Cybercriminalité … Fin

02/10/2016

Bonsoir le Monde !

avec ce troisième et dernier volet de mes pérégrinations sur le sujet, je vais vous résumer ce qui peut quand même un petit peu servir si vous avez un souci avec une attaque cybercriminelle genre ransomware, phishing, mail spoofing et autres joyeusetés dans le genre **!**

Je tiens d'abord à remercier Carine P. qui m'a envoyé une petite alerte sur le sujet en février 2016 et l'article publié par la RTBF en août 2016 qui m'ont intrigués et suscités ces 3 articles.

Ce qu'il faut retenir, c'est **TTP** s'il t'arrive quelque chose: **Tire Ton Plan !**
Et ce malgré tous les beaux discours et les innombrables publications sur le sujet !
Au final, c'est toi qui devra résoudre ton problème mais il reste tout de même important de signaler le souci aux autorités afin qu'un jour peut-être …
Ben oui, je suis un doux rêveur, on ne se refait pas !

Expliquons ces termes barbares que sont ransomware, mail spoofing et phishing et voyons que faire en cas de coup dur…

Ransomware: traduit par le doux nom de rançongiciel en français, on comprend tout de suite mieux de quoi il s'agit.
C'est un programme qui s'exécute sur votre PC Windows ou Linux, Mac, tablette ou Smartphone parce que vous avez malencontreusement cliqué sur un lien ou une pièce jointe pourris et que votre antivirus et/ou antimalware n'a pas reconnu le danger !
Ce programme va crypter vos fichiers de sorte que vous ne sachiez plus les utiliser et va vous demander de l'argent en échange d'une clé de décryptage qui ne fonctionnera même pas toujours.
Pour se prémunir de cela, il ne faut pas ouvrir de mail bizarre ni cliquer sur des liens douteux et bien maintenir ses antivirus et antimalware à jour.
L'utilisation d'un PC Linux ou d'un Mac est aussi une certaine protection car

Windows ayant la part de marché la plus importante, les pirates développent leurs cochonneries pour Windows.

Si vous deviez être victime d'un ransomware, **déconnectez immédiatement votre PC de l'Internet** (coupez le WIFI, la 3G/4G ou retirez le câble réseau).
Ensuite, utilisez un autre PC pour vous rendre sur **https://www.nomoreransom.org/** (malheureusement en anglais) pour voir si vous pouvez décrypter sans devoir payer; cliquez sur le bouton **YES**, cela vous amène sur un écran où on vous demande deux fichiers encryptés d'exemple et/ou le fichier du pirate qui vous demande la rançon (ou une copie exacte du texte de ce message) que vous aurez copiés de votre PC infecté via une clé USB de préférence.
Cliquez ensuite sur le bouton « **GO! FIND OUT**« , croisez les doigts et , si vous avez du bol, suivez les instructions pour décrypter votre PC (je n'ai pas pu essayer cette partie…).
Si vous n'avez pas de chance, à vous de décider si cela vaut la peine de payer ou pas pour peut-être récupérer vos données.
Dans tous les cas, je vous conseille de **changer tous vos mots de passe** à partir d'un PC « propre » (Un Linux de préférence), de vous rendre dans votre commissariat et de déposer une plainte pour piratage informatique avec une description éventuelle des coûts engendrés.
Si il y a préjudice financier, contactez aussi votre assureur, sait-on jamais (oui, je sais, je suis un doux rêveur)…

Mail Spoofing: utilisation de votre adresse mail à votre insu et donc usurpation d'identité. J'aime à expliquer qu'envoyer un mail via Internet revient à envoyer un courrier dans une enveloppe transparente laissant apparaître en clair toutes les information de votre mail (ainsi que votre message) ce qui permet à un pirate même novice de capturer suffisamment d'information pour pouvoir envoyer un mail en votre nom à vos contacts sans que vous le sachiez… Vous pourriez également recevoir un mail ayant un un aspect véridique de l'un de vos contacts s'étant fait « spoofer »…
Cela semble un peu risible à première vue mais si le pirate s'adresse en votre nom à une autorité officielle (banque, électricité, eau, police, fournisseur Internet, employeur, administration communale ou autres), cela peut vous causer de sérieux soucis. Imaginez aussi que le pirate demande de l'argent en urgence à tous vos contacts parce vous êtes soi-disant en grande difficulté, il y a forcément

des amis ou connaissances qui vont tomber dans le panneau !
Le seul moyen de contrer cela est d'encrypter vos échange de mail mais c'est malheureusement trop compliqué pour le commun des mortels qui n'est en général pas très diplômé en informatique (et même ces diplômés trouvent ça compliqué)… Je vous ferai un article là-dessus un de ces quatre …

Si vous êtes victime de mail spoofing, la première chose à faire est de **changer les mots de passe de tous vos comptes de messagerie** et de **créer une nouvelle adresse mail** (sur Gmail ou Outlook.com par exemple) qui ne sera pas connue du pirate afin de contacter vos correspondants et les prévenir que cette nouvelle adresse est la seule fiable au moins temporairement… Il faudra être très clair dans votre message et fournir, si possible, une preuve irréfutable de votre identité afin que vos contacts fassent confiance à cette nouvelle adresse mail.
Si le même mot de passe que votre messagerie est aussi utilisé pour d'autres comptes (banque, sites d'achats, forums, etc…), il faudra les changer aussi !
Suivant la gravité de ce que le pirate aura envoyé en votre nom, il faudra peut-être aussi aller **porter plainte dans votre commissariat afin de vous mettre à l'abri de plaintes d'autres victimes qui vous prendront pour le pirate !**
Ensuite, il faut **essayer d'isoler les infos du pirate et voir si il est possible de l'éradiquer de vos comptes mail** si il s'en est servi (le pirate pourrait aussi avoir envoyé des mails en votre nom depuis d'autres serveurs que ceux de votre messagerie électronique. Ce travail n'est pas facile à faire et l'aide d'une personne connaissant bien la messagerie électronique sera nécessaire, soit via une connaissance soit via des forums spécialisés (où il ne faudra JAMAIS fournir le mot de passe de votre mail).
Il faut savoir qu'un pirate qui a capturé vos infos mail se dépêche de les revendre un peu partout et vous, ainsi que vos contacts, allez sans doute recevoir sous peu beaucoup plus de mails non-sollicités (spam) qu'auparavant ainsi que subir plus de tentatives d'usurpation.
Dans les cas extrêmes, il vaudra mieux supprimer ces comptes de messagerie et informer vos correspondant de placer les adresses mail correspondantes dans leur filtre anti-spam pour qu'ils ne soient plus non plus importunés.

Phishing: ou hameçonnage en français, consiste à collecter des informations confidentielles et/ou de connexion à vos comptes Internet quels qu'il soient (carte

de crédit, réseaux sociaux, banques, sites de rencontre, serveur mail et j'en passe…) par tous les moyens possibles et imaginables (interception des mails, keylogger, contact téléphonique, etc …). Avec ces infos, un pirate peut agir à votre place sur n'importe lequel de ces comptes ou utiliser par exemple votre compte en banque et/ou cartes de crédit à votre place ! Il s'agit aussi d'une usurpation d'identité.
Ici encore, la meilleure prévention est de ne pas ouvrir de mail louche ni cliquer sur des liens douteux, ni de fournir des infos confidentielles par téléphone, de bien vérifier d'être sur un site sécurisé avant de faire tout paiement via carte de crédit ou de se connecter à sa banque, de ne pas utiliser de mot de passe trop simple ou trop facile à déduire et de bien maintenir ses antivirus et antimalware à jour.

Si vous êtes victime de phishing, il faut **immédiatement contacter l'organisme au nom duquel le pirate vous a demandé des infos (que vous les ayez fournies ou non) !**
Si vous avez fourni les informations demandées il faut en plus bloquer le compte (banque, carte de crédit ou autres) et **changer les mots de passe de tous vos compte en ligne** quels qu'il soit car, trop souvent, le même mot de passe est utilisé pour tous les comptes d'une même personne voire famille.
À nouveau, ne pas hésiter à porter plainte à la police pour vous mettre à l'abri d'autres plaintes qui pourraient être déposées contre vous du fait des agissements du pirate en votre nom.
Phishing et mail spoofing peuvent être combinés et, dans ce cas, il faut appliquer les solutions pour ces deux problèmes.

Même si vous êtes rigoureux et suivez toutes ces recommandations, vous n'êtes évidemment pas 100% à l'abri d'une attaque mais il en va de même dans votre maison ou sur la voie publique, il ne sert donc pas à grand chose de devenir parano… Il est simplement bon de savoir que cela existe et de savoir plus ou moins quoi faire en cas de souci.
Notez aussi que je ne suis pas un spécialiste de la sécurité informatiques et que je n'ai sans doute pas couvert tous les cas de figure dans cet article.

Pour parfaire vos défenses, vous pouvez par exemple utiliser une carte de débit spéciale (et non de crédit) pour faire vos achats en ligne (la poste propose ce service ainsi que de plus en plus de banques), d'utiliser une carte de crédit qui ne soit pas liée directement à votre compte bancaire (en Belgique, on n'est pas

légalement obligé de faire une domiciliation à l'organisme de crédit, on peut toujours exiger de payer par virement, ce qui vous laisse la possibilité de vérifier votre facture **AVANT** de payer).
Dans le même esprit, éviter de payer en ligne avec votre carte de banque (Bancontact, icône de votre banque, etc…) car là, vous exposez directement votre compte en banque !

Pour le mail, il est possible d'obtenir un certificat gratuit renouvelable annuellement qui permet d'encrypter vos messages. Cela demande une gestion de vos destinataires à qui vous devrez fournir d'une manière ou l'autre votre clé publique afin de pouvoir décrypter votre mail. Vous devrez aussi prendre soin de sauvegarder votre clé privée qui permet l'encryption avant l'envoi.
Ce système est assez fastidieux mais permet de garantir votre identité et que votre mail n'ait pas été modifié entre vous et votre correspondant.
Comme dit précédemment, je vous ferai un article là-dessus un de ces quatre jeudis…

Pour les mots de passe, il faut toujours utiliser un mot de passe complexe comprenant lettres minuscules et majuscules, chiffres et caractères spéciaux tout en sachant s'en souvenir facilement sans devoir les noter partout et surtout pas dans un fichier sur votre PC ou alors ce fichier doit être encrypté (par vous-même, pas par un ransomware).
Prudence aussi avec tous ces programmes qui vous proposent de conserver tous vos mots de passe soi-disant à l'abri, même si les auteurs sont de bonne foi, ces programmes sont les cibles privilégiées des pirates et aucun ne peut vous offrir de garantie sérieuse.
Certains sites limite encore la longueur de leur mots de passe à 8 caractères; c'est totalement insuffisant de nos jours et il vaut mieux passer votre chemin…
Avant de taper un mot de passe pour se connecter à un site, toujours bien vérifier que vous êtes sur une page sécurisée c'est-à-dire dans l'adresse commence par « http**s** » et pas « http ». Cette info n'est pas toujours visible et certains navigateurs montrent un cadenas ou un autre signe clair indiquant que la page est sécurisée. Apprenez à connaître votre navigateur sur ce point, c'est impératif et vital… Je vais essayer de faire une page de référence quelque part qui montrera comment chaque navigateur montre cela… Il est dommage que cela ne soit pas standardisé, pas vrai ?
De plus en plus de sites, surtout sensibles évidemment, proposent une

double authentification avec aide à la récupération de mot de passe via SMS; c’est en général une bonne solution mais il faudra penser à adapter/bloquer immédiatement ces comptes si vous vous faites voler ou perdez votre GSM/Smartphone !
Ça, c’était juste pour en rajouter une couche ! :-)

Ouf ! C’est bon, j’ai ma dose, assez pour aujourd’hui !

Li P’ti Fouineu vous salue bien !