

# Le Hacking



M1 Information Communication, option NPJ  
- Promo 2012-2013 // ICOM, Université  
Lumière Lyon 2

*Par Blaise Fayolle, Mathilde Régis, Wildried  
Devillers, Pauline Bouveau*

# 1<sup>ère</sup> partie : les premiers pas du hacking

Lorsqu'on parle de « pirate », on ne pense pas forcément aux “pirates du net”. Pourtant, ils sont bien présents dans le monde entier, et, en terme de hacking, ils n'en sont pas à leur coup d'essai. On va s'intéresser ici plutôt au Hacking et donc aux hackers, de leur naissance, jusqu'à la démocratisation d'Internet (avec des grandes figures du hacking). Nous allons pour cela recenser les différents types de hackers, comprendre leurs intentions et leur fonctionnement, mais également nous intéresser aux techniques qu'ils utilisent. Il sera également intéressant de nous pencher sur le côté législatif relatif au hacking en France et aux USA.

- **Qu'est-ce que le Hacking ?**

Selon John Drapper, considéré comme le père du hacking, c'est “l'art de savoir et de pouvoir modifier un programme, une machine, de façon à ce qu'il fasse ce que vous voulez qu'il fasse et non ce pour quoi il a été conçu.”

Un hacker est alors une personne qui recherche la maîtrise totale des outils qu'il utilise - ordinateurs, logiciels, téléphones ou autres-, pour en comprendre le fonctionnement profond et qui n'hésite pas à le modifier pour l'adapter à ses besoins.

## 1- Les origines : Le Tech Model Railroad club

En 1959 leTech Model Railroad Club (TMRC), une association d'étudiants du MIT possédant comme son nom l'indique une maquette avec des trains électriques.

Pour la faire fonctionner, ils détournent la technologie de composants électroniques, dédiés par exemple à la téléphonie, et utilise le terme de hacking pour définir leurs actions

Quelques années plus tard, le MIT se munit de son premier ordinateur. Les membre du TMRC s'y intéressent et essayent de lui faire faire de nouvelles tâches, en créant de nouveaux programmes par exemple. Ils transposent leur mentalité de hacker a l'informatique.C'est le début du Hacking.

- **L'éthique du hacking**

L'éthique du hacking a été créé au MIT. C'est grâce à Steven Levy, un journaliste spécialisé dans le domaine de l'informatique, que l'idée a été vraiment diffusée.

Il publie un livre dans lequel il met en avant 6 règles de l'éthique du hacker :

Dans son livre ***Hackers : Heroes of the Computer Revolution***, publié en 1984.

L'auteur de l'éthique du hack moderne invite à ne plus regarder le hacker comme étant uniquement « un étudiant imaginaire et audacieux » ou « un spécialiste en informatique », mais à étendre cette vision du hacker à l'ensemble de la société et même à la « planète ».

- L'accès aux ordinateurs - et à tout ce qui peut nous apprendre comment le monde marche vraiment - devrait être illimité et total.

- L'information devrait être libre et gratuite.
- Méfiez-vous de l'autorité. Encouragez la décentralisation.
- Les hackers devraient être jugés selon leurs œuvres, et non selon des critères qu'ils jugent factices comme la position, l'âge, la nationalité ou les diplômes.
- On peut créer l'art et la beauté sur un ordinateur.
- Les ordinateurs sont faits pour changer la vie.

## 2- Phreaking/ blue box

Dans la pensée commune le hacking commence avec l'intrusion dans les systèmes informatiques, en réalité les premiers hackers sont des gens qui se sont introduits dans le réseau téléphonique.

En 1957, Joe Engressia trouve le moyen de passer des appels gratuitement grâce en d'un simple sifflement.

Il se rend compte qu'en sifflant dans le récepteur du téléphone, la sonorité reproduite permettait de signaler au serveur téléphonique que la ligne qu'il utilise est libre et qu'il a raccroché alors que ce n'est pas le cas.

La légende urbaine veut que ce soit John Draper aka Captain Crunch qui découvre cette technique en 1969 grâce à un simple sifflet trouvé dans un paquet de céréale.

C'est la naissance du phreaking, une contraction de phone et de freak.

Pour simplifier son utilisation et être plus performant, Captain Crunch fabrique un petit boîtier qui émet ce son correspondant à la fréquence 2600 hz : la bluebox

Grâce a cet outil, la pratique du phreaking se démocratise et s'étend aux États-Unis et dans le reste du monde.

Le réseau téléphonique devient pour les phreakers une sorte de réseau social, où ils organisent des conférences téléphonique, échange sur leurs pratiques,...

Mais c'est surtout un nouveau terrain d'exploration pour les hackers en soif de découvertes et d'accès à l'information. Ces derniers parviennent à s'immiscer dans n'importe quels réseaux, en dupant les compagnies de téléphone.

Ce sont les premiers à avoir développé une sensibilité et une démarche propre au hacker informatique

En 1971, un article de Ron Rosenbaum publiés dans esquire met fin à l'age d'or des phreakers, avec cet article tout le monde veut se munir d'une bluebox, le réseau téléphonique est envahi.

## 3- Législation à l'époque

Des agents spécialisés de la compagnie de téléphone se rendent chez les hackers pour faire pression sur leurs parents (beaucoup sont mineurs à l'époque). Beaucoup d'avertissements

de ce type sont réalisés. Les hackers désignent ces agents en les appelant M. Duffy Il rend visite aux hackers pour les menacer (la dissuasion fonctionne pendant quelques temps)

En parallèle, l'Etat américain prend des mesures informelles pour punir les hackers. La possession d'une Bluebox peut conduire jusqu'à 2 ans de prison. Captain Crunch est inculpé par le FBI pour fraude électronique, il passe 4 mois en prison. C'est la peine la plus lourde parmi les hackers puisque Captain Crunch est considéré comme le pilier du système.

#### **4- Le Home Brew Computer Club et l'arrivée des ordinateurs personnels**

Révolution dans le monde de l'informatique et développés par des entreprises mais également par des hackers, les PC sont apparus quand la dimension et les coûts de production ont été suffisamment réduits pour en permettre l'accès au grand public.

Les premiers ordinateurs accessibles au public sont disponibles en kit (Alter 8800) que l'on peut assembler chez soi, une aubaine pour les bidouilleurs en tout genre.

En 1975 un groupe de passionnés d'informatique et des micro-ordinateurs se forme : c'est la création du Home Brew Computer Club,

Ils se retrouvent pour la première fois pour parler du Alter MITS et réfléchissent à de nouvelles manières d'utiliser les ordinateurs.

Le groupe se retrouve tous les quinze jours pour discuter technique de programmation, de fabrication, ils partagent leurs connaissances, leurs programmes.

L'échange d'information est primordial au sein du groupe, il y a une sorte de fierté de faire part de ses découvertes, de ses avancées. La mentalité du hacker commence à prendre forme traduit par une importance du partage et de l'accès total à l'information.

Elie F. décrit d'ailleurs le Home Brew Computer Club comme un repère de hackers avec un partage total d'information.

L'apparition des PC attire une génération de hacker passionné par l'accès à une technologie informatique qu'ils peuvent enfin maîtrisée, transformée,...

Ils se mettent donc à fabriquer leurs propres ordinateurs, expérimentent de nouvelles techniques

Avec ces expérimentations, l'informatique connaît de réelles avancées, on pensera notamment à Steve Vozniak le co-fondateur d'Apple (membre du HBCC)

Certains composants et programmes des ordinateurs ont pour source les hackers.

#### **5- Le chaos computer club (CCC)**

'Le Chaos Computer Club e. V. (CCC) est la plus grande association de pirates de d'Europe. Depuis plus de trente ans, nous fournissons des informations sur des problèmes techniques et sociétaux, comme la surveillance, la vie privée, la liberté d'information, le hacktivism, la sécurité des données et d'autres sujets autour de la technologie et des questions de piratage'

Fondé en 1981, il rassemble poignée de hackers passionnées par les réseaux informatiques et la programmation. Ces derniers militent pour une liberté de l'information totale et étudient la répercussion de la technologie sur la société.

Ils portent également un regard critique sur la concentration des informations dans un même système ou sur le net. Comme par exemple la concentration d'informations sur les différentes plates-formes de la Galaxie Google : Drive, répertoire, boîte mail, Google +,...

Une réunion annuelle est organisée depuis 1984 entre Noël et le nouvel an, le 'Chaos Communication Congress'

Ils s'attachent à mettre en évidence les failles des systèmes de sécurité des entreprises et des administrations

Leur action la plus connue est sûrement le 'BTX-hack' : en 1984 le CCC détourne 135.000 DM sur le compte en banque de la caisse d'épargne de Hambourg qui utilisait le protocole BTX proclamé inviolable. Le lendemain, ils rendent la somme dans son intégralité et montrent les failles de ce système de sécurité.

Les médias et la justice critiquent cette action qu'ils jugent illégale alors que le CCC agit dans une logique totalement désintéressée.

En 2006 : Le CCC publie un rapport dans lequel il montre qu'il est facile de manipuler les ordinateurs utilisés pour les élections. Le rapport est sérieusement pris en compte par la cour constitutionnelle fédérale qui se penche sur le problème. depuis plusieurs municipalités ont renoncé à utiliser ces ordinateurs.

Le Home Brew Computer Club et le Chaos Computer Club, bien que très réputé dans le monde informatique ne sont que deux groupes de hacker parmi tant d'autres. Aujourd'hui il existe une multitude de groupes dont on ignore même l'existence.

## **2ème partie : La démocratisation d'Internet**

La démocratisation d'Internet dans les pays occidentaux des années 2000 donne aux hackers un bien plus grand terrain d'expérimentation.

## **1- Une communauté de hackers**

Les compétences se sont transmises et continuent à se transmettre :

On trouve de nombreuses conférences annuelles sur le hacking. Depuis 1992, la Defcon réunit les hackers à Las Vegas. La conférence black Hat précède la Defcon depuis 1997 et rassemble officiellement des experts des agences gouvernementales américaines et des industries, américaine ou non, avec les hackers les plus respectés de "l'underground". En Europe, des conférences ont lieu depuis 2000, et il existe le très réputé Hackfest au Québec.

On trouve désormais des magazines spécialisés sur le Hacking. Le plus connu est "2600", un trimestriel qui explique comment infiltrer, modifier, ou neutraliser des applications et des réseaux informatiques à l'aide de procédés technologiques ou d'ingénierie sociale.

Sur le réseau, on trouve évidemment de nombreux forums de discussion en ligne, et des logiciels malveillants automatisant la découverte et l'exploitation de vulnérabilités informatiques sont désormais disponible sur le marché.

Un peu partout dans le monde, se créent des écoles de hacking.

## **2- La formation de hackers professionnels**

En France, l'Université de Valenciennes forme des anti pirates, des "hacker éthiques", depuis 2008 dans le cadre d'une licence professionnelle CDAISI (collaborateur pour la défense et l'anti-intrusion des systèmes informatiques). Les élèves y apprennent les techniques des pirates car pour eux, il est indispensable d'avoir les moyens de défense basés sur les méthodes utilisées par les attaquants. C'est donc de la protection informatique dans une forme offensive, mais utilisée dans un but bienveillant. Pour éviter toute dérive, la promotion est placée sous la surveillance de la DCRI (Direction centrale du renseignement intérieur) et un avocat spécialisé suit constamment les travaux des élèves. C'est apparemment un secteur professionnel qui embauche puisque 100% des étudiants diplômés ont trouvé rapidement un emploi.

### **Chez les hackers, on trouve différents niveaux d'expériences:**

On appelle les "script kiddies" les débutants qui ne disposent que de connaissances rudimentaires – voire inexistantes – sur les langages de programmation qui constituent l'architecture d'internet et des applications informatiques. Ils doivent recourir à des applications malveillantes conçues par des pirates beaucoup plus expérimentés qui automatisent la découverte et l'exploitation des vulnérabilités.

Le “Super utilisateur”, un terme utilisé par le juriste Paul Ohm pour désigner la figure mythique du pirate omnipotent capable de s’introduire sans peine dans les systèmes les plus sécurisés et de les manipuler à sa guise. Cette figure mythique a largement été alimenté par la culture de masse (personnages de films, séries ...)

Le “Pirate entrepreneur” est celui qui s’affranchit des considérations de prestige et mobilise de manière très instrumentale une expertise technique qui lui permet de générer des revenus criminels de la manière la plus efficace possible, utilisant indifféremment des logiciels prêts à l’emploi ou des scripts « sur mesure ».

- **Quelques techniques de hacking :**

### **Sniffing**

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d’informations (trafic). Mais, il est toujours possible qu’une personne malveillante récupère ce trafic. Elle peut alors l’analyser et y trouver des informations sensibles.

### **Le scanning**

Il consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanner. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C’est un outil très utile pour les hackers. Cela leur permet de connaître les points faibles d’une machine et ainsi de savoir par où ils peuvent attaquer. D’autant plus que les scanners ont évolué. Aujourd’hui, ils peuvent déterminer le système d’exploitation et les applications associées aux ports.

### **Le “social engineering”**

Ce sont des techniques d’intrusions sur un système qui repose sur les points faibles des personnes qui sont en relation avec un système informatique plutôt que sur le logiciel. Le but est de piéger les gens en leur faisant révéler un mot de passe ou toute autre information qui pourrait compromettre la sécurité du système informatique.

Le piège classique est de se faire passer pour un technicien et de demander le mot de passe, par téléphone ou via un faux mail de quelqu’un de légitime (feignant une urgence ou des travaux d’administration du système). Il peut aussi s’agir de deviner le mot de passe d’un utilisateur en recherchant des informations sur lui disponibles sur le Web (prénom des enfants, date de naissance, etc...).

### 3- Les intentions des hackers

#### Les Black Hat

On appelle les "Black Hat" les hackers qui violent la sécurité informatique pour des raisons malveillantes ou des gains personnels.

Voici un exemple relativement récent : C'était en janvier 2008, Un pirate grec de 58 ans est arrêté par la police locale. Il a été arrêté pour s'être introduit illégalement dans les serveurs de Dassault Systèmes et avoir volé un logiciel qu'il a ensuite revendu sur Internet.

C'est donc en s'introduisant dans les serveurs de Dassault que ce hacker de 58 ans a pu obtenir un accès à tout le réseau de l'entreprise. Il lui a alors été facile de dérober plusieurs documents, notamment un logiciel de modélisation destiné aux professionnels. Il avait évidemment pensé à effacer ses traces avant de quitter le réseau.

Il s'est ensuite occupé de revendre ce logiciel, ce qui a causé des pertes estimées par Dassault à plus de 245 millions d'euros. Il effectuait cette revente sur Internet avec l'aide d'un complice, dont l'identité n'a pas été révélée, mais qui résidait au Royaume-Uni. Il a été arrêté à son domicile d'Athènes par la police, qui a perquisitionné chez lui 16 CD et DVD, ainsi que son disque dur.

Donc on voit très bien ici l'exemple d'un hacker malveillant, un black hat, qui a voulu gagner de l'argent en piratant des informations.

#### Les White Hat

Les "White Hat" sont les hackers qui ont des raisons bienveillantes, et testent les systèmes de sécurité dans le but de les améliorer. Leur but est de détecter les failles d'un réseau avant que des malfaisants ne s'y engouffrent.

On appelle ça le Hacking "éthique", les techniques sont sensiblement les mêmes, seul l'intention sépare les White Hat des Black Hat. Les techniques sont similaires à celles des black hat.

#### → Exemple des entreprises qui recrutent des hackers white hat :

Les entreprises sont désormais amenées à travailler avec des hackers pour plus de sécurité. Elles vont même jusqu'à en recruter afin qu'ils puissent mettre leur expertise à profit.

En effet, les technologies liées à Internet se développent sans cesse, et beaucoup d'entreprises font preuve de plus en plus de vigilance afin de sécuriser au maximum leurs données. Certaines d'entre elles sont de très bonnes cibles pour les black hat qui souhaiteraient accéder à des données confidentielles. Recruter un white hat est donc une bonne solution pour faire face au problème. Il pourra savoir, comment un de ses confrères essaierait de s'introduire dans le système informatique de l'entreprise. Il saura alors mieux que n'importe qui où trouver les failles du système.



Et tout cela se fait en toute légalité, puisque ces derniers sont mandatés par leurs clients pour réaliser ces tests d'intrusion dans les systèmes informatiques. Ils se rangent donc du côté des "white hat", les gentils hackers, ceux qui ont de bonnes intentions. Il faut tout de même faire preuve de vigilance et le hacker doit gagner petit à petit la confiance de son client.

Ces hackers sont pour la plupart autodidactes, contrairement à des ingénieurs informaticiens qui ont suivi un enseignement technique donnant lieu à un diplôme.

La DGSE (Direction générale de la sécurité extérieure) par exemple, ainsi que l'Agence nationale de la sécurité des systèmes d'information, ont recruté beaucoup de hackers afin d'assurer la défense de données ultraconfidentielles.

On distingue aussi les **Grey hat**, ces hackers qu'on ne peut pas vraiment catégoriser. Par exemple : un hacker qui taille dans un système informatique pour notifier à l'administrateur que le système a un défaut de sécurité mais qui moyenne des honoraires pour le corriger.

**L'Hactivisme** consiste à aller chercher au-delà du hack technologique pour comprendre-et hacker- les processus politiques. Un exemple récent est celui de Telecomix, un groupe décentralisé d'activistes du net engagé en faveur de la liberté d'expression. En 2011, ils avaient détourné les connexions au web syrien et redirigé les internautes vers une page qui contenait des instructions permettant de contourner la censure du régime.

Le groupe d'hacktiviste le plus connu est le groupe des Anonymous, ces internautes agissent de manière anonyme dans un but particulier et généralement en faveur de la liberté d'expression sur Internet.

Les attaques qu'ils utilisent le plus sont les attaques par **déni de service, les DoS**. Il s'agit d'une attaque contre un site ou un réseau qui cherche à le rendre inopérant en le saturant de requêtes d'information qui dépassent sa capacité de traitement, ce qui l'empêche de répondre aux requêtes légitimes et le déconnecte de l'Internet.

## La législation aujourd'hui

### 1) En France

Selon le code pénal (article 323-1), « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de 2 ans d'emprisonnement et de 30 000 euros d'amende. »

Pour la législation française, le hacker est donc directement considéré comme un pirate, puisque sans attendre l'agissement du hacker sur le programme ou l'utilisation que celui-ci va faire des données, il est déjà hors-la-loi.

Le terme de système de traitement automatisé représente la totalité des systèmes informatiques

(ex :les ordinateurs, les logiciels, les systèmes d'exploitation) ainsi que les réseaux de télécommunications (ex : le réseau internet, les réseaux de télévision ou encore les réseaux téléphoniques).

Toujours selon l'article 323-1, « lorsque l'intrusion dans le système de traitement automatisé a eu pour conséquence de supprimer ou de modifier frauduleusement les données qu'il contient, la sanction peut aller jusqu'à cinq ans d'emprisonnement et de 75 000 euros d'amende ».

La législation française punit sévèrement la suppression de données ce qui peut apparaître normal, mais quant à la modification, il existe une ambiguïté. En effet, comme nous l'avons vu, les hackers ont souvent modifié des programmes informatiques en vue de les améliorer et ainsi faire évoluer la technologie. La loi française, en punissant ces hackers, se prive peut être de nouvelles avancées.

Enfin, des peines supplémentaires peuvent être appliquées, comme la saisie du matériel informatique utilisé par le pirate lors de son infraction. Il faut aussi noter que le pirate s'expose, en plus des sanctions pénales (amende ou peine de prison), à certaines sanctions civiles : il doit par exemple indemniser ses « victimes » selon le préjudice qu'il a engendré.

(Sources : site de la SCP Henri LECLERC & associés, cabinet d'avocats inscrit au Barreau de Paris depuis 1972, avec la compétence en matière de droit de l'informatique, de droit des nouvelles technologies, de droit à la protection des données personnelles et de la vie privée)

## **2) Aux Etats-Unis**

Aux Etats-Unis, pays d'origine du hacking, la législation est comparable à celle de la France. Le piratage informatique relève des lois fédérales. C'est donc le FBI qui se charge de faire respecter ces lois. Le hacking, comme toute autre forme de piratage sur internet est puni par la cour fédérale d'une peine de 5 ans d'emprisonnement et 250 000 dollars d'amende (maximum).

Top 5: Les plus grands pirates condamnés

Il existe une multitude de hackers. Beaucoup passent à travers les mailles du filet. Mais certains se font attraper, et pour eux, les peines sont lourdes.

### **Number 5 : Jonathan James**

Entre le 23 aout et le 27 octobre 1999, il s'introduit dans différents systèmes dont celui du département de défense américaine. Il a alors seulement 16 ans. Il pirate la NASA, en brisant le mot de passe du serveur gouvernemental. Ceci lui donne libre accès au réseau de

la NASA, il en profite pour récupérer le code source secret-défense d'une base spatiale. La valeur des fichiers est évaluée à près de 1,7 millions de dollars.

Il est condamné le 21 septembre 2000. Étant mineur il échappe à la prison. Il est assigné à résidence pendant 6 mois. Il doit également rédiger une lettre d'excuse à la Nasa et au département de défense. S'il avait été majeur ceci aurait pu lui coûter 10 ans de prison.

Source : Wikipédia

Number 4 : **Robert Tappan Morris** (26 juillet 1989)

Étudiant diplômé d'Harvard, il est l'auteur du premier « ver » informatique, un programme qui s'occupe de faire le travail à la place du hacker. Le ver est un logiciel malveillant qui se reproduit sur différents ordinateurs en utilisant le réseau internet. Il utilise les ressources de l'ordinateur et cherche à espionner les données de l'ordinateur, ouvrir une brèche pour les pirates, détruire des données ou saturer un réseau. Avec son premier virus informatique, Robert Tappan Morris a infecté des milliers de machines en seulement quelques heures. Selon un calcul du FBI, entre 100 000 et 10 millions de dollars de données ont été perdues à cause de ce ver.

Il écope de 400 heures de travaux d'intérêt général et une amende de 10 050 dollars, en 1990, pour l'intrusion non-autorisée aux ordinateurs fédéraux.

Source : <http://www.findingdulcinea.com>, encyclopédie informatique

Number 3 : **Albert Gonzalez**

A 25 ans, alors qu'il est employé par les services secrets américains pour 75 000 dollars par ans, il continue ses activités illégales en parallèle. Il monte une opération baptisée « get rich or die trying ». Il repère les enseignes les plus riches au monde dans le magazine Fortune. Ensuite, il arpente les rues de Miami et repère les communications sans fil non sécurisées avec un logiciel renifleur (technique du sniffing). Il intercepte ensuite les données échangées entre les terminaux de paiement et les caisses enregistreuses des enseignes. Il obtient ainsi les numéros de carte de crédit des clients. Au total, il se procure 130 millions de numéros de carte bancaires. Le préjudice s'élève à 250 millions de dollars.

Le 25 mars 2010, il est condamné à 20 ans de prison, la peine la plus lourde pour un hacker.

Source : L'évolution du piratage informatique : De la curiosité technique au crime par soustraction

Benoit Dupont (Chaire de recherche du Canada en sécurité, identité et technologie - Université de Montréal)

Number 2 : **Gary Mckinnon**

Responsable du « Plus grand piratage informatique militaire de tous les temps » selon le gouvernement américain. Alors qu'il est au chômage, cet administrateur système britannique s'introduit dans près de 100 ordinateurs de la Nasa, du pentagone et de l'US Army. Il se défendra en arguant qu'il cherchait juste à établir l'existence de vaisseaux extraterrestres. Il cause 700 à 800 000 dollars de dommages.

Poursuivi et arrêté sur la base des lois informatiques britanniques en 2002, il est finalement relâché faute de preuves. Il est de nouveau arrêté en 2005 et relâché sous caution et conditions (notamment le fait qu'il n'a plus le droit d'accéder à internet. Les Etats-Unis cherchent à l'extrader. Dans ce cas, il risque 70 ans de prison. Mais après plusieurs recours, le premier ministre britannique refuse son extradition en 2009 pour raisons de santé.

Source: Wikipédia

#### And Number 1: **Kevin Mitnick**

Premier hacker à figurer dans la liste des 10 personnes les plus recherchées par le FBI aux Etats-Unis. Il commence son œuvre en entrant dans la centrale téléphonique de Pacific Bell en 1980. Il détourne les lignes téléphoniques à titre personnel. N'ayant que 17 ans à l'époque, il est condamné à 3 mois de rétention dans un centre de redressement pour mineurs et une année de mise à l'épreuve. En 1983, il s'introduit dans l'Arpanet et accède aux données du département de la défense. Il écope de 6 mois de détention dans un centre pour jeunes. En 1987, il est de nouveau arrêté et mis à l'épreuve durant 3 ans pour vol de logiciel et utilisation illégale de cartes de crédits. Mais il continue son activité. Il cherche à s'introduire dans un laboratoire de recherche de Palo Alto pour obtenir le code source d'un logiciel d'exploitation. Pour cette attaque, Mitnick doit purger un an de prison et suivre un programme pour réduire sa dépendance à l'informatique.

On retrouve Kevin Mitnick en 1992. Alors qu'il semble s'être racheté une conduite, Le hacker fait l'objet de poursuite pour usage illégal de système de données. Le FBI se rend à son domicile mais il a disparu. Les fédéraux mettent plus de 2 ans à le retrouver. Mitnick a toujours un temps d'avance sur le FBI. Finalement, le 15 février 1995, Mitnick est arrêté à Raleigh par le FBI aidé de Tsotomu Shimomura, un hacker rival de Mitnick. Il est condamné à 5 ans de prison, à l'époque la peine la plus lourde pour un hacker, 1,5 millions de dollars de dédommagement et 10 millions de dollars de frais de procédure.

Source : Wikipédia

## **Conclusion**

Nous pouvons donc conclure cet exposé en mettant en avant le fait que les hackers originels ont laissé la place à une foule énorme de hackers. Parmi ces derniers, certains agissent de façon malveillante, d'autres pour faire entendre ou défendre une opinion ou un idéal. Actuellement, le contrôle de la technologie est un véritable enjeu politique et les hackers en sont probablement la clé.