INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS

COMMUNIQUÉ DE PRESSE

L'Institut belge des services postaux et des télécommunications (IBPT) et le Centre pour la cybersécurité Belgique tirent à nouveau la sonnette d'alarme face à un tsunami de messages de smishing après de faux SMS.

Bruxelles, le 14 septembre 2021 – Depuis la semaine dernière, les opérateurs mobiles ont bloqué plus de 2 millions de SMS par jour. En effet, le dangereux virus Flubot fait à nouveau rage. Ce virus peut prendre le contrôle total d'un GSM et envoyer des SMS au nom de la victime vers tous les contacts enregistrés dans le répertoire de l'appareil ainsi que vers d'autres numéros de GSM. Plus de 2 000 GSM infectés ont déjà été bloqués par les opérateurs mobiles au cours de ces derniers jours en raison d'un trafic de SMS anormalement élevé.

« Les SMS suspects semblent à nouveau provenir d'un service de colis. Si vous cliquez sur le lien contenu dans le SMS, on vous demande alors de télécharger une application. Ne le faites surtout pas. Vous installerez un virus sur votre appareil qui pourra avoir accès à vos données personnelles telles que vos mots de passe, vos données de carte bancaire et l'ensemble de votre liste de contacts », déclare Katrien Eggers, porte-parole du CCB.

Les SMS sont envoyés depuis les GSM de clients infectés par le malware mobile Flubot (nom du virus qui se propage via les SMS). Il est difficile de déterminer l'origine exacte des SMS, car une fois infecté, c'est le GSM du client qui devient le vecteur de transmission aux autres utilisateurs. En d'autres mots, ces SMS viennent donc de clients légitimes des opérateurs de télécommunications.

Avertissement urgent

Jack Hamande, membre du Conseil de l'IBPT : « Lorsque les opérateurs constatent qu'un client a été infecté, par exemple sur la base d'un trafic anormal de SMS, ils bloquent temporairement ce client et lui donnent les raisons du blocage et les instructions à suivre pour éliminer le malware. C'est donc au client lui-même d'éliminer le malware mobile de son appareil. Il est important que les clients le fassent. En effet, le logiciel malveillant envoie également des messages internationaux et peut donc éventuellement entraîner des factures élevées. »

Les opérateurs bloquent temporairement les numéros des clients infectés. Le client peut alors encore appeler et recevoir des SMS, mais ne peut plus en envoyer. Après une certaine période, ou après que le client a indiqué avoir éliminé le malware, il peut à nouveau envoyer des messages. Si un nouveau trafic suspect de SMS est détecté, le client sera à nouveau bloqué temporairement.

Depuis la semaine dernière, les opérateurs mobiles ont bloqué plus de 2 millions de SMS par jour. Plus de 2 000 GSM infectés ont déjà été bloqués par les opérateurs mobiles au cours de ces derniers jours en raison d'un trafic de SMS anormalement élevé.

Institut belge des services postaux et des télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 Bte 1 | 1030 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **E** info@ibpt.be| **www.ibpt.be**

C'est la raison pour laquelle l'IBPT et le CCB lancent un appel urgent aux utilisateurs de téléphones mobiles :

1. Soyez toujours vigilants lorsque vous recevez un message inattendu

2. Ne cliquez pas sur un lien dans un SMS !

3. N'installez jamais d'applications via un lien dans un SMS
Installez uniquement des applications depuis une boutique d'applications standard (Google Play, App Store). Si, lors de l'installation d'une application, vous recevez un message empêchant l'installation ou un avertissement de sécurité, ne continuez surtout pas.

Toute personne qui a installé Flubot sur un GSM doit immédiatement supprimer le virus. Comment ?

Méthode 1 : Restaurez les paramètres d'usine de votre appareil

Méthode 2 : En redémarrant l'appareil en « mode sans échec », puis en supprimant la fausse application

Après avoir supprimé le virus, modifiez tous les mots de passe des comptes auxquels vous avez accès depuis votre smartphone. Comme il se peut qu'un SMS ait été envoyé au nom de la victime vers tous ses contacts, ceux-ci doivent également être avertis le plus vite possible.

En outre, les victimes ne remarqueront pas toujours immédiatement qu'un très grand nombre de SMS a été envoyé. Il sera toutefois possible de constater l'envoi massif de SMS sur la facture de téléphone. Dans ce cas, la victime doit contacter son opérateur. Ce n'est que lorsque l'application aura été supprimée que le numéro ne pourra plus être utilisé de manière abusive.

Vous pouvez envoyer des captures d'écran des messages frauduleux à suspect@safeonweb.be.

Plus d'infos : https://safeonweb.be/fr/actualite/attention-au-dangereux-virus-flubot-ne-cliquez-pas-sur-les-sms-suspects

---

Personnes de contact pour la presse
Katrien Eggers (porte-parole CCB, NL/FR) : 0485 765 336, katrien.eggers@cert.be
Jimmy Smedts (porte-parole IBPT) : 0478/63.91.82, jimmy.smedts@bipt.be

Concernant le 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

Concernant l'Institut belge des services postaux et des télécommunications
L'IBPT est le régulateur fédéral compétent pour le marché des communications électroniques, le marché postal, le spectre électromagnétique des radiofréquences et la radiodiffusion sonore et télévisuelle dans la Région de Bruxelles-Capitale.

Pour plus d'informations :

Jimmy Smedts | Porte-parole

Institut belge des postes et télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 bte 1 | 1030 Bruxelles
T +32 2 226 88 22 | **M** +32 478 63 91 82 | **www.ibpt.be**