VBI – Mémo sécurité

R. Politis – sept 2018

Protection contre le piratage / malware / vol de données

4 mesures de prévention globales :

1. Utiliser les dernières versions mises à jour du système d'exploitation (OS) : Windows 10, MacOS 10.14
2. Utiliser des versions récentes et à jour du navigateur Internet : Chrome, Firefox, Edge, Safari. N'utilisez pas Internet Explorer, qui n'est plus maintenu.
3. Conservez une sauvegarde régulièrement mise à jour de vos données sur un support séparé (disque dur externe), et si possible une image de restauration de l'OS – Windows 10 et Mac OSX ont cette fonction intégrée (pour Windows il faut juste une clé USB de 32Go).
4. Installer un antimalware léger genre **Malwarebytes**. Un antivirus usine à gaz type Norton ou Macafee n'est pas nécessaire, mais le garder si vous l'avez déjà. Préférer les versions payantes, dont le coût est modeste comparé au risque et protègent mieux en temps réel.

4 types d'attaques:

1 : L'intrusion sur votre réseau local depuis Internet

- N'est possible qu'en l'absence de firewall (pare-feu), ou lorsque celui-ci est désactivé. Dans ce cas, tout le réseau local est visible depuis Internet à partir de son adresse IP publique.
- Effets : Comme si on laissait sa maison ouverte 24h sur 24 !
- Prévention :
  - Laisser les firewall actifs ! Aujourd'hui on en a au moins 2 par défaut, un sur la box de l'opérateur et sur les versions récentes de Windows / MaxOS. On peut en ajouter un 3ème en le demandant à son opérateur (Orange par ex.)

2 : Le virus « à l'ancienne » : un programme malveillant s'installe sur l'ordinateur.

- Introduit par l'installation d'un programme par l'utilisateur (téléchargement, pièce jointe, etc.)
  - Dans tous les cas, et à condition que l'OS et le navigateur soient raisonnablement récents, ceci a nécessité la participation active de l'utilisateur et le fait de négliger plusieurs mises en garde : ouverture PUIS exécution d'une pièce jointe, clic sur un lien / bouton dans un site PUIS acceptation de la mise en garde de l'OS, installation d'un programme d'origine inconnue (piraté, téléchargé), PUIS acceptation de l'avertissement de sécurité de Windows / MacOS.
- Actions possibles du logiciel malveillant (par ordre de gravité):
  - Altérations ennuyeuses mais non destructives, en général dans le navigateur : publicités intempestives, changement du moteur de recherche, ralentissements…
  - Inscription dans un Botnet – le PC devient un « zombie » silencieux, on ne s'aperçoit de rien. Il est utilisé dans des réseaux pour des actions illégales : envois de spam, attaques, déni de service.
  - Spyware : Le logiciel ne se manifeste pas, mais récupère vos listes d'adresses, vos contacts, données personnelles, etc. Dans les pires cas, peut récupérer tous vos documents ou enregistrer vos frappes de clavier dans l'espoir de récupérer des Nos de carte de crédit, mots de passe, etc…
  - Ransomware : Blocage de l'ordinateur, ou plus grave cryptage des fichiers contre rançon. Ne jamais payer, les documents ne seront pas restitués – le meilleur remède est la sauvegarde des données.
- Prévention :
  - Ne jamais cliquer sur des pièces jointes exécutables de provenance inconnue.

- Ne jamais installer de programmes piratés ou téléchargés de provenance inconnue. Ne pas dire automatiquement « oui » à toutes les alertes de sécurité de l'OS sans comprendre de quoi il s'agit, et sans être certain que l'action est légitime et sans danger.
- Eviter les sites non sécurisés ou douteux, et surtout sur ces sites ne jamais « accepter » ou télécharger quoi que ce soit, cliquer sur des alertes de sécurité bidon, etc. L'antimalware payant est une bonne protection contre cela, en identifiant les sites à risque en temps réel.

- Lorsque le mal est fait :
  - Si vous êtes certain(e) d'être infecté(e), n'essayez pas de régler le problème vous-même, adressez-vous à une personne compétente. Dans ce cas comme dans d'autres, l'auto-médication fait souvent plus de bien que de mal !

3 : Le piratage de vos comptes chez un tiers : Gmail, Amazon, Yahoo, fournisseur d'accès…

C'est une méthode de vol des contacts et autres données personnelles.

- Le tiers est lui-même piraté et vos données volées parmi d'autres.
  - Remède : Dès que vous êtes averti du piratage, changez le mot de passe de vos comptes.
- Votre compte été compromis individuellement, par la découverte / vol de votre mot de passe.
  - Prévention : Pour les comptes importants, choisissez des mots de passe forts composés de majuscules, minuscules, chiffres, symboles.
  - Remède : Changez votre mot de passe. Si le pirate l'a lui-même changé et que vous n'avez plus accès à votre compte, lancez une procédure de récupération de compte avec le prestataire.

4 : Le « social engineering », ou arnaque transactionnelle

C'est une escroquerie au sens classique du terme (abus de confiance), mais utilisant le support informatique.

- L'arnaque Nigériane : Une personne vient d'hériter d'une immense fortune dans un pays lointain (ce qui lui cause une grande détresse), et comme vous avez l'air honnête vous offre de la partager avec vous si vous l'aidez à sortir l'argent de son pays. No comment…
- L'ami en détresse : un ami issu de votre liste de contacts est en galère dans un pays exotique mais pas trop (genre Montenegro ou Grèce), mais curieusement a accès aux mails pour vous demander de l'argent.
  - Prévention : Ne rien faire !
  - Si vous tenez absolument à contacter la personne, il y a 2 possibilités : soit son compte a été compromis, et le mail vient VRAIMENT de ce compte – dans ce cas l'appeler au téléphone (au moins pour la prévenir !) Soit seule sa liste de contacts a été volée, et dans ce cas le véritable expéditeur n'est pas cette personne. Envoyez-lui un mail à sa bonne adresse.
- Le mail avec pièce jointe : Un mail vous envoyant une facture, un reçu, un remboursement, etc. Vous demande d'ouvrir une PJ, qui est en fait un exécutable (un programme).
  - Prévention : N'ouvrir en PJ que des documents textes (pdf, doc) et des images (jpg), de préférence provenant d'expéditeurs connus. L'OS vous préviendra avec une alerte de sécurité avant de lancer une PJ exécutable, ne l'ignorez pas !
- Le Phishing : Un site contrefait ressemblant à celui de votre banque, d'Ameli, des impôts, de votre fournisseur d'accès, etc vous propose :
  - soit un remboursement d'un montant assez faible pour être crédible, et assez important pour être motivant,
  - soit une action immédiate faute de quoi votre prestation (compte, accès Internet, etc) sera fermé ou interrompu.

  Dans les 2 cas, il faut cliquer sur un lien ou bouton dans le mail, et saisir des données financières : numéro de compte en banque, de carte de crédit, code secret, CVV, nom / prénom, etc
  - Prévention : Jamais vous ne recevrez ce genre de message d'un vrai prestataire, donc évidemment ne rien faire et détruire le mail !
  - Si vous voulez avoir une certitude, laissez le pointeur de la souris sur le lien en question, vous verrez que l'adresse qui s'affiche n'est jamais celle de l'expéditeur supposé.