Question écrite de la Députée Kattrin JADIN
à Monsieur Charles MICHEL, Premier ministre
concernant
la cybercriminalité mobile
- déposée le 23 août 2018 -

Monsieur le Premier Ministre,

Au niveau mondial, le spécialiste antivirus Kaspersky a détecté 61.045 chevaux de Troie dans la banque mobile, soit des virus permettant aux hackers d'accéder à l'application bancaire des utilisateurs.

Selon Kaspersky, le nombre d'attaques à l'encontre de ces applications a doublé en un an.

Le procédé est le suivant : les chevaux de Troie s'introduisent dans les smartphones via des applications contrefaites ou cachées installées par des utilisateurs et prennent ainsi l'apparence d'une application classique. Lorsque l'utilisateur introduit des données, elles sont ensuite volées par un malware.

Jusqu'à présent, aucun cas n'a été identifié en Belgique mais la menace continue d'augmenter et il faut s'attendre à une croissance d'attaques de ce genre.

Un analyste en sécurité de Kaspersky mentionne également que « *la croissance globale des malware mobiles, et en particulier de ceux qui visent le secteur bancaire, montre que les cybercriminels ne cessent d'améliorer leurs logiciels et de les rendre plus difficiles à identifier* ».

Monsieur le Premier Ministre, mes questions sont les suivantes :

- Des attaques cybercriminelles au niveau des applications ont-elles déjà eu lieu dans d'autres domaines ? Quel est l'état de ce phénomène en Belgique ?
- Comment peut-on lutter contre ce genre d'attaques ?
- Des mesures sont-elles d'application pour éviter ce genre de pratiques frauduleuses ?

Je vous remercie, Monsieur le Premier Ministre, pour les réponses que vous voudrez bien m'apporter.

Kattrin JADIN

26-10-2018

Doc. 54 2017201824726
D01
N° 341

Réponse de Monsieur le Premier Ministre à la question parlementaire n° 341 « La cybercriminalité mobile » qui lui a été posée le 2 octobre 2018 par Madame la Représentante Kattrin JADIN

1. Slachtoffers van cybercriminaliteit kunnen aangifte doen of klacht neerleggen bij de politie . Het is dan ook de politie die alle gegevens en cijfers bijhoudt van het aantal en type cybercriminaliteit in België.

2. Voor het bestrijden van malware op mobiele toestellen gelden dezelfde regels als bij malware voor computers. Preventief kunnen belangrijke maatregelen worden getroffen zoals voornamelijk het installeren van een antivirussoftware en regelmatig updates uitvoeren.

Deze niet technische preventieve maatregelen kunnen genomen worden door de eigenaar van het toestel. Voor de bestrijding van deze aanvallen is het daarom belangrijk dat de bevolking bewust wordt gemaakt voor de gevaren van malware op mobiele toestellen en dat ze makkelijk toegang heeft tot de juiste informatie om dit te voorkomen.

Het installeren van een antivirus/antimalware app op het mobiele toestel helpt om gekende problemen zo snel mogelijk te detecteren en te verwijderen.

Door mobiele apparaten up-to-date te houden worden kwetsbaardheden in applicaties zo snel mogelijk opgelost. Dit zorgt ervoor dat het mobiele toestel minder vatbaar is voor malware.

Op safeonweb.be, de informatiewebsite rond online-veiligheid voor de Belgische bevolking dat wordt beheerd door het Centrum voor Cybersecurity België, wordt de bevolking geïnformeerd over de te nemen beveiligingsmaatregelen op mobiele toestellen. Daarnaast organiseert het CCB een jaarlijkse

1. Les victimes d’actes de cybercriminalité peuvent faire une déclaration ou porter plainte auprès de la police. C'est donc la police qui conserve l’ensemble des données et des chiffres relatifs au nombre et au type d’actes de cybercriminalité commis en Belgique.

2. Les règles de lutte contre les logiciels malveillants sont les mêmes, que ces malwares s'attaquent à des appareils mobiles ou à des ordinateurs fixes. D'importantes mesures préventives peuvent être prises, notamment l'installation d'un logiciel antivirus et la réalisation de mises à jour régulières.

Ces mesures préventives non techniques peuvent être appliquées par le propriétaire de l'appareil. Dans le cadre de la lutte contre ces attaques, il importe donc que la population soit sensibilisée aux dangers des logiciels malveillants sur les appareils mobiles et qu'elle ait facilement accès aux informations adéquates pour les prévenir.

L'installation d'une application antivirus/antimalware sur l'appareil mobile permet de détecter et de supprimer au plus vite les problèmes connus.

La mise à jour des appareils mobiles permet de résoudre rapidement les vulnérabilités dont souffrent les applications. L'appareil mobile devient ce faisant moins sensible aux logiciels malveillants.
Sur safeonweb.be, le site d'information sur la sécurité online destiné à la population belge et géré par le Centre pour la Cybersécurité Belgique, la population est informée des mesures de sécurité à prendre au niveau des appareils mobiles. En outre, le CCB organise une campagne annuelle de sensibilisation à la

sensibiliseringscampagne rond cyberveiligheid, zowel op computers als mobiele toestellen, tijdens de European Cyber Security Awareness Month in oktober. Zo was het doel van de campagne in 2016 het aanmoedigen van de Belgische bevolking tot het installeren van antivirusscanners en is het huidige thema van de campagne (2018) het regelmatig uitvoeren van updates en het maken van back-ups.

3. Sommige maatregelen kunnen specifiek op mobiele toestellen genomen worden. De belangrijkste zijn het controleren van de gegeven permissies bij het installeren van een applicatie, het installeren van applicaties uit een vertrouwde bron en het nakijken van de beoordelingen van een applicatie.

Tenslotte is het belangrijk te kijken naar het besturingssysteem van het mobiele toestel. IOS en Android hanteren een verschillend niveau van app-controle voor het aanbieden van een applicatie op de applicatiestore.

cybersécurité, tant sur les ordinateurs que sur les appareils mobiles, pendant le Mois Européen de sensibilisation à la Cybersécurité (European Cyber Security Awareness Month) qui a lieu en octobre. Ainsi, l'objectif de la campagne de 2016 était d'encourager la population belge à installer des scanners antivirus. Le thème actuel de la campagne (2018) s'axe quant à lui sur la réalisation de mises à jour et de sauvegardes régulières.

3. Certaines mesures peuvent être prises spécifiquement sur les appareils mobiles. Les plus importantes sont la vérification des permissions accordées lors de l'installation d'une application, l'installation d'applications à partir d'une source fiable et la vérification de l'évaluation d'une application.

Enfin, il est important d'examiner le système d'exploitation de l'appareil mobile. IOS et Android utilisent un niveau différent de contrôle des applications pour offrir une application sur l'« app store ».