs.

Des simulations d’attaques personnalisées, inopinées et régulières

Afin de maintenir le niveau de vigilance des collaborateurs, les simulations d’attaques s’effectuent de manière inopinée et régulière. Ce nouveau module dédié aux ransomwares permet de choisir un modèle d’attaque préconçu ou de composer soi-même des scénarios de ransomware. Ces modèles couvrent les techniques et les sujets les plus fréquents et les plus innovants utilisés par les cybercriminels.

À chaque sujet, une pièce-jointe différente est associée (au format word ou excel, avec d’autres formats à venir début 2022) :

- Facture impayée
- Règlement RGPD à acter
- Bon d’achat à recevoir
- Salaires employés
- Paiement encaissé

- Livraison produit prévue
- Informations personnelles

Si le collaborateur se fait piéger, la page de sensibilisation qui sera envoyée aux collaborateurs rançonnés sera adaptée en fonction du sujet choisi.

*Source : Rapport Ransomware Marketplace

_

À propos de Mailinblack :
Fondée en 2003, Mailinblack est la pépite française qui rend la cybersécurité accessible à toutes les organisations. Ses équipes, constituées de 70 collaborateurs basés à Marseille, conçoivent, développent et hébergent en France ses solutions de cybersécurité. Parmi elles, la solution Protect (protection de messagerie contre malware, phishing, ransomware, spam, scam…) ou encore l'outil de sensibilisation et de formation Phishing Coach, qui réduit de 70% les risques de cyberattaques. Lauréate du Grand Défi Cyber et forte de plus de quinze années d'expertise en sécurité, R&D et intelligence artificielle, Mailinblack recense aujourd'hui 1 million d'utilisateurs et 14 000 clients dans le secteur public et privé.

Contact presse : Agence Oxygen RP
Caroline Hoffmann - caroline.h@oxygen-rp.com - 06 77 51 58 42
Henry de Romans - henry@oxygen-rp.com - 02 72 88 12 69