03 jan 2023 -11:00

13 millions de clics vers des sites suspects évités en 2022

En 2022, la collaboration avec la population a permis d'éviter pas moins de 13 millions de clics vers des sites Internet suspects, soit environ 25 avertissements aux internautes par minute.

Le « *Belgium Anti-Phishing Shield* » (BAPS) est un système conçu par le Centre pour la Cybersécurité Belgique (CCB) pour mettre en garde les internautes surfant vers des sites Internet dangereux.

Depuis de nombreuses années déjà, le CCB peut s'appuyer sur la collaboration de la population grâce aux notifications de messages suspects. Chaque jour, nous recevons des milliers d'e-mails suspects. En 2021, 4.500.000 messages ont été transférés à l'adresse suspect@safeonweb.be. En 2022, ce chiffre a encore grimpé pour atteindre 5,5 millions de messages, ce qui a permis la détection de plus de 1,5 millions d'URL suspects, soit une moyenne de 15.000 messages analysés par jour.

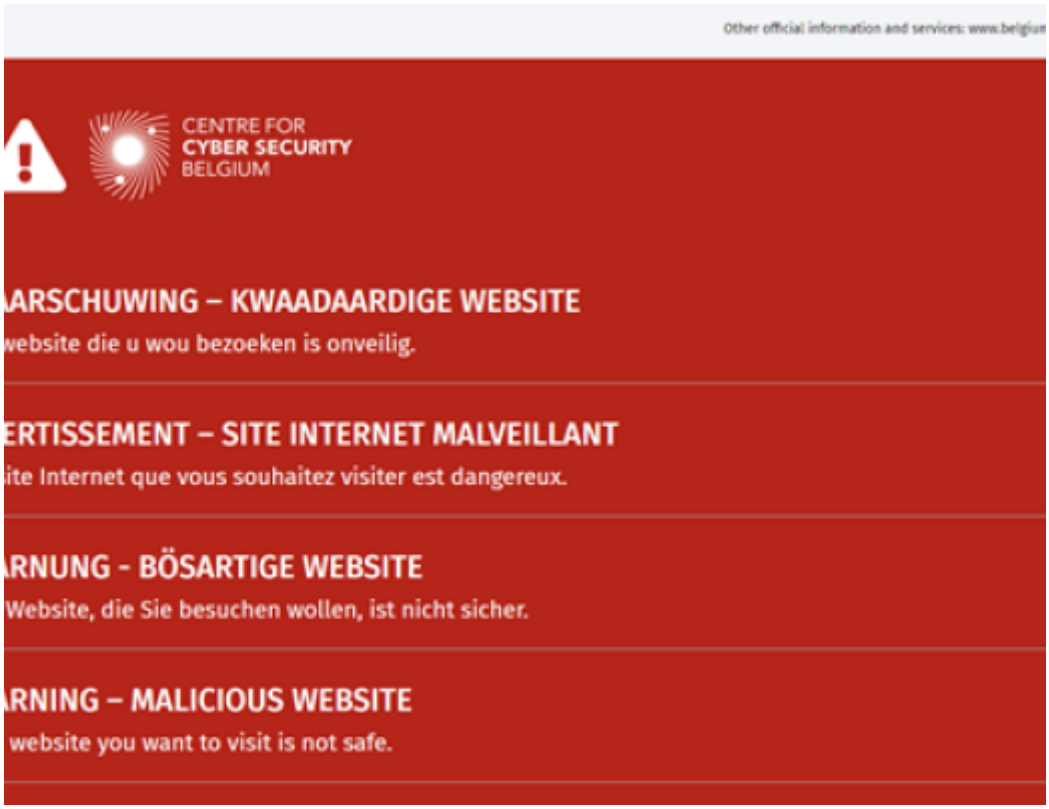
Les URL suspects figurant dans ces e-mails sont transférés à Google SafeBrowsing et Microsoft SmartScreen. Les navigateurs utilisent alors ces informations pour mettre en garde les citoyens contre les sites Internet malveillants. Etant donné que nous n'avons aucun contrôle sur la vitesse d'exécution de Google et Microsoft quant au blocage de ces liens, le CCB et les fournisseurs d'accès à Internet Belnet, Proximus, Telenet et Orange sont parvenus à développer leur propre système ainsi qu'une procédure permettant d'avertir les internautes en temps réel: le *Belgium Anti-Phishing Shield* (BAPS).

Le Centre pour la Cybersécurité Belgique demande au public de continuer à transmettre les messages suspects à suspect@safeonweb.be. La rapidité d'envoi des messages permet de réduire au minimum le nombre de victimes. Une personne moins attentive qui serait tentée de cliquer sur un lien aboutira les cas échéant sur une page de mise en garde. Le BAPS ne peut donc être efficace sans l'envoi des messages suspects par la population.

Il est aussi possible d'envoyer une capture d'écran de SMS frauduleux et de messages contenant des QR-codes. Notre technologie est en mesure de détecter les URL sur les images et dans les QR-codes.

> "Voici un bel exemple de collaboration constructive entre la population et les pouvoirs publics. Une collaboration unique en son genre en Europe et une preuve de plus que notre pays est capable de grandes choses avec peu de moyens. C'est en alliant nos forces dans la lutte contre la cybercriminalité que nous parviendrons à l'endiguer dans les prochaines années.
>
> Le chemin est encore long mais nous ne devons pas abandonner."

Miguel De Bruycker
Directeur du Centre pour la Cybersecurité Belgique



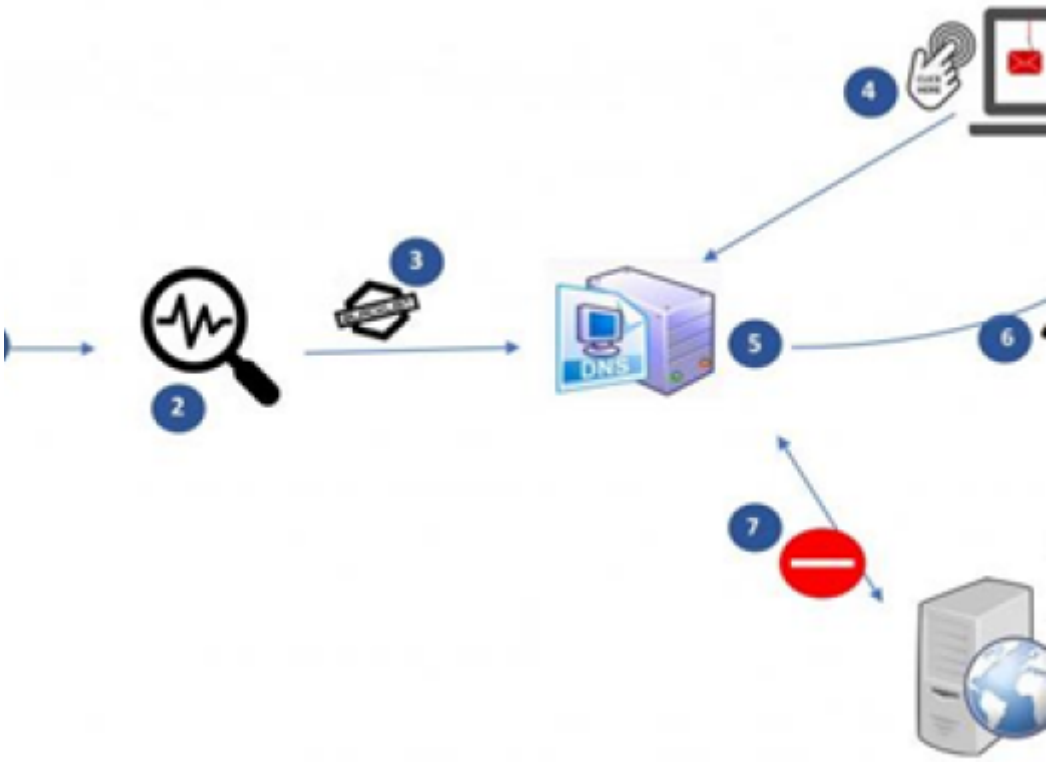
Qu’est-ce que le « Belgium Anti-Phishing Shield » ou BAPS?

Le Belgium Anti-Phishing Shield (BAPS) avertit la population en fonction des liens malveillants transmis au CCB via suspect@safeonweb.be. Le BAPS a été testé en 2021 et a progressivement été mis à la disposition des citoyens.

Lorsqu’un utilisateur en Belgique clique sur un lien, la demande de consultation de la page Internet est envoyée à son fournisseur d’accès Internet (FAI). Ce dernier vérifie alors à l’aide du BAPS si le domaine (site Internet) auquel l’utilisateur veut accéder ne figure pas sur une liste des domaines malveillants. Si c’est le cas, le serveur du fournisseur Internet transfèrera l’internaute vers une page de mise en garde.

Comment cette liste des sites Internet malveillants est-elle établie?

La liste des sites Internet malveillants est établie grâce aux milliers de messages suspects transférés chaque jour par les citoyens à l'adresse suspect@safeonweb.be. Les domaines Internet qui apparaissent dans ces messages sont automatiquement évalués et très rapidement transférés aux fournisseurs d'accès Internet – au plus vite, au mieux ! Une évaluation approfondie permet d'éviter qu'un site Internet légitime n'apparaisse par erreur sur cette liste alors que le BAPS vise exclusivement le phishing. Seuls les sites désignés comme « dangereux » sont consignés dans la liste.



Comment fonctionne le BAPS?

- Le CCB reçoit des informations sur les sites Internet potentiellement malveillants via suspect@safeonweb.be;
- Les sites Internet potentiellement malveillants sont analysés et consignés dans une liste;
- La liste des sites Internet malveillants est transmise aux fournisseurs d'accès à Internet;
- L'internaute clique sur l'URL malveillant;
- Le fournisseur internet vérifie si le site qui fait l'objet de la demande DNS figure dans la liste des sites (domaines) Internet malveillants;

- Si c’est le cas, l’internaute est redirigé vers une page de mise en garde;
- L’internaute n’accède pas au site Internet malveillant.

Contact pour la presse

Michele Rignanese (Porte-parole CCB, NL/FR): 0477 38 87 50, michele.rignanese@ccb.belgium.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

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Michele Rignanese
Porte-parole FR
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Porte-parole NL
+32 485 76 53 36
katrien.eggers@cert.be