7 Secrets Sur Le Hacking

Disclaimer :

Le site web Le Blog Du Hacker dont ce document est issu publie des informations en ligne ***dans le but d'apprendre la sécurité informatique*** *uniquement. Ces informations ne sont en aucun cas destinées à d'autres fins que la sécurité informatique dans le cadre privé et ne doivent pas être considérées* comme des conseils légaux ou professionnels*. L'utilisateur s'engage à utiliser ces informations sous son entière responsabilité et dégage l'éditeur de toute responsabilité à cet égard.*

Les termes « hacker » et « pirate » sont souvent ***confondus*** *(même volontairement), mais un « hacker éthique » qui apprend pour se défendre en toute légalité n'a rien à voir avec le pirate (« hacker malveillant ») qui cause des dommages à autrui.*

Sommaire

1. Un pirate n'est pas nécessairement un génie en informatique

Si l'on peut se permettre de définir des « vrais » hackers, on parlera généralement de **professionnels certifiés en sécurité informatique** dont le métier consiste à trouver des failles dans les systèmes et à les **sécuriser**. On appelle ces personnes des « hackers éthiques ».

On qualifiera également de « certifiés » les hackers simplement reconnus dans les communautés pour leurs exploits.

Ces hackers certifiés ne constituent qu'un **très faible pourcentage** des hackers dans le monde. En conséquence, **ce ne sont pas eux** qui viennent vous pirater ! Il faudrait de ce fait appeler les pirates des « **pirates** » et non pas des « hackers » dans le sens éthique du terme.

L'expansion des méthodes ***RAD*** (*Rapid Application Development*) a beaucoup favorisé la création très **rapide** de programmes **malveillants** puissants. Maintenant, n'importe quel internaute disposant d'un manuel et d'un environnement de développement intégré peut **programmer des logiciels puissants sans connaissances spéciales**.

De plus, les codes sources de logiciels espions et autres programmes malveillants sont trouvables sur la toile assez facilement et sans débourser un centime.

Cela va même plus loin, les programmes tous faits eux-mêmes sont souvent distribués et orientés tout public.

Attention : Si cela vous tenterait, sachez que les programmes que vous téléchargez en pensant pouvoir pirater votre cible sont souvent **eux-mêmes infectés**. L'arroseur arrosé en quelque sorte.

On a également inventé le terme « *script-kiddy* » (« gamin qui utilise les scripts » en français) pour désigner ce genre de pirates qui utilisent simplement des programmes trouvés ici et là, se faisant passer pour les créateurs originaux.

Au sein des communautés de Hacking, un niveau de compétence intermédiaire à élevé est **demandé**, **apprécié et reconnu**. Le hacking étant bien plus que de savoir utiliser un programme après avoir lu son mode d'emploi.

2. Utiliser Google vous permet de trouver énormément d'informations

N'importe qui peut se faire passer pour un professionnel dans un domaine très précis peu importe lequel en sachant simplement **trouver** les informations au bon endroit et au bon moment.

On appelle communément **Doxing** (*Documents Tracing*) le fait de collecter des informations sur un individu ou une société.

Le célèbre moteur de recherche *Google* permet de trouver énormément d'informations très précises. Mais beaucoup d'internautes n'utilisent pas tout le **potentiel** de *Google*.

Parmi les expressions les plus puissantes de Google il y a les doubles guillemets: "*EXPRESSION*"

Entourer une expression de ces guillemets permet de chercher les pages qui contiennent **exactement** cette expression, et non pas des mots-clés ou pages similaires.

Vous devinez donc ce qui s'affiche en tapant : "Votre mot de passe est"

La deuxième expression utile est l'astérisque : *

C'est le caractère joker signifiant pour Google « tous les mots ».

Ainsi l'expression « Votre mot de passe * » fonctionnera de la même manière que dans le premier exemple.

La troisième expression permet d'éliminer un mot clé de la recherche.

Il s'agit du tiret (-) à placer juste avant le mot clé à retirer :

« Wordpress version -4.0.2 » vous assure donc que les résultats retournés ne seront **pas** liés à la version 4.0.2 de WordPress.

Vous pouvez également utiliser les mots clés spéciaux comme :

inurl:EXPRESSION

intitle:EXPRESSION

Le premier cas permet de rechercher un mot clé dans une **URL** et le deuxième cas permet de rechercher dans le **titre** d'une page.

Plus d'informations sur l'article complet dédié à ce sujet :

http://www.leblogduhacker.fr/google-hacking/

3. Celui (ou celle) qui vous pirate vous connaît dans 90% des cas et vous en veut

On ne pirate que **très rarement un compte pour le plaisir** sachant notamment les conséquences qui peuvent s'en suivre.

Il y a de fortes chances qu'une personne de votre entourage proche ou éloigné **soit à l'origine d'un piratage de votre compte**.

Loin de moi l'idée d'accuser qui que ce soit, mais la preuve est là, **90%** des demandes de piratage qui me sont directement adressées sont liées à des histoires de **couples et de travail**. À ce propos, je refuse toutes les demandes de piratage qui me sont adressées, Le Blog Du Hacker n'est pas un site de piratage à la demande.

Nous sommes tous minuscules sur *Internet*, et nous sommes souvent que des « utilisateurs normaux », c'est-à-dire des utilisateurs sans importance pour les grandes organisations de cyberterroristes.

Un pirate donné **n'a pas beaucoup raisons** de vous pirater, il ne s'en prend pas aux particuliers mais plutôt aux gouvernements et aux **entreprises**, si déjà l'idée de causer des dommages ou d'obtenir un gain financier conséquent lui vient à l'esprit.

Attention cela ne signifie pas non plus que vous êtes entièrement à l'abri d'un piratage massif et non ciblé.

Il y a bien sûr des possibilités de se faire pirater si par exemple le site sur lequel vous êtes inscrit(e) se fait lui-même **pirater**. Une base de données dans de mauvaises mains peut effectivement représenter un danger pour tous les utilisateurs.

Il est également possible que vous soyez victime de *phishing* qui peut viser des personnes aléatoires.

Point important : la personne qui vous pirate de son plein grès, si elle vous connaît, est généralement débutante et fait des erreurs, il est donc aussi facile de la **reconnaître**.

Gardez donc les programmes téléchargés et les virus en quarantaine. Ils peuvent servir à **retracer** le hacker.

Plus d'informations et de statistiques ici :

http://www.leblogduhacker.fr/la-peur-des-hackers/

4. Vous pouvez vous faire pirater en cliquant sur un lien anodin, ou là où vous ne pensiez jamais vous faire pirater

Un piratage réussi repose souvent sur la **ruse**.

Rappelez-vous des fameux e-mails de *phishing* vous disant que vous avez **gagné au loto**, ou des sites web vous félicitant d'être le 1 000 000e visiteur.

Ces méthodes sont maintenant **bien connues**, mais le principe est resté le même et **beaucoup de personnes cliquent encore** sur des liens et téléchargent des programmes **par peur ou par manque de sensibilisation**.

Pourquoi par peur ?

Car, en guise d'exemple, des fenêtres **très semblables** aux fenêtres de *Windows* (entre autres) s'affichent vous informant que votre ordinateur contient des virus.

Les personnes à l'origine de ces pièges proposent ensuite des solutions tout-en-un pour **supprimer** ces virus **virtuels**.

En téléchargeant leur antivirus, vous **vous faites pirater** et vous ne vous en rendez même pas compte, vous êtes simplement content(e) car tous les virus de votre ordinateur auront à ce moment **miraculeusement** disparu, sans même avoir été présents.

Plus d'informations en ligne à cette adresse :

http://www.leblogduhacker.fr/attention-votre-ordinateur-est-infecte/

Un autre point concerne les programmes malveillants cachés soit dans des programmes sains, soit dans des sites sains.

Pour obtenir des scénarios et des moyens de prévention je vous conseille les articles suivants :

http://www.leblogduhacker.fr/un-antivirus-ca-sert-a-rien/

http://www.leblogduhacker.fr/hacker-en-visitant-site-java-drive-by/

Les nouvelles technologies donnent également des nouvelles pistes pour les créateurs de programmes malveillants.

Même avec toutes ces mises en garde, il n'est pas non plus question de devenir paranoïaque, mais au moins **méfiant**.

5. Vous ne savez pas toujours que vous êtes piraté(e), car l'antivirus ne lance pas toujours l'alerte

À partir du moment où votre antivirus sonne, c'est qu'un virus a été **trouvé et n'a pas été exécuté** (même chose pour un site web malveillant).

Cela veut dire qu'effectivement votre antivirus fait du bon travail, mais ça ne certifie absolument **pas qu'il n'y ait aucun autre virus** sur l'ordinateur.

Un autre programme malveillant peut très bien fonctionner discrètement sur le PC **depuis des mois sans se faire repérer**.

Cela ne certifie pas non plus que le programme détecté n'a jamais été exécuté auparavant avant de se faire repérer.

Cela est possible car un programme malveillant peut être **crypté afin de le rendre indétectable** par les antivirus.

Il est également possible de trouver la **signature** du virus à la main et de la changer sans altérer le fonctionnement du programme.

La plupart du temps, le pirate prendra soin de rendre son programme indétectable avant de le déployer, ce qui rend donc les antivirus partiellement inutiles.

Et même si à la longue l'antivirus finit par détecter le virus, c'est bien souvent **trop tard**.

Ne vous fiez donc pas aveuglément à votre antivirus en téléchargeant n'importe quel programme car vous ne serez pas nécessairement protégé(e) à 100%.

Souvenez-vous également que les sites de *phishing* sont difficilement détectés, ils paraissent totalement **légitimes** et fonctionnent aussi bien sous Mac, Linux, Windows et sur les systèmes d'exploitation mobiles.

Plus d'informations via cet article en ligne :

http://www.leblogduhacker.fr/pourquoi-les-anti-virus-ne-sont-pas-vos-amis/

6. Vous pouvez potentiellement retrouver le propriétaire d'un logiciel malveillant

Je disais plus haut que le responsable du piratage de l'un de vos comptes est généralement **une personne que vous connaissez, et qui est potentiellement débutante**.

Vous pouvez facilement en avoir le cœur net si cette personne n'est pas très à l'aise en piratage.

Effectivement, il est possible de dé-compiler un programme malveillant comme n'importe quel autre programme.

On peut souvent dans le cas des *keyloggers* trouver **l'adresse e-mail** et **le mot de passe** du pirate dans le code source de son programme.

Cela est possible car le pirate doit fournir ces informations pour faire fonctionner son programme et donc pour **recevoir les fichiers de logs dans sa boite mail**.

Des identifiants comme les mots de passe *FTP* ou d'autres services peuvent bien entendu être trouvés.

Gardez donc toujours un historique des sites visités et programmes téléchargés, notamment ceux qui sont **suspects**.

Car si un jour vous devenez victime de piratage, vous pourriez toujours au moins essayer de pister le hacker qui vous en veut.

Pour dé-compiler un programme, la méthode est plutôt simple, il suffit de télécharger un programme dédié (*.NET Reflector*) et de dé-compiler le programme malveillant en question.

.NET Reflector permet de récupérer les codes sources des programmes de la **famille dotnet** (.NET) c'est-à-dire crées avec *Visual Basic .NET* et *C#,* entre autres.

Les keyloggers basiques et autres programmes malveillants sont souvent programmés avec l'un de ces deux langages, il y a donc de grandes chances que **la technique fonctionne**.

Plus d'informations pour pister un hacker :

http://www.leblogduhacker.fr/comment-pister-un-hacker/

7. Le piratage permet potentiellement de gagner beaucoup d'argent, mais un pirate finit souvent par être repéré ou arrêté

Vous connaissez probablement les groupes de hacking célèbres tels que *Anonymous* et *Lulzsec.* Ils sont censés refléter les meilleurs « hackers » et ceux qui ont le plus d'influence mais ils se font prendre un par un.

Prenez également le cas du piratage du *Sony Playstation Network*, le responsable de l'attaque **a aussi été pris**.

La découverte de l'agence de surveillance NSA (*National Security Agency*) prouve que nous pouvons être espionnés un peu partout à notre **insu**.

Les plus grandes entreprises ont donné leur accord pour fournir à la *NSA* les informations qu'elle voudrait obtenir, au besoin.

Le fameux réseau TOR permettant de surfer « anonymement » a aussi été infiltré par des agents du FBI. Il y a eu plusieurs arrestations de propriétaires de sites illégaux du « deep web ».

Voici l'article qui en parle :

http://www.leblogduhacker.fr/tor-garantit-pas-lanonymat/

Pirater un système ou un utilisateur est risqué, vous prenez ce risque en effectuant des actions malveillantes peu importe votre lieu d'habitation.

Vous ne faites donc pas le poids face aux stratagèmes perfectionnés de la « cyber police », ne jouez pas les super héros ou assumez les **conséquences**.

De plus, *Facebook*, *Google* ou encore *Microsoft* **payent les hackers pour trouver des failles dans leurs systèmes et les signaler**.

Gagner de l'argent en « piratant » légalement n'est-il pas une meilleure idée ?

Voici l'article à ce sujet :

http://www.leblogduhacker.fr/gagner-de-largent-en-piratant/

Ce document vous a plu ?
Apprenez-en maintenant encore plus avec le guide Comment Devenir Un Hacker :

Social Engineering, Failles web, failles réseau, failles applicatives, principes de sécurité, etc.

Vous saurez-tout sur les hackers éthiques, et vous en deviendrez un.

Mais aussi :

Les 5 erreurs les plus communes des débutants en hacking
Ce qu'il faut maitriser avant de commencer le hacking
Top 6 des erreurs en sécurité informatique que vous ne devez plus faire
Être anonyme sur Internet
et bien d'autres !

Le Blog du Hacker

Ce qui est sécurisé à 99% n'est pas sécurisé