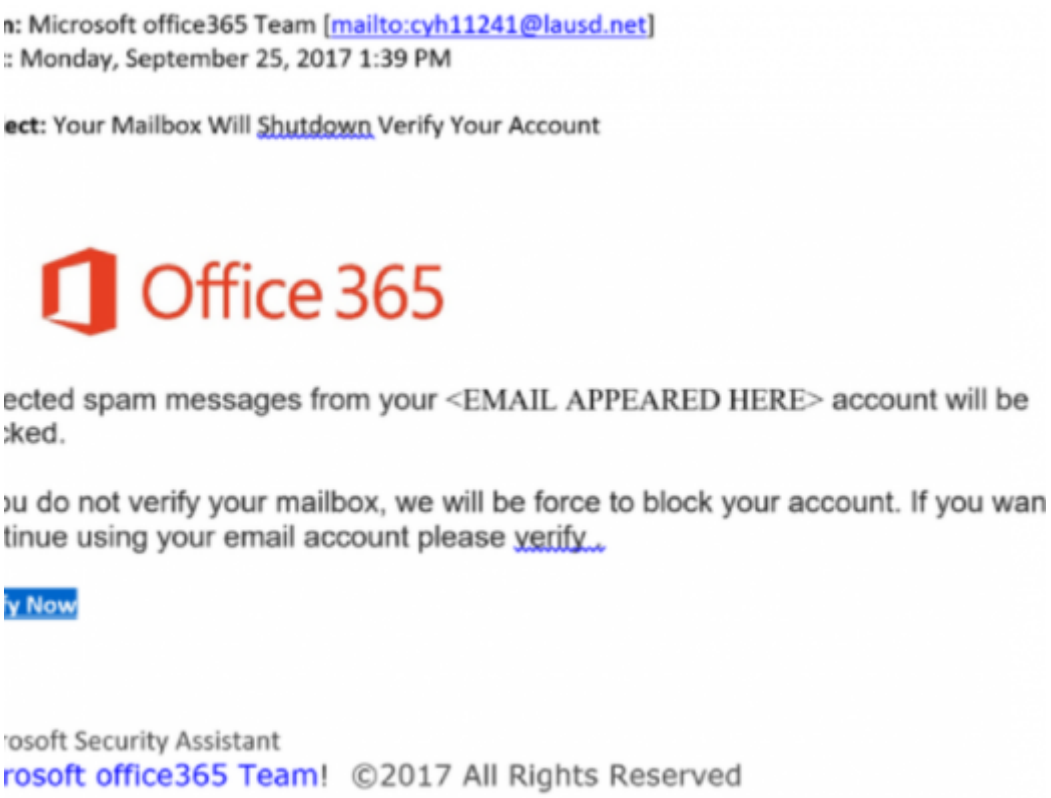
04 fév 2021 -08:00

Les cybercriminels exploitent les boîtes mail d’entreprises belges pour voler des mots de passe

La pandémie de COVID-19 semble être l’occasion rêvée pour les cybercriminels de passer à l'action. Plusieurs partenaires en charge de la cybersécurité font état d'attaques visant des entreprises belges. Il est difficile d'estimer le nombre de victimes car les relevés ne reflètent pas la réalité. D’une part, les gens n'aiment pas admettre qu'ils ont été victimes et, d’autre part, les entreprises craignent que leur image en prenne un coup.



Quel est le modus operandi des cybercriminels ?

Les escrocs recréent méticuleusement les pages de connexion de plateformes populaires telles que Microsoft Office 365, PayPal et d'autres services en ligne. Ils envoient ensuite à leurs victimes un message de phishing contenant un lien ou une pièce jointe, les incitant à se connecter en donnant un motif comme « Votre boîte mail va être bloquée. Vérifiez votre compte ». L'utilisateur peu méfiant saisit ses données de connexion sur le faux site Internet et les transmet ainsi sans le savoir aux criminels.

"Dans ce type d'attaques, les cybercriminels peuvent contaminer en un rien de temps d'autres utilisateurs et entreprises, en exploitant les contacts de la victime."

Phédra Clouner
vice-directrice du CCB

Comment se protéger contre le piratage de ses données de connexion ?

- Soyez prudent si vous recevez un message d'une plateforme vous demandant de saisir votre mot de passe.
- Contrôlez l'adresse électronique de l'émetteur et l'URL du lien sur lequel vous devez cliquer. Si certains aspects vous paraissent inhabituels, il s'agit probablement d'un cas de phishing.
- Que faire ? Ouvrez votre navigateur et introduisez l'URL correcte, p. ex. : https://www.office.com/ https://www.paypal.com/

"Le phishing peut avoir des conséquences désastreuses. La meilleure défense consiste à rester sur ses gardes et savoir quels éléments doivent attirer notre attention. Soyez par exemple très prudent lorsque vous recevez des messages qui qui requièrent des actions urgentes ou aux mails qui présentent des fautes d'orthographe. Pour trouver des conseils, rendez-vous sur notre site Internet"

Bart Asnot
Security expert auprès de Microsoft BeLux

Comment savoir si l'on est victime de l'attaque ?

- Des mails sont envoyés en votre nom depuis votre boîte mails alors que vous n'êtes pas à l'origine de l'action.
- Quelques semaines plus tard, il est possible que vous receviez plus de messages de phishing qu'à l'accoutumée. Vos données ont peut-être été diffusées sur Internet et réutilisées par des cybercriminels.

Que faire si vous êtes victime ?

- Modifiez immédiatement votre mot de passe (sur chaque compte où vous l'utilisez) ;
- Prévenez vos contacts ;
- Activez l'authentification à double facteurs (Configurer votre connexion Microsoft 365 pour l'authentification multifacteur) ;
- Les cybercriminels ont peut-être activé une réponse automatique. Supprimez-la ;
- Il est possible qu'un paramètre redirige vos mails vers un dossier d'archives interne ou une adresse mail externe. Supprimez ce paramètre ;
- Vérifiez les informations disponibles par le biais de cette boîte mail. Certaines informations sensibles ou confidentielles peuvent avoir été compromises. Il est préférable d'en être informé.

Si vous recevez un message de phishing, envoyez-le à suspect@safeonweb.be. Nous ferons bloquer les liens afin que d'autres internautes moins attentifs ne tombent dans le panneau.

Pour plus d'informations :

- https://www.safeonweb.be
- https://anchor.fm/fraudeur-hacker-en-jij (Podcast)
- https://www.microsoft.com/security/blog/2019/10/16/top-6-email-security-best-practices-to-protect-against-phishing-attacks-and-business-email-compromise/

Personnes de contact pour la presse

- Andries Bomans (responsable presse CCB, NL/FR) : 0471 66 00 06, andries.bomans@ccb.belgium.be
- Katrien Eggers (responsable presse CCB, NL/FR) : 0485 765 336, katrien.eggers@cert.be

- Cathy Suykens (responsible presse Cyber Security Coalition, NL/FR : 0499 71 84 96, cathy.suykens@cybersecuritycoalition.be

À propos du Centre pour la Cybersécurité Belgique

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique. Il supervise, coordonne et veille à la mise en œuvre de la stratégie belge en matière de cybersécurité. Grâce à un échange d'informations optimal, les entreprises, les autorités, les opérateurs de services essentiels et les citoyens peuvent compter sur une protection adéquate. www.ccb.belgium.be

À propos de la Cyber Security Coalition vzw

La mission de la Cyber Security Coalition est de renforcer la résilience de la cybersécurité en Belgique en construisant un écosystème de cybersécurité solide au niveau national. Nous le faisons en réunissant les compétences et l'expertise du monde académique, du secteur privé et des pouvoirs publics sur une plate-forme de confiance visant à favoriser l'échange d'informations, la collaboration opérationnelle, en émettant des recommandations pour des politiques et des lignes directrices plus efficaces et finalement en réalisant des campagnes de sensibilisation conjointes s'adressant aux citoyens et aux organisations. Plus de 500 représentants de nos 102 organisations membres participent à nos activités et, à ce titre, contribuent à notre mission.

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be