Le Cahier pratique

SOMMAIRE

L'ARTILLERIE DES PIRATES : VIRUS, VERS ET CHEVAUX DE TROIE

Les pirates disposent d'une large panoplie de logiciels malveillants (malwares). En tête, les **virus.** Ce sont des codes informatiques cachés dans des logiciels, des applications mobiles, des scripts Web ou de simples pièces jointes à des mails. Lorsqu'ils sont exécutés, ces codes infectent vos terminaux et se propagent par les réseaux en utilisant votre carnet de contacts (on parle alors de vers). Ils peuvent détériorer ou détruire vos fichiers personnels. Les **ransomwares,** du type de WannaCry, chiffrent vos données, puis vous réclament de l'argent contre une clé de déchiffrement. Le **cheval de Troie,** lui, ouvre une brèche dans votre ordinateur, qu'un pirate pourra utiliser pour voler vos données, installer des logiciels espions ou prendre le contrôle de la machine.

Bien s'armer contre les attaques informatiques

En mai, le virus WannaCry a fait trembler la planète en infectant les ordinateurs de particuliers et de grandes sociétés. L'occasion de faire le point sur les principales menaces informatiques et les façons de s'en prémunir.

Sébastien Casters

ISTOCK PHOTOS

2 LA TECHNIQUE DE L'HAMEÇONNAGE

L'hameçonnage, ou phishing, consiste à faire livrer ses données personnelles (identifiants de comptes et informations bancaires, par exemple) par la victime elle-même. Il prend souvent la forme de faux courriers électroniques, censés émaner de votre banque, d'administrations (CAF, Pôle Emploi…), de vos services en ligne (opérateur, sites marchands). Ces mails font généralement miroiter des gains financiers et vous invitent à suivre des liens vers de fausses pages Web où on vous incite à saisir vos données bancaires afin de les utiliser. Une technique semblable existe sur les mobiles, où vous pouvez recevoir des SMS ou des appels promettant lots ou promotions. Ils n'ont qu'un but : vous pousser à contacter un numéro fortement surtaxé.

À SAVOIR

Le PC plus menacé que le Mac ?

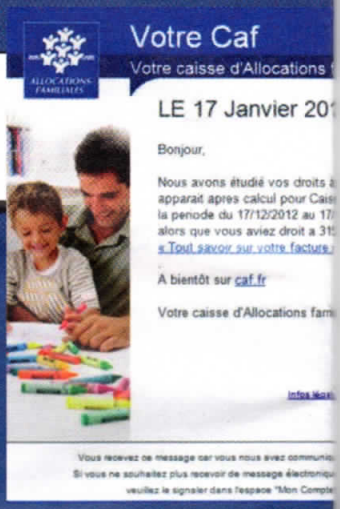
Tous les environnements informatiques ne sont pas égaux face à la menace virale. Les appareils sous Windows sont plus souvent ciblés que les Mac. Parce que Apple contrôle mieux la partie matérielle et logicielle de ses appareils. L'environnement Windows est plus ouvert, ce qui a pour conséquence un parc de machines aux configurations hétérogènes, plus difficile à sécuriser et à maintenir à jour. Windows accaparant aujourd'hui 70 % du marché des ordinateurs, il est statistiquement bien plus rentable pour les pirates de s'attaquer en priorité à cette plateforme. Pour les mêmes raisons, les appareils mobiles Android (80 % des parts de marché) sont plus fragilisés que l'iPhone. Toutefois, si vous suivez nos conseils et si vous êtes prudent, les risques s'équilibrent.

MODE D'EMPLOI

BIEN S'ARMER CONTRE LES ATTAQUES INFORMATIQUES

3 LES MÉTHODES D'INFECTION

Vous pouvez être infecté par le biais d'une clé USB ou d'un CD-Rom, mais la menace vient surtout des réseaux et d'internet. La porte d'entrée principale des virus est votre messagerie. Vous pouvez en attraper en cliquant sur la pièce jointe d'un courrier, d'un SMS ou sur des liens contenus dans des messages de phishing, qui vous demanderont, par exemple, d'installer un faux plug-in (petit logiciel d'extension) pour pouvoir regarder une vidéo ou jouer en ligne. Vous pouvez aussi récupérer des codes malveillants en téléchargeant et en installant des applications ou des jeux gratuits. Cela peut être des copies de logiciels existants et très connus, mais dont le code a été modifié. Les risques sont évidemment plus grands si les programmes proviennent de sites ou de réseaux de téléchargement illégal.



Un phishing ressemble souvent à s'y méprendre à un courrier officiel et est même parfois nominatif.

4 LA PRÉVENTION DES RISQUES

La mesure la plus efficace est de faire appel à votre bon sens. Sans tomber dans la paranoïa, restez toujours en alerte, posez-vous les bonnes questions avant d'ouvrir un mail ou de cliquer sur un lien. D'où provient-il ? Est-ce que je connais son expéditeur ? Est-il de confiance et crédible ? Ai-je vraiment besoin de cliquer ? Vous écarterez ainsi la plupart des menaces. Pour limiter les risques, il est également vital de combler toutes les failles de sécurité que peut comporter votre installation informatique. Cela signifie faire la mise à jour régulière de votre système d'exploitation et de vos logiciels (voir Bon Plan), mais aussi protéger votre réseau wi-fi par une clé d'accès complexe.

5 LES PARADES : ANTIVIRUS ET SAUVEGARDES

Se munir d'un bon antivirus est impératif. Si ces logiciels ne sont pas infaillibles, ils vous permettront de parer les menaces les plus courantes. À condition de les mettre à jour régulièrement, eux aussi. Procurez-vous une suite de sécurité plutôt qu'un simple antivirus. En plus de chasser les virus, ces suites incluent un pare-feu (pour repérer les activités réseau anormales), des outils contre le phishing et de détection des sites potentiellement dangereux… Le risque zéro n'existant pas, pour limiter les conséquences d'une infection, il est vital de faire des sauvegardes régulières (hebdomadaires, a minima) de vos données les plus importantes sur un support amovible que vous débrancherez chaque fois pour qu'il ne soit pas contaminé et/ou sur un service d'hébergement distant et sécurisé (tel le cloud).

8 CONSEILS POUR

Faites les mises à jour

Pour limiter les risques de piratage, comblez les failles de votre configuration en faisant une mise à jour régulière :

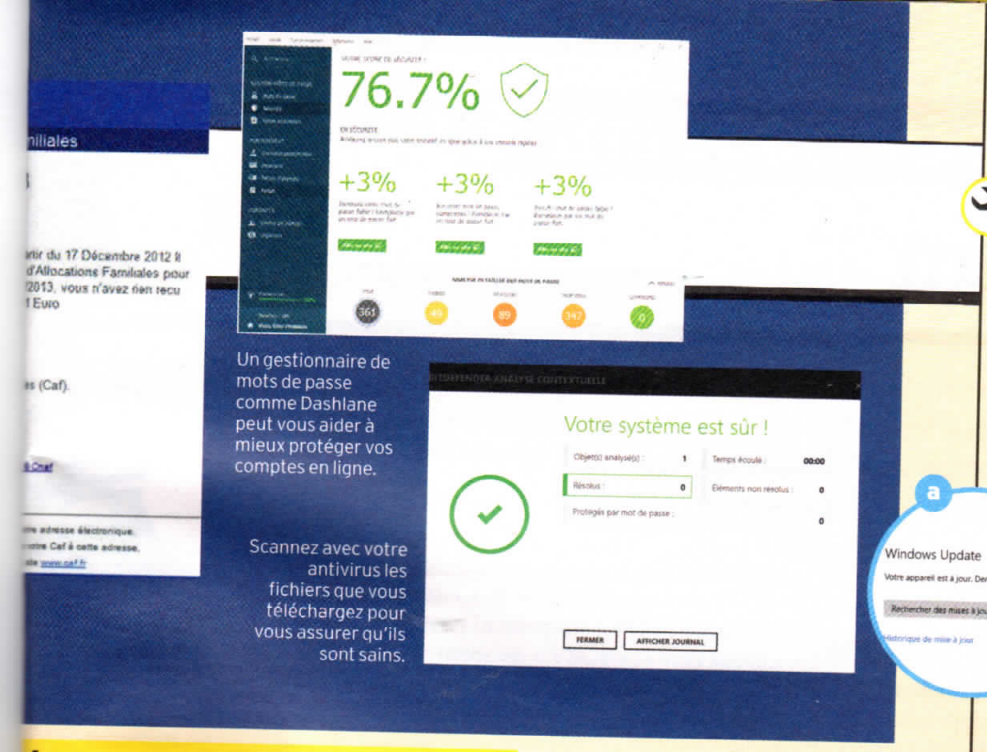
- de votre système d'exploitation (Windows, Mac OS, Android…) ;
- de vos navigateurs ;
- de tous les logiciels que vous avez installés, y compris les pilotes de vos périphériques.

Ne cliquez pas aveuglément sur les pièces jointes

N'ouvrez pas une pièce jointe si elle provient d'un expéditeur inconnu. Prenez garde aux fichiers portant des extensions de type .exe, .bat ou .vbs.

Méfiez-vous de tout le monde !

Soyez suspicieux : si un courrier ou un message sur les réseaux sociaux vous paraît louche, ne l'ouvrez pas et n'y répondez pas sans vous être assuré de son origine. Les adresses mail ou les comptes de réseaux sociaux de



Un gestionnaire de mots de passe comme Dashlane peut vous aider à mieux protéger vos comptes en ligne.

Scannez avec votre antivirus les fichiers que vous téléchargez pour vous assurer qu'ils sont sains.

ÉCARTER LES MENACES

vos amis peuvent, à leur insu, avoir été piratés et propager des vers.

Ne croyez pas au Père Noël

Si vous recevez un mail d'EDF, du fisc ou de votre fournisseur d'accès internet (FAI) vous proposant le remboursement d'un trop-perçu inattendu, méfiez-vous. C'est certainement une arnaque. Si vous avez un doute, contactez directement la société ou l'organisme concerné. Ne cliquez jamais sur les liens contenus dans ces mails.

Ne transmettez jamais vos données bancaires

Aucun service sérieux ne vous demandera de lui communiquer votre numéro de carte bancaire et son cryptogramme par mail ou par un formulaire Web. Si on vous le réclame, c'est forcément une escroquerie.

Sécurisez tous vos mots de passe

Utilisez des mots de passe complexes et différents pour tous vos services. Vous éviterez ainsi de mettre en péril l'ensemble de vos comptes d'un coup si l'un d'eux venait à être piraté (voir *LPP* n° 426, p. 50)

Protégez votre compte administrateur

Sur un PC, le compte administrateur dispose de droits plus élevés qu'un compte utilisateur. Pour limiter les risques, réservez ce compte à la maintenance du PC et utilisez un compte utilisateur simple pour surfer sur le Web. Si le PC est partagé en famille, pensez au contrôle parental pour éviter que vos enfants n'aient accès à des contenus inadaptés.

Ne téléchargez pas n'importe quoi

Lorsque vous téléchargez des applications ou des jeux, faites-le à partir de services ayant pignon sur rue et scannez les fichiers téléchargés à l'aide de votre antivirus avant de les ouvrir. Évitez les sites inconnus et surtout ceux de téléchargement illégal, sur lesquels les applications vérolées sont monnaie courante.

EN PRATIQUE

Mettre à jour votre système vous protège

Les dernières versions de Windows se mettent à jour automatiquement pour tout ce qui concerne la sécurité. Pour être sûr que le système est à jour :

- **sous Windows 10**, tapez *update* dans le menu **RECHERCHER**, puis allez à **PARAMÈTRES** de Windows Update ; a
- **sous Windows 8**, allez au menu **PARAMÈTRES**, puis à la rubrique **MISE À JOUR ET RÉCUPÉRATION** ;
- **sous Windows 7**, cela se passe dans le **PANNEAU DE CONFIGURATION**, puis dans la rubrique **SYSTÈME ET SÉCURITÉ**. b

Microsoft assurera les mises à jour de Windows 7 jusqu'en 2020. Si vous conservez ce système après cette date, ce sera à vos risques et périls. Il est, d'ailleurs, déconseillé de continuer à utiliser des systèmes anciens, comme Vista ou XP, dont la maintenance n'est plus assurée. Pour mettre à jour vos **logiciels et vos navigateurs**, il faut trouver le menu **À PROPOS**, qui se cache, en général, dans les **PRÉFÉRENCES** ou les **PARAMÈTRES** du programme. c Il affiche le numéro de version actuelle du logiciel et les mises à jour disponibles. Afin d'éviter tout oubli, nous vous recommandons d'activer la mise à jour automatique ou la notification de disponibilité de mise à jour, lorsqu'elle est proposée.