07 jan 2021 -10:22

Près de deux fois plus de messages transférés à suspect@safeonweb.be en 2020

L'année dernière, les internautes ont transféré pas moins de 3 225 234 messages à l'adresse e-mail suspect@safeonweb.be, soit plus de 8800 messages par jour. Il s'agit d'un nombre presque deux fois plus élevé que celui de 2019, lorsque quelque 1 700 000 messages nous avaient été transmis.

Que faisons-nous de ces 3 millions de messages ?

Il est désolant de constater que les cybercriminels envoient toujours plus de messages avec pour seul et unique objectif de piéger les internautes. Ces messages arrivent non seulement par e-mail, mais aussi par SMS ou sur les réseaux sociaux. Nous ne lisons évidemment pas tous les messages que vous transférez à l'adresse suspect@safeonweb.be ; leur analyse est automatisée.

Cette analyse commence par la détection des liens et des pièces jointes. Sur les 3 millions de messages que nous avons reçus, nous avons repéré 8 545 658 liens, dont 667 356 correspondaient à des tentatives de fraude (phishing, faux webshop, scam, ...) . Nous transmettons ensuite ces liens suspects à Google Safebrowsing et Microsoft Smartscreen, qui publient à leur tour un message d'alerte. Si une personne essaie de visiter ces pages Internet, elle verra apparaître un écran rouge affichant un message clair : Attention, la page que vous essayez de consulter est dangereuse. Parmi ces messages transférés, nous avons par ailleurs pu détecter 26 109 pièces jointes dont 4370 contenaient un virus.

La crise du coronavirus a-t-elle joué un rôle ?

Les cybercriminels ont semblé d'autant plus actifs au cours de cette crise du coronavirus. Nous ne sommes toutefois pas en mesure de confirmer qu'il y a effectivement eu plus de tentatives de phishing durant cette période. Ce qui est sûr en revanche, c'est que vous nous avez transmis ces messages à une fréquence beaucoup plus élevée.

Nous avons trouvé un mot-clé lié au coronavirus dans 45 195 messages ; une minorité donc. Nous avons en revanche assisté aux énièmes retours des traditionnels messages de phishing :

- Les messages provenant soi-disant d'un service de livraison et vous demandant de d'abord payer les frais de port.
- Les messages provenant soi-disant de banques et vous incitant à demander une nouvelle carte ou à débloquer votre compte.
- Les messages provenant soi-disant d'un organisme public et vous promettant une prime ou une compensation.
- Les messages provenant soi-disant de services tels que Dropbox, PayPal, Microsoft.
- Les messages surfant sur l'actualité : masques de protection, périodes de fêtes, une prime promise.

Quand un message devient-il suspect ?

Si plusieurs éléments doivent vous mettre la puce à l'oreille, la première recommandation est surtout de faire preuve de bon sens. Si vous doutez de la véracité d'un message, c'est probablement qu'il est faux.

- Un message trop beau pour être vrai ? Soyez sur vos gardes.
- Vous devez réagir vite, sinon… Vous pouvez être sûr que quelqu'un essaie de vous tendre un piège.
- Le message est inattendu ou vient d'un inconnu ? Cherchez d'abord plus d'infos avant de répondre à une demande ou une question. Le message est probablement faux.
- Examinez minutieusement l'expéditeur et l'URL du lien. Ils ont une apparence inhabituelle ? Ne cliquez surtout pas et ne répondez pas non plus.
- Vous devez transmettre vos coordonnées bancaires ou d'autres informations importantes ? Alerte rouge ! Commencez par vous informer par une autre voie avant de transmettre l'information et de voir votre compte bancaire se vider d'un coup.

Apprenez à reconnaître les e-mails frauduleux.

Que faire ?

Transférez immédiatement les messages suspects à l'adresse suspect@safeonweb.be. Plus vite nous pouvons traiter le message, moins il fera de victimes.

Désormais, vous pouvez également nous transmettre des images (captures d'écran) des messages suspects. Notre technologie est désormais capable de détecter les URL directement à partir d'images. Nous invitons chacun à faire preuve d'un esprit très critique avant d'ouvrir un message et à réfléchir à deux fois avant de cliquer sur un lien ou une pièce jointe.

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

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

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