Cinq générations de criminels

17 Mars 2023

claude@lemarson.com
https://www.lemarson.com

Sommaire

Sécurité du TI : les générations de criminels

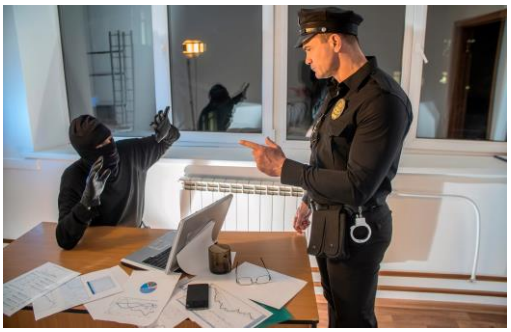
- *Hackers et criminels, attention aux mots*
- *Les grandes familles de hackers et leurs motivations*
- *Des chapeaux de couleur… une autre classification*
- *Jobs et Wojniak auraient pu mal tourner*
- *La pouponnière : les "script kiddies"*
- *Quelques personnages célèbres : Poulsen, Levin, Morris, Mitnick, McKinnon…*
- *Terrorisme et religion : des organisations redoutables*
- *Les femmes et le "hacking" : peu nombreuses mais efficaces*
- *Les hackers les plus bêtes du monde*
- *En résumé, 3 grandes familles*

En 2020 (Verizon), 86 % des attaques avaient une finalité financière

Criminels et hackers

Attention aux mots : ils ont un sens

- Hacking : vient de l'anglais hack (pirater, connotation d'astuce, de "bidouillage").
- Un "hacker" est un virtuose susceptible d'intervenir dans tous les domaines du TI, sans intention belliqueuse manifeste : codage, matériels et jeux d'instructions, administration système, protections sécuritaires… mais aussi dans d'autres domaines que l'informatique.
- L'idée est de comprendre les systèmes complexes, d'en "faire le tour" et de les utiliser en dehors des fonctions prévues.
- Les spécialistes de la maintenance "mainframes" étaient des hackers, obligés de comprendre la complexité des systèmes pour les pénétrer et les réparer.
- Le terme est né en 1959, proposé par un groupe d'étudiants du MIT.
- Crime et criminels : différences de compréhension
  - Anglo-saxons : le criminel est celui qui commet un délit, quel qu'il soit.
  - Francophones : le crime est associé au meurtre et à l'assassinat.

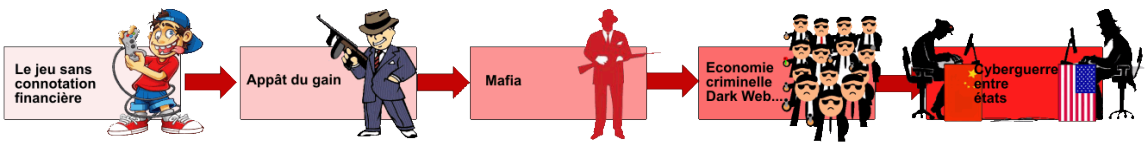


Qualifier un individu de criminel n'est pas nécessairement "très" péjoratif… D'où l'admiration que certaines leur témoignent.

Des jeux à la cyberguerre

Les générations de criminels, ces inconnus…

- La première génération a débuté avec le premier virus de Robert Morris. On s'amuse.
- La deuxième génération est celle de la recherche du profit. Avec des initiatives individuelles.
- La troisième génération est celle des organisations criminelles de la finance, mafias…
- La quatrième génération (actuelle) est celle de l'économie cybercriminelle, un véritable marché de services ("dark web").
- La cinquième génération est celle de la cyberguerre entre les états, mais aussi celle des terroristes et espions.



Les motivations courantes

- Sentiment d'impunité : on peut tout se permettre
- Gains financiers en volumes
- Gains financiers d'opportunité : "il n'y a qu'à se baisser…"
- Motivations politiques ("hacktivisme") : pour manipuler les élections, déstabiliser les états, interférer dans les économies…
  - Vol de données
  - Blocages (DDoS)
- Espionnage "corporate" :
  - Récupérer et vendre des secrets industriels
  - Nuire à l'économie en s'attaquant aux "majors"
  - Voler des fichiers clients
  - Détourner des stratégies industrielles (ex du nucléaire actuellement)
  - Vol de tout ce qui est sensible
- Besoins de reconnaissance et de réputation
  - Dans l'entreprise
  - Vis-à-vis de l'entourage : plutôt les jeunes générations
- Revanche personnelle
  - Anciens employés (plus de 5 % des attaques)
- Moyen détourné pour acquérir des compétences.
- Le défi : très masculin comme approche.
- Sadisme, sans raison particulière, autre que "pourrir" la vie des concitoyens
- Les Saint-Just du hacking : référence à la pureté, ils attaquent ceux qui attaquent !
- La bêtise… particulièrement répandue dans ces milieux.
- Extension des jeux vidéos : certains hackers ne font plus la différence entre le réel et le virtuel.
- Motivations philosophiques : éthique, religieuse, les plus incontrôlables.

Louis Antoine de Saint-Just

Une autre manière de distinguer les adversaires

- Les « **Black Hats** » sont les « crackers », ceux qui détruisent : les terroristes et les maffieux. Leurs objectifs sont clairs et ils possèdent une grande compétence.
- Les « **White Hats** » sont les hackers éthiques. Ils protègent les actifs de l'entreprise, que l'on pourra déployer en deux familles, « reds » ou « blues ».
  - Ce sont les « gentils », qui mettent leur technicité au service de l'entreprise.
- Les « **Gray Hats** » sont une sorte d'intermédiaire entre les black et white hats. Ils ne cherchent pas à gagner de l'argent, ni à détruire la société, mais s'intéressent au sujet.
  - Pourront constituer un vivier utile, car ils sont généralement brillants et compétents. L'ennui, c'est qu'en général, ils le savent…
- Les « **Green Hats** » sont des « Black Hats » incompétents, ceux qui posent des questions idiotes, auxquelles les vrais hackers répondent avec parcimonie et mépris.
- Le « **Red Hat** » est le Rambo de la sécurité, celui qui croit qu'il mettra fin aux activité des « black Hats », seul et sans armes.
  - Pour bien comprendre la dangerosité des malwares, il les télécharge et les incorpore dans son propre système, oubliant au passage, qu'il est connecté au reste du système d'information…
  - Il arrive que l'un de ces « Red Hats » fasse plier un hacker maladroit. Mais c'est en général au prix de 100 000 machines bloquées et de 3 millions $ de pertes de production.
- Le « **Blue Hat** » est une sorte de « script kiddie », pas plus compétent, mais animé d'un désir de vengeance inassouvi. Il n'a aucun désir d'apprendre.

Steve Jobs et Steve Wojniak, déjà…

- L'étrange parcours des deux Steve, fondateurs d'Apple, Wozniak et Jobs, qui rappelons-le, ont commencé leur carrière en tant que hackers en fournissant illégalement des « Blue Box » pour pénétrer les systèmes téléphoniques longue distance et éviter à leurs "clients" de payer les communications.
- Wozniak était connu sous le pseudo de « Berkeley Blue » et Jobs se cachait derrière un certain « Oaf Tobar ».
- Steve Wozniak avait été exclu lors de sa première année de collège à l'Université de Colorado » pour faits de hacking sur les machines de l'institution. C'était bien parti…
- Le dispositif "Blue Box" de pénétration des systèmes téléphoniques, était un générateur d'impulsions électroniques (« phreaker ») pour effectuer des appels longue distance, qui pouvait aussi se transformer en mini centrale opérateur, pour router les communications.
- Le « Blue Box » est exposé au « Computer History Museum » à Mountain View : quand le crime devient preuve de "savoir faire"… On finit par en être fier…

Wozniak s'est permis d'appeler le Vatican avec la "Blue Box", de demander le Pape et de se faire passer pour Henry Kissinger…

La pouponnière du hacking

- Tranche d'âge de 5 à 12 ans !
- « script kiddies » : enfants capables d'écrire des bouts de scripts et de profiter des faiblesses béantes du TI.
  - Motivation : s'attaquer au monde des adultes, par bravade.
  - Généralement sans intérêt financier, au-delà d'un complément d'argent de poche indument gagné.
- Paul Reuben montre à 10 ans comment voler les données, messages et contacts d'un téléphone Android.
- Betsy Davis, n'a eu besoin à 7 ans que d'un simple tutoriel pour hacker un réseau Wi-Fi public, dont elle a mis en évidence les faiblesses.
- Kristoffer Von Hassel trouve, dès 5 ans, un moyen pour entrer dans une Xbox. Microsoft le récompense par une prime de 50 $, le don de quatre jeux et un abonnement gratuit à "Xbox live" dans le Cloud. Tout en le plaçant dans sa liste officielle des chercheurs spécialisés en sécurité…
- CyFi, pseudonyme derrière lequel se cache une jeune personne de 10 ans, connue pour ses capacités à modifier le scénario du jeu en ligne FarmVille, etc.

Kevin Mitnick, la référence

- Kevin Mitnick est une sorte de totem, le hacker "au grand cœur" qui a fait amende honorable…
- Sauf que :
  - En 1980, Mitnick a 17 ans : il pénètre le central téléphonique COSOS de Pacific Bell, vole des mots de passe, des combinaisons de fermetures de portes…
  - Il est accusé (pas prouvé) d'avoir intégré en 1979 les services de la North American Air Defense Command (NORAD).
  - Autres intrusions chez Motorola, Fujitsu et Nokia.
- Le premier hacker à figurer dans la liste des 10 fugitifs les plus recherchés par le FBI.
- Arrêté, il est condamné à 5 ans de prison.

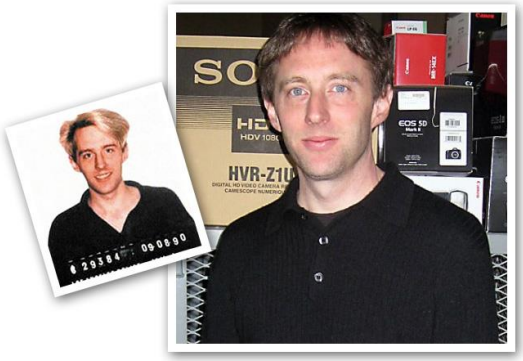
Kevin Mitnick aurait été pris comme modèle pour le film "wargames"

Robert Trapan Morris : le premier ver

- Une tentative qui a mal tourné…
- Etudiant à Cornell (1988)
- Son idée : écrire un programme qui se démultiplie sans aide !!!
- Malchance : des erreurs de code le rendent dangereux
- Les machines "infectées" sont inutilisables
- Les dégâts sont estimés entre 10 et 100 millions $
- Morris est condamné à 3 ans de probatoire (pas d'incarcération), 10.000 $ et quelques centaines d'heures de travaux d'intérêt général

Kevin Poulsen : interdiction de PC !

- Se fait connaître pour avoir pénétré à 17 ans le réseau de l'université de Californie, puis ceux de l'armée de terre américaine et de la compagnie téléphonique Pacific Bell.
- Devient célèbre surtout pour être entré dans le TI d'une radio de Los Angeles, à l'occasion de l'un de ses concours, dont le gros lot était une Porsche.
- Il fallait pour le gagner être le 102 ème appelant, ce qu'il effectue grâce à un code spécifique.
- Le FBI l'intercepte et le condamne à 5 ans de prison.
- Il lui est interdit de se "servir d'un ordinateur" pendant 3 ans…



Matthew Bevan et Richard Pryce

Le sentiment d'invulnérabilité

Richard Pryce et Matthew Bevan

- Le syndrome du délire et du sentiment de surpuissance.
- Ont failli déclencher une troisième guerre mondiale en 1996.
- Ils piratent plusieurs réseaux militaires à travers le monde, notamment aux États-Unis et en Corée du Sud et envoient des documents confidentiels à des pays ennemis.
- Leurs cibles : base de Griffiss Air Force, la "Defence Information System Agency", la NASA et le Korean Atomic Research Institute (KARI).
- Ils ont assuré être à la recherche de preuves de l'existence d'une vie extraterrestre… Evidemment !
- Le plus étonnant : l'inconscience absolue de ces hackers, qui ne se rendent pas compte de ce qu'ils font…

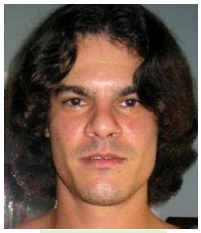
Garry McKinnon : la honte suprême

- L'écossais Gary McKinnon (Solo) a pénétré 97 ordinateurs appartenant aux principales agences militaires américaines et à la NASA, pour enquêter sur des affaires secrètes et les OVNIS.
- Il agit depuis Londres, détruit de nombreuses ressources et laisse un message explicite :
  - "votre système de sécurité est à chier. Je suis Solo. Je vais continuer de le détruire à ses plus hauts niveaux".
- Coût estimé des intrusions : 700 000 $.
- McKinnon étant britannique, le Gouvernement américain a réclamé son extradition qui a toujours été refusée.
- Il a purgé toutefois une peine de 3 ans au Royaume Uni.
- McKinnon bénéficie de nombreux soutiens : Sting, Peter Gabriel, David Gilmour et les "Pink Floyd" enregistrent "change the world" en son honneur.

Et, il n'y a pas qu'eux...

- Adrian Lamo, autiste très brillant, avait modifié un article de Reuters, en glissant une « fake new » qu'il avait attribuée à l' « Atorney General » John Ashcroft.
- Jonathan James : infiltre la NASA et la Défense Nationale à 15 ans.
  - Il vole pour 1,7 million $ de données, dont les informations importantes pour la survie de l'équipage d'une station spatiale (contrôle de température et d'humidité).
  - La NASA doit fermer son accès pendant 20 jours.
  - Vu son âge, il écope de 6 mois d'assignation à résidence et de l'obligation d'écrire des lettres d'excuse à la NASA et au DOD.
  - En 2007, suite à l'attaque contre le TGX, il crain de ne pouvoir se dédouaner et se suicide.
- Albert Gonzalez est accusé d'avoir volé et revendu 170 millions de cartes de crédit et débit, sous couvert du groupe "Shadowcrew"). Il vendait également des courriels, avec mots de passe et dates de naissance.
  - Il est arrêté et pour éviter la prison, coopère avec la justice.
  - Pendant sa "collaboration", il continue ses activités et vole 45 millions de cartes lors du hack de TJX.
  - Il est condamné à 20 ans de prison et devient une sorte de référence en matière de sécurité… depuis l'établissement pénitencier.
- Cas particulier du hacker Astra, dont on ne connaît pas l'identité réelle.
  - Pirate un logiciel Dassault très utilisé dans l'aéronautique, l'automobile et les équipements militaires, qui lui permet d'accéder à des données confidentielles.
  - Le hacker, un grec, a vendu les données à 250 clients en France, Allemagne, Italie, Afrique du Sud, Brésil, dans les Balkans et en Asie.
  - Plus de 300 millions de pertes pour Dassault.
  - Considéré comme l'un des hackers les plus "brillants" du domaine.

Jonathan James



Albert Gonzalez

Des organisations redoutables

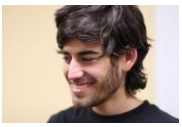
- Les terroristes : les plus redoutables, car les plus motivés.
  - Pour des questions politiques ou religieuses, ils s'estiment en guerre et exploitent les techniques de pénétration les plus sophistiquées.
  - Organisations très compétentes, capables de mettre en œuvre des schémas de pénétration sur plusieurs années.
  - Nombreux groupes de ce type : l' « Unified Cyber Caliphate », bras armé de Daesh (état islamique), spécialisé dans les attaques informatiques ou l'Institut Mabna, lié au gouvernement des mollah iraniens, qui a fait de nombreuses victimes, parmi lesquelles cinq agences fédérales, onze sociétés privées étrangères et 144 universités américaines.
  - Leurs motivations sont claires, « pures » et « loyales » de leur point de vue, tout comme un saboteur pendant un conflit peut être considéré comme un héros ou un terroriste, selon le camp dans lequel il se trouve.
  - Il existe de véritables écoles pour former les membres de ces organisations, avec un niveau des enseignants très élevé, en analyse numérique, technologies de chiffrement, intelligence artificielle, etc.
- Les espions. des hommes et femmes de l'ombre, formés au vol d'informations confidentielles, politiques mais surtout économiques et à la diffusion de fausses informations.
- L'exemple des élections américaines et le rôle joué par Cambridge Analytica, fondé par Steve Bannon et Robert Mercer, est un bon exemple de déstabilisation, venu cette-fois de l'intérieur

Hackers et groupes récents

Elliott Gunton : la diversité du répertoire
Vol d'identités, attaque de l'entreprise de télécoms Talk Talk, blanchiment d'argent via les cryptomonnaies…
20 mois de prison. Procédure en cours.

Evgeniy Bogachev : l'auteur du botnet GameOver Zeus.
100 millions de dégâts. Son produit a été utilisé par les services russes.
Le FBI a offert une prime de 3 millions $, pour le traduire en justice. La plus élevée de l'histoire.

Graham Ivan Clark : la plus grosse attaque sur Twitter.
Twitter est le véhicule pour une vaste arnaque sur le bitcoin.
100 000 $ et 3 ans de prison.



AaronSwartz, hacktiviste utopiste, peu intéressé par les gains financiers. Utopiste, voulait faire d'Internet une plate-forme libre et ouverte. Très intéressantes initiatives : flux RSS, Creative Commons…
Traqué par le FBI, se suicide à 26 ans.

Alexsey Belan L'un des pires.
L'un des pirates les plus dangereux du monde : 700 millions de comptes Yahoo piratés. Toujours en fuite…

Donk_enby. Effort légal de salubrité publique…
Utilise le réseau social "Parler" pour sauvegarder 56 Tbytes de données publiques sur l'attaque du Capitole.

Des groupes militaires plus ou moins reconnus

TAO, pirates de la NSA

Bureau 121, Corée du Nord

Fancy Bear : Russie

PLA Unit 61398 : Chine

Unit 8200 : Israël

Les femmes et le "hacking"

- Le hacking n'est pas une spécificité féminine.
- Peu nombreuses, mais très performantes.

Xiao Tian
A l'origine du groupe "China Girl Security Team" en réaction au monde des hackers, dominé par les hommes. Liée à de nombreux groupes dans le monde. L'organisation féminine la plus importante au monde. Très surveillée.

Adeanna Cooke
Modèle Playboy dont les photos ont été illégalement publiées sur un site non autorisé. Grâce à ses compétences, a hacké le site et a retiré ce qui la concernait. Intervient depuis en consultante pour d'autres modèles dans la même situation.

Anna Chapman
Hacker russe, arrêtée à New York en 2010 pour activités d'espionnage. Renvoyée en Russie.

Ying Cracker
Educatrice chinoise de Shanghai, spécialisée dans l'apprentissage des techniques de hacking. Très célèbre…

Raven Adler
Passé de hacking, désormais repentie. Conçoit des systèmes de détection, de tests et d'audit de protections. Connue pour ses publications dans la presse technique et sa collaboration avec de nombreuses compagnies.

Joanna Rutkowska
Hacker éthique polonaise qui a développé des outils pour recenser les hackers dans le monde. Très connue pour avoir montré les vulnérabilités de Vista au Defcon. A lancé sa propre structure de sécurité "Invisible Things Labs".

Kristina Svechinskaya
Très connue pour ses activités de transferts financiers illégaux ("mule money") au détriment de banques américaines et britanniques. A volé 3 millions $ environ en quelques mois.
Virtuose du cheval de Troie Zeus.

Jude Milhon
Hacker (St Jude) et membre du groupe délictueux Cypherpunks. Membre de l'organisation "Computer Professional for Social Responsability". A écrit plusieurs livres et a contribué à divers magazines spécialisés en sécurité et programmation. Disparue en 2003.

Natasha Grigori
Débute ses activités de hacking dans ls années 80 et connaît la célébrité grâce à un BBS destiné à aider la communauté des hackers. Fonde antichildporn.org (ACPO) pour combattre la pornographie pornographique. Succès foudroyant. Disparaît en novembre 2005, mais ACPO continue ses activités.

Les hackers les plus bêtes du monde

- En général, les hackers ne s'en vantent pas…
- Difficile de faire un choix.
- Higinio Ochoa : hacktiviste du mouvement "Occupy WallStreet".
  - S'introduit dans plusieurs départements de police pour relever l'identité des policiers violents.
  - Pénètre la base de données criminelle du FBI et laisse une image en tant que signature portée sur le ventre de sa "petite amie" en bikini :
    "Vous avez été niqué par Wormer (son nom de guerre) et Cabin Cr3W. On vous aime bande de putes".
  - Problème, l'image comporte des données GPS qui mènent à son arrestation : 18 mois de prison et interdiction de s'approcher d'un moyen d'accès à Internet.
- Un groupe de hackers de l'Ouzbekistan, qui se situe comme chacun le sait entre le Turkmenistan, le Tadjikistan et le Kirghizistan, ne trouve rien de mieux que d'acheter un nom de domaine avec son propre nom et des données réelles et vérifiables, pour abriter ses activités délictueuses…
  - Même les russes n'en sont pas revenu…
- Attaque bien connue d'un groupe de hackers turc, sur 70 sites supposés israéliens avec "defacing", messages et déni de service : en fait les sites étaient palestiniens… qui utilisaient des serveurs israéliens.
- La faillite de FTX, place de marché de cryptomonnaies, fondée en 2019, par Sam Bankman-Fried a été provoquée par une intrusion non autorisée qui a détourné 400 millions $.
  - L'auteur de l'attaque a paniqué, car il avait utilisé son propre compte Kraken (plate-forme d'échange)…
- Un hacker finlandais (Julius Kivimäki) recherché depuis 2 ans et connu sous le pseudo Zeekill est arrêté à Courbevoie par la police française… pour violences conjugales !!!
- Pour le plaisir : un hacker lors d'une session IRC se plaint que le modérateur fait tomber la liaison.
  - Il demande l'adresse IP du modérateur qu'il menace de lui "crasher" son système Celui-ci la lui donne : 127.0.0.1 (!!!).
  - Le hacker met sa menace à exécution et grâce à un logiciel gratuit, casse le serveur à cette adresse. Qui est la sienne.
  - Un cas de pirate qui se pirate lui-même.

En résumé, 3 grandes familles

Le reste n'est que littérature

Jeunes "abrutis" inconscients à l'égo surdimensionné. Le résultat de l'"éducation" par les jeux vidéos, qui ne savent plus faire la différence entre le bien et le mal. Vont s'assagir.

Terrorisme et philosophie, les moteurs les plus dangereux. Incontrôlables. Personnels motivés et compétents, convaincus de détenir la "vérité"…

Criminalité financière. Internet, par la faiblesse native de ses protocoles et le manque de volonté pour le réformer, est le terrain idéal pour les appétits mafieux.

Ne pas confondre les comportements d'huluberlus inconscients et généralement peu compétents, avec l'activisme de l'ombre : politique, financier, religieux.

Sécurité : cinq générations de criminels

17 Mars 2023

Nos prochains webinaires

24 mars 2023	**L'enseignement de demain, comment abêtir les enfants**
31 mars 2023	**Santé et ondes : soyons sérieux**
7 avril 2023	**Oracle, Intel et IBM, colosses aux pieds d'argile**
14 avril 2023	**Ethereum, au cœur de l'Internet de demain**
21 avril 2023	**Backup et restauration des datacenters**
28 avril 2023	**Pourquoi l'IA est-elle stupide ? Elle nous imite**
5 mai 2023	**L'hyperautomation : les temps modernes du TI**
12 mai 2023	**Quand la biométrie sort des sentiers battus**
26 mai 2023	**Productivité, il n'y a pas qu'Office. Ah, bon ?**
2 juin 2023	**Les grandes utopies du TI : capitaliser sur nos erreurs**
9 juin 2023	**Les transports du futur : verts et sans pilotes**
16 juin 2023	**Sécurité : les reproches faits à la suite TCP/IP**
23 juin 2023	**La fédération d'identités : "you will never walk alone..."**
30 juin 2023	**Les grandes figures du TI... dont on parle moins**

claude@lemarson.com
https://www.lemarson.com