CENTRE FOR CYBER SECURITY BELGIUM

Communiqué de presse, 29/03/2019

Mise en garde du Centre pour la Cybersécurité Belgique :

Chaque jour, des escrocs qui se font passer pour des techniciens d'une entreprise informatique s'emparent de milliers d'euros

Chaque jour, 3 à 4 Belges en moyenne sont victimes d'escrocs qui se font passer pour des techniciens de Microsoft ou Apple. Les montants perdus se situent dans une fourchette entre 1 000 et 10 000 euros en moyenne mais, dans certains cas, la perte a dépassé les 100 000 euros. Les pertes annuelles pourraient même se chiffrer en millions d'euros.

Le point de contact du SPF Économie pour les fraudes, confirme lui aussi cette courbe ascendante. En 2018, 971 cas de cette forme d'escroquerie lui ont été signalés, contre 174 seulement en 2016.

> *Ce type d'escroquerie, également connue sous le nom de « Microsoft Scam » ou « Tech Scam », représente une véritable menace en ce moment. Nous estimons dès lors qu'il est important de sensibiliser la population et de la mettre en garde. Le phénomène n'est pas neuf, mais CERT.be, le service opérationnel du CCB, reçoit des dizaines de signalements de la part de victimes ces dernières semaines. Aujourd'hui encore, ces escrocs parviennent à mener des gens en bateau. Nous sommes convaincus que ces chiffres ne lèvent qu'un coin du voile sur le nombre réel de victimes. De nombreuses personnes ont honte d'être tombées dans le panneau et ne portent donc pas plainte auprès de la police.* Miguel De Bruycker, Directeur du Centre pour la Cybersécurité Belgique :

Le « Microsoft Scam », qu'est-ce que c'est exactement ?

Tout le monde en a entendu parler. Quelqu'un qui se fait passer pour un collaborateur de Microsoft ou d'Apple prend contact avec vous sur votre ligne fixe. Votre ordinateur est soi-disant confronté à un problème de sécurité mais la personne au bout du fil prétend pouvoir vous aider. À l'heure actuelle, le premier contact peut également prendre une autre forme : une alerte signalant la présence d'un virus apparait subitement à l'écran et votre ordinateur se retrouve complètement bloqué. Vous êtes invité à composer un numéro commençant par 078. Votre interlocuteur vous proposera volontiers son aide et tentera de vous garder longtemps en ligne (payante).

La personne au bout du fil ne s'exprime souvent qu'en anglais ou dans un français hésitant. Cet escroc vous fait croire que votre ordinateur est confronté à un problème de sécurité et vous propose donc de le sécuriser. L'escroc vous demande ensuite d'effectuer certaines actions : démarrer l'ordinateur, se rendre sur un certain site Internet ou télécharger une application. Certains essaient de vous vendre un logiciel antivirus totalement inconnu pour éliminer les virus qui n'ont en réalité pas du tout infecté votre ordinateur.

L'escroc peut ainsi obtenir un accès à votre ordinateur. Les escrocs essaient de faire peur à leurs victimes et paraissent souvent très menaçants. Ils ne se contentent pas de bloquer vos écrans et votre ordinateur : ils n'hésitent pas non plus à mettre en marche votre imprimante ou à activer votre webcam à distance. Ils forcent également les gens à éteindre leur téléphone portable pour éviter que les victimes puissent être averties d'une transaction suspecte par leur banque, par exemple.

Au final, l'objectif est bien de piller votre compte. Pour régler le problème, vous devez d'abord payer. L'escroc vous mènera ensuite sur un site Internet sur lequel vous devez effectuer un achat et il en profitera pour voler vos données et vider complètement votre compte bancaire. Dans certains cas, ces escrocs demandent aux gens d'ouvrir un compte Bitcoin pour transférer les montants. Tout ça est évidemment tout à fait suspect.

Recommandations

« Méfiez-vous toujours des coups de téléphone provenant de sociétés qui vous demandent d'effectuer une série d'actions sur votre ordinateur. Microsoft ne prendra pas contact avec vous pour régler un problème si vous n'en avez pas fait la demande », confirme Karel Dekyvere, Chief Security Officer chez Microsoft Belgique et Luxembourg.

- Ne laissez pas quelqu'un que vous ne connaissez pas prendre le contrôle de votre ordinateur.
- N'effectuez pas de paiement, même de petits montants, lorsqu'un inconnu a pris le contrôle de votre ordinateur.
- Supprimez toutes les applications ou programmes que vous avez installés sur votre ordinateur à la demande de l'escroc.
- Procédez ensuite à un scan anti-virus total et supprimez les malwares éventuellement détectés.
- Changez vos mots de passe, si vous les avez communiqués.
- Si votre écran est bloqué, vous pouvez fermer le navigateur en appuyant simultanément sur les touches Ctrl-Shift-Esc de votre clavier et ensuite sur « Fin de tâche ».

Plus d'informations

Lisez nos conseils sur Safeonweb.be : https://www.safeonweb.be/fr/je-suis-contacte-par-un-inconnu-pour-un-probleme-de-pc

Les conseils de Microsoft : https://pulse.microsoft.com/fr-be/making-a-difference-fr-be/na/fa2-evitez-de-vous-faire-pieger-5-astuces-contre-labus-ou-le-hameconnage/

À propos du Centre pour la Cybersécurité Belgique

Le Centre pour la Cybersécurité Belgique (CCB) est le centre national pour la cybersécurité en Belgique. Le CCB a pour objectif de superviser, de coordonner et de veiller à l'application de la stratégie belge en matière de cybersécurité. L'optimalisation de l'échange d'informations permettra d'offrir une protection adéquate à la population, aux entreprises, aux autorités et aux secteurs vitaux. www.ccb.belgium.be

À propos de CERT.be

La cyber emergency team (l'équipe d'intervention d'urgence en sécurité informatique) fédérale (CERT.be) est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB), qui soutient les autorités publiques, les services vitaux et les entreprises dans la prévention, la coordination et l'assistance sur le plan des cyberincidents. www.cert.be

Contact Presse

Katrien Eggers: 0485/76.53.36, katrien.eggers@cert.be