Courriels : Les modes d'infection les plus courantes

1.Par courriel : classique mais toujours aussi efficace.

Les criminels à l'origine de vagues de courriels malicieux cherchent, de plus en plus, à diversifier leurs cibles. Ainsi, ce ne sont pas uniquement les utilisateurs de Windows qui sont visés. Ces dernières semaines, on a observé différentes vagues cherchant à distribuer des maliciels et ciblant les utilisateurs de MacOs, le système d'exploitation développé par Apple. Il est important de rappeler que la prudence s'impose pour tous les utilisateurs, quel que soit le système d'exploitation qu'il utilisent.

En matière de courriel, la règle indispensable à retenir, est de ne JAMAIS ouvrir un courriel dont la provenance vous semble suspecte. De plus, aucune entreprise ne vous demandera votre login, mot de passe, code d'accès ou numéro de carte de crédit par courriel.

Ce mode d'infection se présente principalement sous deux formes : **Téléchargement de pièces jointes malveillantes ou Clic sur des liens malveillants inclus dans des courriels.**

Commençons par les pièces jointes malveillantes. Un attaquant envoie un courriel en se faisant passer pour une des entreprises légitimes, telles que les offices fédéraux ou entreprises connues (La Poste, Swisscom, entreprises électriques, etc.). Un fichier malveillant y est joint, sous la forme d'un fichier, d'un document Word ou Excel. Le destinataire ouvre la pièce jointe en pensant que le courriel provient d'une source légitime. Une fois le fichier ouvert la charge utile du virus est automatiquement téléchargée et le processus d'infection du système démarre. Quant aux liens malveillants dans un courriel, il est souhaitable de l'analyser un peu.

Un exemple concret (voir Figure 1) : je reçois un courriel de Swisscom me demandant de sécuriser mon compte suite à une connexion suspecte.

Les liens malveillants contenus dans les e-mails ont le même effet que les pièces jointes malveillantes. Que faire de ce courriel : déplacez-le dans la corbeille puis videz-la.

2. Les virus peuvent aussi se propager en visitant des sites internet malveillants

Chaque jour des centaines de virus apparaissent. Les antivirus traditionnels nécessitent une mise à jour constante de leur base de données. En effet ces antivirus sont incapables de détecter des virus qui ne sont pas encore inscrits dans leur base de données. Les virus sont des codes sophistiqués qui profitent des failles d'un système. Le plus souvent, ils agissent, lorsqu'une victime visite un site Web compromis. Le code malveillant est principalement caché dans une image ou une photo, qui la redirige vers la page de destination du pirate, sans que la victime s'en aperçoive.

3. Comment éviter les dégâts

Installez toutes les mises à jour du système d'exploitation et des programmes. Vous voilà devant votre écran et l'une de ces petites fenêtres s'affiche, vous indiquant, qu'une fois encore, il vous faut mettre à jour votre PC. - Installer et mettre à jour régulièrement les logiciels peut sembler fastidieux mais ignorer ces demandes de mise à jour peut coûter bien plus cher que les quelques minutes qu'elles exigent !

Ces mises à jour ciblent d'importants changements apportés aux programmes, comme la résolution de failles de sécurité et la correction de bogues, ainsi que les dernières fonctionnalités qui améliorent la performance de vos logiciels. Les virus peuvent prendre le contrôle de votre système de différentes façons et apporter toutes sortes de modifications pour le rendre in- utilisable, y compris les disques durs externes connectés à votre ordinateur. Les virus visent tout particulièrement les disques durs de sauvegarde et il est donc très important de les déconnecter de votre PC, où ils sont hors d'atteinte.

Il existe deux options :

Les sauvegardes en ligne utilisent un service sur le cloud, ce qui peut s'avérer une option pratique. Toutefois, l'utilisation de plus en plus fréquente du cloud risque d'augmenter l'intérêt des criminels à trouver de nouvelles failles

Les disques durs externes sont une bonne option, car il est facile de les stocker hors ligne, déconnectés de tout ordinateur et en mettant à jour vos données.


SR
Service Reminder <support@temp.org>
pier-luigi.galli@bluewin.ch
Problème avec votre colis
Ce message a été envoyé avec l'importance Haute.
L'expéditeur est : support@temp.org. A l'évidence, cette adresse courriel n'est pas du domaine de la Poste
SWISS POST
Bonjour
Votre colis n'a pas pu être livré le 25.10.2022, car aucun droit de douane n'a été payé (2,99 CHF). Suivez les instructions
Date d'expédition : 15.08.2022 - 16.08.2022
Référence de la commande : WS31237939
Total à payer: 2,99 CHF
Bénéficiaire : Post CH AG
https://cutt.ly/9noliy1
Cliquez ou appuyez pour suivre le lien.
Pour confirmer l'envoi du votre colis cliquez ici
En survolant le lien avec la souris mais surtout sans cliquer, une petite fenêtre s'ouvre indiquant la vraie destination (on constate que le lien pointe vers un site qui n'est pas celui de la Poste
Vous recevrez un email ou SMS à l'arrivée de votre envoi dans l'adresse domicile. Vous disposerez de 8 jours, à compter de la date de mise à disposition, pour retirer le colis. Au moment du retrait, une pièce d'identité vous sera demandée.
Pour plus de services, retrouvez le suivi de votre envoi en cliquant ici
Nous vous remercions de votre confiance,
Cordialement,
Votre service client Post CH AG.
Cet e-mail est envoyé de façon automatique. Il n'est donc pas possible d'y répondre en retour.
Avec ses 60 000 collaborateurs et collaboratrices, des start-up et des partenaires, la Poste encourage et développe en permanence des solutions axées sur l'avenir et fait avancer de nouveaux modèles c ommerciaux de manière ciblée. Ainsi, elle simplifie le quotidien de ses clients tout en soutenant son activité clé.

Figure 1