SÉCURITÉ DES DONNÉES – LA MENACE CROISSANTE DE L'HAMEÇONNAGE TÉLÉPHONIQUE

Publié le 22 septembre, 2022

Catégories: Perspectives, Publications

Si vous possédez un téléphone, vous avez probablement déjà reçu un appel douteux d'un numéro inconnu visant à vous soutirer des renseignements confidentiels. Il se trouve que ces appels sont de plus en plus nuisibles aux entreprises.

Qu'entend-on par hameçonnage téléphonique?

L'hameçonnage téléphonique (aussi appelé hameçonnage vocal) est une technique par laquelle un hameçonneur tente d'obtenir d'une personne ses renseignements confidentiels en se faisant passer pour quelqu'un d'autre[1], par exemple un employé de la banque ou du service de TI d'une entreprise, ou un fonctionnaire. Les renseignements personnels ainsi soutirés serviront ensuite d'autres fins, comme détourner l'identité et l'argent de la victime, ou attaquer par rançongiciel le système informatique d'une entreprise[2].

Les hameçonneurs se font souvent passer pour des fonctionnaires de l'Agence du revenu du Canada (« **ARC** »). L'ARC présente des transcriptions d'arnaques téléphoniques dans ses alertes à l'arnaque. Les fraudeurs tentent de faire peur aux gens, par exemple en prétendant que des poursuites criminelles sont intentées contre eux, qu'un privilège sera inscrit sur leurs biens, ou que des actions en justice seront prises à leur encontre[3].

Une technique en hausse

Ces dernières années, les fraudeurs ont raffiné leurs techniques d'hameçonnage téléphonique et emploient des outils de plus en plus sophistiqués pour convaincre les gens de leur révéler des renseignements. Il peut s'agir par exemple de modifier l'identité de l'appelant pour qu'un numéro officiel figure à l'écran, ou encore de cloner une voix au moyen d'algorithmes d'apprentissage automatique et de technologie de voix pour reproduire la voix d'une personne de confiance[4].

En janvier 2021, dans un avis au secteur privé, le FBI mettait en garde contre une hausse du nombre d'attaques par hameçonnage téléphonique visant des réseaux d'entreprise[5], et plus particulièrement d'attaques hybrides, qui combinent attaques ciblées (« harponnage ») et hameçonnage téléphonique[6]. L'efficacité de ces attaques hybrides est inquiétante : des tests d'IBM ont révélé qu'elles sont trois fois plus efficaces que les

attaques par harponnage uniquement (taux de clic de 53,2 %) [7].

Mesures de prévention et d'atténuation

Le Centre canadien pour la cybersécurité, le FBI et le département de la Santé et des Services sociaux des États-Unis ont publié des lignes directrices pour protéger les gens et les entreprises de telles menaces :

- Utilisez les fonctions intégrées de protection des téléphones intelligents[8].
- Efforcez-vous de bloquer les appels automatisés ou les appels provenant de numéros inconnus.
- Méfiez-vous des comportements ou éléments douteux, par exemple :
    - la sollicitation d'information sensible;
    - les tactiques de peur ou les demandes urgentes;
    - les offres trop belles pour être vraies;
    - les éléments inhabituels pour l'entreprise ou le ministère ou organisme dont il est prétendument question, par exemple des appels de piètre qualité, un interlocuteur à la voix robotique ou au débit inhabituel[9].

Les entreprises ont tout intérêt à former leur personnel sur l'hameçonnage téléphonique, les nouvelles formes d'hameçonnage et la manière d'y réagir[10]. Il est également bon de mettre régulièrement les employés à l'épreuve par des simulations afin de déterminer s'il y a lieu d'offrir davantage de formation ou d'information sur le sujet. Mais comme il est impossible de se prémunir entièrement du risque d'hameçonnage, mieux vaut adopter une approche de sécurité multiniveaux. Voici quelques mesures d'atténuation pertinentes :

- Mettez en place l'authentification multifactorielle (MFA) pour l'accès aux comptes employés afin de réduire les risques de compromission initiale [11]. Privilégiez les mots de passe à usage unique plutôt que les notifications poussées (qui sont parfois acceptées sans que soit connue la source, par lassitude devant les notifications répétées)[12].
- Accordez aux nouveaux employés des droits d'accès minimaux[13].
- Analysez et surveillez activement les réseaux pour détecter les accès et modifications non autorisés[14].
- Segmentez votre réseau en plusieurs petits réseaux de manière à mieux en contrôler le trafic[15].
- Dotez les administrateurs de deux comptes : un compte avec accès administrateur avec lequel il est possible d'apporter des changements au système, et un compte pour l'envoi de courriels, la gestion des mises à jour et la production de rapports[16].

Si vous avez des questions sur les risques croissants d'hameçonnage téléphonique et la conception de programmes et politiques de cybersécurité, communiquez avec un membre du groupe Protection de la vie privée et des données.

[1] Centre canadien pour la cybersécurité, Qu'est-ce que l'hameçonnage vocal? – ITSAP.00.102 (25 juillet 2022) Il existe également de l'hameçonnage par texto et par code QR.
[2] Centre canadien pour la cybersécurité, Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage –00.101 (août 2022)
[3] Gouvernement du Canada, Exemple d'arnaque au téléphone (17 mai 2022)
[4] Qu'est-ce que l'hameçonnage vocal?, Comment fonctionne l'hameçonnage vocal?
[5] Federal Bureau of Investigation, Cyber Division, Private Industry Notification 20210114-001, en anglais seulement (14 janvier 2021).
[6] Rodika Tollefson, Spearphishing meets vishing: New multi-step attack targets corporate VPNs, en anglais seulement (15 décembre 2020).
[7] IBM, X-Force Threat Intelligence Index 2022 , page 5 (février 2022).
[8] Qu'est-ce que l'hameçonnage vocal?, Conseils pour repérer l'hameçonnage vocal et éviter de tomber dans le piège.
[9] Ne mordez pas à l'hameçon, Il pourrait y avoir anguille sous roche si.
[10] Qu'est-ce que l'hameçonnage vocal?, Conseils pour repérer l'hameçonnage vocal et éviter de tomber dans le piège.
[11] FBI Private Industry Notification, page 2.
[12] Une technique en hausse, page 2.
[13] Précité, note 11.
[14] *id.*
[15] *id.*
[16] *id.*

Par Robbie Grant, Vaughan Rawes (stagiaire en droit) et Zijian Yang (étudiant d'été)

Mise en garde