REMISE AU POINT SUR LE HACKING

Le terme « Hacking » est flou pour le grand public, car souvent orienté vers le péjoratif. Cet automatisme, certainement dû à l'influence que les médias ont sur le point de vue du grand public sur le hacking. Il ne faut pas faire d'amalgame et s'écarter de la définition originale, pour pouvoir comprendre la définition exacte de cette notion. En effet, le « hacking » définit « l'art et la manière de modifier un élément physique ou virtuel de sorte que celui-ci n'ait pas le comportement prévu initialement par ses créateurs ».

On peut illustrer cette définition, en dehors du domaine de l'informatique, en se référant à la vie de tous les jours. En effet, on peut considérer que démarrer une voiture sans utiliser la clé de contact de celle-ci peut être considérée comme du hacking, dans son sens le plus large. Dans le domaine de l'informatique, le terme de hacking définit ceux qui utilisent leurs connaissances pour exploiter des failles dans des environnements distincts, afin d'effectuer des modifications entrainant une attitude différente de celle que l'auteur a prévu, dans le but d'en tirer avantages. On peut délimiter la catégorie des hackers informatiques en deux grandes familles, comme deux cotés d'une même pièce :

D'un côté, on va trouver ceux que l'on appelle les « Black Hat ». Cette partie des hackers est responsable de l'image péjorative et disons-le, criminelle, du hacking. Ces personnes exploitent ces failles dans le but de nuire aux personnes physiques ou morales visées par ces attaques. Elles peuvent être avoir différents buts, comme récupérer des informations confidentielles ou voler de l'argent.

Des exemples mis en avant par les médias tels que le vol de 10.000.000 $ à la CityBank de New York par le russe Vladimir LEVIN en 1994, ou, plus récemment, en 2008, par le vol de 245.000.000 € à la société DASSAULT par un hacker grec, ont permis de mettre en avant ses hackers de l'ombre, faisant d'eux des modèles pour leurs pairs, mais surtout en instaurant un climat de peur et d'insécurité, en présentant une nouvelle forme de criminalité, capable de s'immiscer directement au sein d'un foyer, en passant par un ordinateur, une tablette ou un Smartphone.

Cependant, il existe également, comme à toute chose, son opposée, les « White Hat ». Très peu connu du grand public, ils représentent l'autre coté de la pièce. Ce sont des hackers qui vont agir pour le bien commun : Hacker étique ou expert en sécurité, ces personnes mettent à profit leurs connaissances au profit de la préservation de la vie privée et de la sécurité des personnes connectés. Il est important de noter que certains « black hat » ce sont détournés de leur voie de criminelles, et travaillent aujourd'hui dans la sécurité informatique, étant donnée qu'ils sont les plus à mêmes de comprendre la logique de leur ancien pair. Alors que cette notion paraissait simple, une troisième catégorie est également apparue, un mélange entre ces deux catégories, les « Grey Hat ».

Cette troisième catégorie désigne ceux qui mettent à contribution des techniques de « Black Hat » telles que l'intrusion ou la détection de faille de sécurité, tout en gardant l'éthique morale des « White Hat ». Contrairement à son homologue « Black Hat », celui-ci va utiliser ces failles de sécurité pour permettre aux créateurs du logiciel ou site de combler cette faille, publiant l'existence de cette faille et, souvent, comment y remédier. Cela a donné des situations quelques peu complexes, comme récemment le cas de Sony, qui a attaqué les hackers qui publier ces articles, entrainant la naissance d'un conflit avec cette communauté.

Aujourd'hui, certains « Grey Hat » se sont regroupés en fonction des idéologies qu'ils défendaient, ce qui a donné naissance à une nouvelle identité de ce groupe, les Hacktiviste, mettant à profit leur compétence dans le but de lutter pour une cause ou une idéologie. Un de ces groupes s'est fait connaitre dans le monde entier à la suite de leurs actions pour la protection de la liberté d'expression et l'expression de la vérité, Le clan des Anonymous.

Une fois cette notion de hacking définie et délimitée, on peut se tourner vers les méthodes de hack les plus utilisées dans le but de comprendre comment le hack peut avoir lieu, et ainsi optimiser ses chances de s'en prévenir.

Tout d'abord, le clickjacking ou « détournement de clic ». C'est une technique qui consiste à créer un site transparent, sous la forme d'un script, qui se place par-dessus le site visité par un utilisateur. En effet, le visiteur pensant naviguer paisiblement sur son site préféré, ne pourra se rendre compte que chacun de ses clicks sur cette page sera récupérée par ce script malveillant (à noter que ces types d'attaques sont indétectables par les antivirus ou autres programme de nettoyage). L'utilité pour les hackers d'utiliser cette méthode sera de pouvoir utiliser ces clicks pour obtenir différentes informations ou procéder à des actions malveillantes tels que la modification de compte, le vol de mot de passe ou l'activation de la webcam (particulièrement intrusive).

Une des méthodes utilisables pour lutter contre ce type d'attaque est l'utilisation de l'addon NoScript qui permet de laisser l'ensemble des scripts activés tout en gardant un œil sur ceux-ci, permettant de détecter la présence d'un script malveillant. A noter que Facebook a été victime de clickjacking en 2015.

Ils ont réglé le problème rapidement mais l'attaque a quand même fait des dégâts. Le clickjacking est souvent assimilé à ce que l'on appelle une « faille de redirection » qui consiste en la redirection d'une URL vers une autre, permettant ainsi à une personne malveillante de diriger un utilisateur vers un site piégé, sans que celui-ci ne puisse s'en rendre compte. Cette faille est exploitée notamment dans le but d'initier des attaques par phishing.

Le phishing, ou hameçonnage, est une technique consistant en l'envoi d'email frauduleux, permettant ainsi de récupérer des mots de passes, des numéros de comptes bancaires, et bien d'autres informations confidentielles. Ce type d'attaque est possiblement identifiable avec un œil avisé. On peut se concentrer sur le contenu de l'email, proposant de récupérer un prix pour un concours inventé de toute pièce, des fautes d'orthographes ou des différences de présentation par rapport au site copié, ainsi qu'un lien cliquable dans l'email, redirigeant le visiteur sur un site piégé. L'utilisation de logiciels de sécurité est également un bon moyen de se prévenir de ces attaques.

D'autres types d'attaque peuvent également être évités grâce à l'utilisation de logiciel de sécurité, notamment, le malware. Il va s'agir ici d'un logiciel espion qui va s'installer sur un ordinateur, tablette ou Smartphone, dont la mission principale sera de voler des informations personnelles ou de l'argent. La plupart des antivirus tels qu'Avast ou MalwareBytes sont d'efficaces protections contre ce type d'attaque.

Malheureusement, les logiciels de sécurité ne peuvent pas protéger nos informations confidentielles de tous les types d'attaques. L'un de ces attaques est le Ramsomware. Il s'agit ici d'un logiciel malveillant qui « prend en otages » des données, en les chiffrant pour les rendre inaccessible par l'utilisateur, et exige une rançon contre la restitution de ces données. Sous cet air d'attaque imparable, cette technique peut être facilement contrée en utilisant des fonctions de restauration du système d'exploitation, par le biais de disque de sauvegarde. Cette méthode est proposée dans la quasi-totalité des supports informatiques.

Il est important de noter qu'il ne s'agit ici que de quelques techniques parmi toute celle qui existent, mais on peut les considérer comme plus essentielle à connaitre puisqu'elle concerne la vie de tous les jours et l'utilisateur que peut faire le grand public ou une entreprise d'un ordinateur, tablette ou Smartphone.

Au vue de la vulnérabilité des utilisateurs face à ces différents types d'attaques, on peut penser que la solution pourrait venir de nouveaux programmes de sécurités plus performants, de nouveaux outils surpuissants pour protéger nos données ou même la mise en place de milices informatiques ; mais la réalité peut être tout autre. La raison de l'efficacité de ses attaques réside dans le manque de formation des utilisateurs quant à l'utilisation de leurs ordinateurs, tablettes ou Smartphone, et à la navigation en toute sécurité. La solution peut donc venir d'une formation, dès la scolarité, pour que l'on apprenne aux utilisateurs et futurs utilisateurs à correctement utiliser ces outils afin de surfer tranquillement sur internet, avec un comportement responsable. Enfin, une méthode particulièrement efficace pour se prémunir contre ses attaques consiste en l'investissement dans un bloc note au format papier, dans lequel on peut facilement inscrire ses mots de passes ou données confidentielles, sans risque de hacking.

« L'Humanité doit apprendre à se responsabiliser, sinon elle court à sa perte »