Vous pouvez très facilement être hackés

Voici comment

Il n'y a pas besoin d'être un hacker possédant des failles 0day, c'est-à-dire non révélées publiquement, pour vous hacker. En réalité, **n'importe qui peut potentiellement vous pirater**.

Certes, cela ne se fera pas avec la même rapidité et la même chance de réussite, mais la possibilité est bien réelle.

Avec des outils clé en main disponibles sur Internet, tout le monde a désormais la possibilité de le faire. Sans compter le nombre croissant d'articles et de vidéos à ce sujet qui mettent entre des mains inexpérimentées des logiciels très performants.

D'ailleurs, l'âge moyen des hackers au Royaume-Uni est de 17 ans ! Il semblerait qu'ils le deviennent en cherchant tout d'abord sur des forums comment hacker/modder leur jeu vidéo préféré et qu'ils se découvrent ensuite d'autres centres d'intérêt…

Mais, peut-on vraiment appeler cela du hacking ?

> Le hacking avec des logiciels, c'est un peu comme la peinture avec des imprimantes.
>
> — **Hachi, Deep Web**

Quel que soit le nom que l'on lui donnera, que ce soit du "script-kidding" ou du "hacking", **le résultat sera le même** : on aura récupéré vos mots de passe et/ou pris le contrôle de votre machine.

C'est pourquoi dans cet article, **j'aborderai deux grandes manières avec lesquelles vous pouvez vous faire avoir**. Ensuite, je vous raconterai par une **petite histoire personnelle** de hacking que l'on pourrait qualifier de "discount". Enfin, je conclurai sur des **conseils pratiques** et des **ressources complémentaires** pour éviter de vous faire pirater.

1) Le phishing

Le phishing consiste à ce que vous vous connectiez à un site, souvent après une notification urgente reçue par e-mail. Cependant, **ce que vous ne savez pas, c'est que le site sur lequel vous vous trouvez n'est pas le site original** sur lequel vous pensez vous connecter.

En effet, ce n'en est qu'une copie, parfois bien réalisée, parfois mal. En vous connectant dessus, **vous donnez directement votre couple utilisateur + mot de passe à celui qui a créé la fausse page** de connexion.

Quelques exemples de phishing

Récemment, **le mouvement d'Emmanuel Macron a été la cible de phishing** avec les Macron Leaks publiés juste avant la fin du deuxième tour de l'élection présidentielle.

D'après les différents articles à ce sujet, **il semblerait que cette tentative (réussie) ait été prévue** par le mouvement "En Marche !" et que **des faux comptes aient été délibérément créés** avec des documents visant à faire perdre du temps aux hackers.

> Nous avons procédé à une contre-offensive. Nous ne pouvions pas nous prémunir à 100% contre une attaque […] Nous avons créé des faux comptes, avec du faux contenu, en guise de piège. Nous l'avons fait de façon massive, afin de les obliger à tout vérifier, si c'étaient de vrais comptes […] Même si cela ne leur faisait perdre qu'une minute, nous étions contents.
>
> **— Mounir Mahjoubi, responsable numérique d'Emmanuel Macron**

Il n'y donc a pas eu besoin de chercher des failles pour les pirates mais plutôt de **simplement compter sur l'erreur humaine** que feraient quelques personnes négligentes.

Également, une campagne de phishing sur Gmail a été organisée. Elle consistait à demander à l'utilisateur de se connecter à Google Docs via la connexion oauth (C'est par exemple cette connexion que vous utilisez pour les applications sur Facebook).

2) L'accès physique

Vous avez sans doute déjà vu des films dans lesquels le héros (souvent un agent secret) connecte une clé USB sur un ordinateur et attend fébrilement le chargement de son virus/clonage des données alors qu'il est sur le point d'être découvert.

Eh bien, dans la réalité **une attaque par accès physique est en effet très efficace.** Un simple clé USB peut vous introduire un trojan, récupérer ce que vous tapez au clavier (c'est nommé un keylogger) ou simplement votre liste de mots de passe (c'est appelé un stealer).

Par exemple, il y a peu est apparu dans les actualités une histoire de clés USB reçues dans la boîte aux lettres. Les personnes les ayant reçu ont évidemment connecté la clé USB à leur ordinateur, ce qui les a immédiatement infectées.

À propos des stealers

Un stealer se contera de récupérer vos mots de passe et de les envoyer. Mais, **vous n'avez pas forcément besoin de faire tout ça pour vous emparer des mots de passe de la personne**.

En effet, si vous n'avez pas de mot de passe principal protégeant vos mots de passe enregistrés dans votre navigateur, **on peut aisément y accéder**. Il suffit pour ce faire de vous rendre sur l'ordinateur de l'individu une fois qu'il a le dos tourné, d'ouvrir son navigateur et d'**afficher la liste de mots de passe enregistrés dans les paramètres**.

Ainsi, **mettez un mot de passe principal** pour la liste de mots de passe stockée sur votre ordinateur **ou simplement n'en sauvegardez aucun** (Même si avouez que c'est très pratique la complétion automatique…)

Illustration d'une protection utilisée par les professionnels

Il y plusieurs mois, je suis allé faire des photos d'identité chez un photographe. Je voulais en profiter pour récupérer le fichier numérique de la photo afin de l'avoir en haute qualité.

Cependant, **j'étais aussi conscient que si n'importe qui venait avec sa clé USB et demandait cela, il suffirait d'une personne mal intentionnée.** Il suffisait d'un seul individu qui tenterait de mettre un virus sur sa clé pour donner un très mauvais souvenir à ce photographe et l'inciter à refuser ces demandes dans le futur.

J'ai donc tout de même demandé. **Sans demander, on est sûr de ne rien avoir.** Pourtant, l'on est souvent surpris de la réponse positive à des demandes que l'on pensait avoir peu de chance d'acceptation.

Le photographe a pris ma clé et l'a insérée dans une borne qui se trouvait dans la même pièce et me l'a ensuite redonnée.

Voici donc une solution simple pour les professionnels : **éviter le contact direct en utilisant une borne pour le transfert des fichiers.**

3) Petite histoire personnelle de "hacking" discount

Je vais dans cette partie vous conter une petite histoire personnelle mettant en lumière **un hacker "discount"** que l'on pourrait qualifier de script-kiddie.

Un ami (Il est gentil, juste pas très doué) m'avait affirmé être un hacker. **Je l'avais donc immédiatement mis au défi de me pirater** pour vérifier ses dires et si je saurais lui résister. Je vais l'appeler Albert ci-après pour garantir son anonymat.

Albert a donc accepté mon défi et m'a envoyé une application .apk (C'est le fichier permettant d'installer une application sur Android). J'ai immédiatement **décompressé le fichier sur mon ordinateur pour en analyser le code source**. En effet, un fichier .apk est une archive tout comme les fichiers .zip ou .rar

C'était la première fois que je faisais cela, mais j'ai rapidement trouvé ce que je cherchais. Tout d'abord, dans le fichier AndroidManifest.xml (C'est le fichier qui donne les informations principales à propos de l'app), j'ai découvert que **cette "application" demandait un nombre énorme d'autorisations**, une bonne vingtaine !

Pourquoi une application aurait-elle besoin de pouvoir envoyer un SMS, lire notre journal d'appel, accéder à nos photos, à notre micro et bien plus encore ? **C'était déjà très louche.**

Voici donc une recommandation importante lorsque vous installez une application sous Android, que ce soit sur le PlayStore ou téléchargée par une autre source : **Vérifiez les autorisations demandées par l'application avant de l'installer, voire bloquez-les.**

Cela semble fonctionner, j'ai finalement installé l'application sur mon téléphone en mettant toutes les autorisations sur "Rejeter" et mon ami m'a avoué que rien ne fonctionnait dans son "centre de contrôle".

J'ai continué l'exploration de cette apk pour finalement découvrir qu'**Albert avait utilisé Metasploit pour la réaliser** et que… **son adresse IP ainsi que le port utilisé était écrit en clair** dans l'un des fichiers !

Après, je suis très loin d'être un expert (C'était même la première fois que je décompressais une apk), mais **théoriquement enlever toutes les autorisations est suffisant**. Si vous avez des exemples de cas où cela ne suffirait pas, n'hésitez pas à me les donner dans les commentaires, que cela soit profitable à tous.

4) Conclusion et pour aller plus loin

En conclusion, et comme dit en programmation :

> Ne faites jamais confiance à l'utilisateur.

Partez du principe que **tout ce que l'on vous envoie**, que ce soient des mails, des liens ou même une simple clé USB **est potentiellement dangereux et infecté**.

Pour lever cette indétermination, **vous pouvez utiliser une machine virtuelle** pour les ouvrir sans risque (Mais cela ne vous protégera pas du phishing, seulement des virus. **Aucun logiciel ne peut vous protéger de votre négligence.**)

Vous pouvez également envisager d'autres solutions comme celle de la **borne pour les clés USB**.

Pour tenter de lutter contre le phishing, **regardez attentivement l'URL de la page** sur laquelle vous vous trouvez. Plus généralement, ne cliquez pas sur les liens douteux et prenez aussi garde à **l'adresse e-mail** qui les envoie.

Par exemple, l'adresse *penetral@muscularly.e164.dissuasiveness.navfpjgx.us* se fait passer pour Lidl dans un e-mail. On voit très clairement que ce message n'est pas crédible au vu de l'adresse utilisée. (J'ai pris le premier exemple venu d'un message directement arrivé dans mes Spams)

Pour aller plus loin dans la sécurisation de vos ordinateurs, je ne peux que vous conseiller des lire les deux tomes (gratuits) du **guide d'autodéfense numérique** :

Tome 1 – Hors connexions

Tome 2 – En ligne

J'ai également réalisé une synthèse PDF sur la protection et l'anonymat informatique. Vous pouvez la télécharger ici.

Est-ce que vous vous êtes déjà fait avoir par l'une des techniques présentées dans cet article ? Si oui, lesquelles ? Si non, quelles sont les mesures que vous utilisez pour vous protéger au mieux ?