



Les Cyber-Attaques contre les Laboratoires de Biologie Médicale
Dr Didier Legeais,



Ne Pas se Cacher La Vérité



Conflits d'intérêts ou intérêts convergents !!!

- ❑ Chirurgien Urologue
- ❑ Vice-président du CDOM Isère
- ❑ Société Savante (AFU), Académie de chirurgie
- ❑ Syndicaliste (SNCUF, SMI, URPS....)
- ❑ Assureur : Courtier (Médirisq) – Directeur médical Assurance (Panacéa)

- ❑ Psychopathe ou brave type.....
- ❑ Aux services des confrères et des patients depuis 25 ans.....



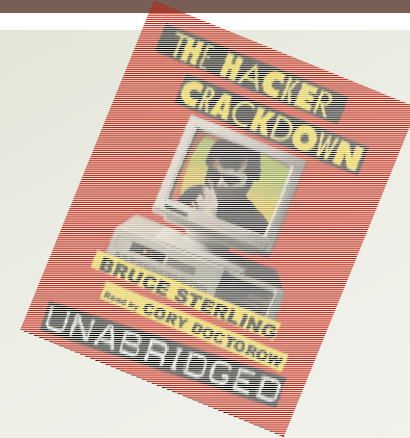
Un peu d'histoire

- **1934** : **Paul Otlet**, documentaliste et humaniste Belge, , décrit « internet » dans son traité de documentation
- **1965** : première **connection** à distance
- **1962-1965** : pour l'**armée américaine** et les chercheurs création d'**Arpanet** pour transmission d'info par paquets en cas de guerre nucléaire
- Notion d'**internet** apparaît en **1972**, **interconnecter des réseaux**,
- **1972** : premier mail
- **1980** : **National Science Foundation NSF** crée 5 centres informatiques ouverts aux utilisateurs
- Premier **PC** : **IBM 1981**
- Premier **Mac** **Juin 1984**
- **1990** : Création du **Web** : Premier application : **WWW: World Wide Web** : la toile d'araignée Mondiale
- **1992** : NSF : crée les noms de **domaines** : Yahoo, Amazon, eBay
- **2016** : **Conseils des Droits de l'homme des Nations Unis** : non violation et **neutralité** d'Internet.



Cybercriminalité

- **1977** : après un concert punk des «Butthole Surfers », « les surfeurs du trou de balle » Bruce Sterling Fusionne l'esprit **DIY** (Do It Yourself) et le **rejet de l'informatique** (2 milles ventes)
- **1990** : opération **Sundevil**/FBI CIA/EFE Electronic Frontier Fondation
- **2007** : première Cyberattaque : sites russes contre administration estonienne (soldat de Bronze) : **attaque par saturation** : **botnet**
- **2005-2007-2009** : pannes électriques géantes au Brésil: cyberattaques ?
- **2008** : invasion Russe en Géorgie précédée par une cyber-attaque.
- **2009** : Corée du Nord attaque la Corée du Sud : ministères, banques
- **2010** : attaque par Israël ou USA paralyse centrale Nucléaire de Bouchehr en Iran: virus Stuxnet (clés USB)



- **2011** : société Lockheed Martin paralysée code de sécurités dérobés : avions de combats F16
- **Juin 2011** : compte Gmails de hauts fonctionnaires américains piratés par la Chine ?
- **2011** : Attaque contre les sites gouvernementaux Japonais
- **2012** : 80 millions de dollars détournées de banques mondiales
- **2014** Sonny attaqué par les « Guardians on peace »
- **2016** : Banque centrale du Bengladesh se fait dérober 81 Millions de \$
- **2017** : explosion sur une faille « Windows »
 - **12 Mai 2017** : WannaCry: « Vouloir pleurer »
 - **15 Mai 2017** : Adylkuzz
 - **27 Juin 2017** : NotPetya



12 Mai 2017 : WannaCry: « Vouloir pleurer »

- ❑ Logiciel Malveillant type « ransomware (rançongiciel) auto-répliquant »
- ❑ En 24 h00, 300 000 ordinateurs sont touchés 150 pays
- ❑ Le plus grand piratage à rançon de l'histoire d'internet
- ❑ Impact : Renault, le ministère de l'intérieur Russe, la Deutsche Bahn, Vodafone, Téléfonica, Fedex, Arrêt des chaînes de production.
- ❑ le NHS (national Health Service) : 20% des hôpitaux, 50 établissements.
- ❑ Utilise faille sécurité EternalBlue coorrigé par Microsoft en Mars 2017
- ❑ Cause: mécontentement contre Donald Trump, ou en réaction au refus d'Apple de partager avec la NSA
- ❑ Rançon 300 puis 600 \$ (3j)en Bitcoins.
- ❑ Gains Hackeurs : 95 000 \$, Corée du Nord ? Groupe Lazarus Group?
- ❑ Coût dizaines de millions de \$
- ❑ Recherche « patient zéro »



Adylkuzz

- Des centaines de milliers d'ordinateurs
- Faille de sécurité EternalBlue de Windows
- Plus de victimes que WannaCry
- **Rançongiciel** : Plusieurs millions d'€, crypto-monnaie : le monéro.



NotPetya : 27 Juin 2017

- Logiciel malveillant
- Rançongiciel en Bitcoins; 300 \$: **Wiper** : « essuie-glace »: destruction +++
- **Ver informatique**,
- Variante Petya puis Non..
- Même faille de Windows : **EternalBlue**, **EternalRomance** (NSA, The Shadow Brokers)
- Banques Ukrainiennes, Mars, Nivéa, pétrolier Russe Rosneft, Merck, Centrale Nucléaire de Tchernobyl, Saint Gobain, Auchan, SNCF



□ **Cyber-attaque** : atteinte **malveillante** des systèmes informatiques par un réseau cybernétique.

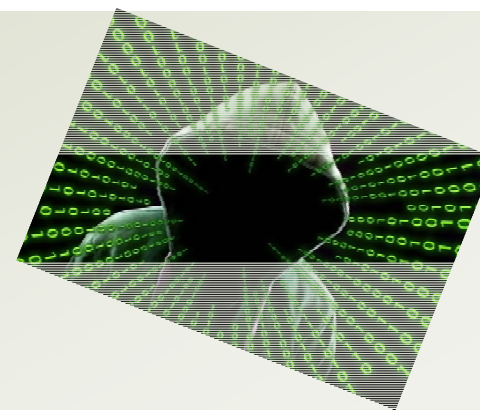
- Crack-ing : craquer
- Phreaking : piratage téléphonique
- Hack-ing: pirater
- Malware : programme malveillant

□ **Objectifs** :

- ▣ Sabotage
- ▣ Espionnage
- ▣ Atteinte à l'image
- ▣ Cybercriminalité : rançon



- ❑ > 400 000 victimes/an dans le monde
- ❑ 100 grandes entreprises
- ❑ **11 attaques/jour** en France
- ❑ Perte financières moyennes **1,5 millions d'€**
- ❑ **80%** des structures françaises cette année
- ❑ La France figure dans le **top 10** des pays les plus touchés
- ❑ Formes très diverses :
 - ❑ du *ransomware* (attaque la plus répandue, ou **rançongiciel** en français)
 - ❑ *au déni de service*
 - ❑ *la défiguration de site web : wiper*
 - ❑ *le vol de données personnelles*



- ❑ Sources :
 - ❑ <http://www.gouvernement.fr/risques/risques-cyber>
 - ❑ <http://economyandco.com/les-5-chiffres-a-connaître-sur-la-cybercriminalité>



- « Près de **90 % des attaques ransomware** » au deuxième trimestre 2016 « ont visé des **établissements de santé** dans le monde » (selon Lexsi).
- « peuvent avoir un impact direct sur **la sécurité des soins** » comme sur **les finances** de l'établissement :
 - **Frais de reconstitution** de données, voir pertes de données définitive si pas d'archivage électronique efficace
 - **Frais de décontamination virale**
 - **Frais supplémentaires d'exploitation** (personnel, utilisation d'équipement extérieur...)
 - **Honoraires d'experts** pour identifier l'origine et les circonstances d'un sinistre
 - **Frais de recours**
 - Éventuelles **rançons** (Bitcoins > €)



- Coût :
 - ▣ 300 000 € < 1 000 salariés ou moins
 - ▣ 1,3 millions d'€ : > 5 000 salariés. (NTT Com Security)
- 127 € : coût d'une seule donnée compromise
- 4,4% de taux de clientèle perdue (l'Usine Nouvelle, mars 2014)
- Temps perdu : en moyenne 9 semaines pour rétablir les systèmes.



□ Source : <http://ideas.microsoft.fr/cybersecurite-5-chiffres-cles-a-connaître/>



Particularités des labos de biologie:

- **CNIL:** « *il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par **le secret médical*** »



Particularités des labos de biologie:

- Pas plus visés que d'autres entreprises, mais les **données** (données médicales des patients) sont **sensibles** !
- **Chaque** organisme de santé (hôpital, labo, fabricant de matériel, doit être sûr à 100 % de sa sécurité : **porte d'entrée** ! pour les pirates informatiques
- Importance de **former le personnel** il n'est pas rare que la **négligence humaine** soit à l'origine des failles de sécurité.
- Etablissements de santé et des entreprises du secteur médical : **proies faciles** car leurs investissements en matière de sécurité informatique restent encore trop insuffisants pour les mettre hors d'atteinte. En outre, **la valeur des données de santé** dépasse très largement celle des coordonnées bancaires et celles des numéros de sécurité sociale.



- Les dossiers médicaux : **une mine d'or** d'informations.
 - **Chantage** pour obtenir de l'argent en échange de la non-publication des données dérobées,
 - Revendent **les numéros de sécurité sociale** et bancaires des patients sur le marché noir par exemple.
 - **L'espionnage industriel** : revendre les informations exfiltrées à d'autres organismes du secteur, comme des données sur la **recherche médicale** aux laboratoires pharmaceutiques ou sur le dossier médical des patients aux **compagnies d'assurance**, entre autres.
- La sécurisation des systèmes informatiques des établissements de santé est donc cruciale. Il est à rappeler qu'en cas de **plainte de la part d'un patient** dont les données médicales ont été piratées, le responsable du laboratoire risque une peine qui peut aller **jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende** (art. 226-17 Code pénal).



Exemples de cyberattaques en santé en France

- En 2015, le **laboratoire de biologie médicale Labio**
 - ▣ cible du groupe de pirates **Rex Mundi**.
 - ▣ **40 000 identifiants** (nom, prénom, login et mot de passe)
 - ▣ centaines de **bilans médicaux**.
 - ▣ rançon **20 000 euros**
 - ▣ refus de Labio : 15 000 identifiants de connexion, immédiatement rendus inutilisables publications d'une dizaine de résultats d'examens avaient été publiées.
- Le 1^{er} mai 2015, au **Centre Marie Curie (Valence)**,
 - ▣ piratage de deux disques réseaux
 - ▣ pendant 24 heures, **pas de radiothérapie**.



Un cadre législatif de plus en plus contraint

- De nouvelles mesures réglementaires, françaises et européennes, obligent les biologistes médicaux à se saisir rapidement du sujet de la cyber-sécurité.
- le 14 avril 2016 par le Parlement européen:
 - Le règlement général sur la protection des données
 - La directive relative à la protection des données à caractère personnel à des fins répressives
- 1 Mai 2018 : Réglementation européenne : obligation de déclaration dans les 72 h00 sinon amende de 4% du CA pour toutes les entreprises y compris professions libérales.
- Obligation de déclaration dans les 72 H00 depuis le 1 octobre 2017 : La France met en place un système de collecte des incidents dans des établissements de santé et des cabinets de radiothérapie : déclaration ARS (Décret 14 sept 2016)
- Obligation de revoir la politique de conformité informatique et libertés.
- 1er octobre 2017, la DGS impose: un plan d'action pour réduire le cyber-risque à 6, 12 et 18 mois opposable aux établissements de santé et aux laboratoires
- Les laboratoires vont devoir mettre en place une véritable politique de protection de données (plan de continuité d'activité et de reprise d'activité en cas de cyberattaque), mais aussi s'assurer que les solutions mises en place répondent à l'état de l'art. Ils vont devoir s'entourer d'experts pour, en cas de suspicion d'attaque, évaluer correctement l'impact.



Cybersécurité au niveau européen

- La Commission européenne va justement faire voter **en 2018 un "paquet cyber"**, c'est-à-dire un ensemble de mesures, au niveau européen, pour mieux lutter contre les cyberattaques.
- L'une des initiatives phares est **la réforme de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)**. L'institution, basée en Grèce, sera transformée en une véritable « *Agence de cybersécurité de l'UE* », aux missions élargies. L'autre grande annonce de Jean-Pierre Juncker concerne **la création d'un label européen destiné aux entreprises** pour inciter les entreprises à intégrer la sécurité en amont, dès la conception du produit.
- Création d'un **Centre européen de recherche et de compétences en matière de sécurité** "dans le courant de l'année 2018 » pour **coordonner le financement de la recherche technologique**, et **favoriser une recherche plus efficace en coordonnant les efforts nationaux**
- Un "**plan d'action**" visant à "**garantir une réaction rapide de l'UE et des Etats membres en cas de cyberattaque de grande ampleur**" devrait aussi voir le jour, piloté par l'ENISA. Source : <http://www.latribune.fr/technos-medias/cyberattaques-que-contient-le-paquet-cyber-que-l-europe-veut-voter-en-2018-751009.html>



Guide des bonnes pratiques de l'informatiques

- 12 Règles essentielles pour sécuriser vos équipements numériques
- Agence Nationale de la sécurité des systèmes d'information
 - CGPME



1 Choisir avec soins ses mots de passe

- ❑ 12 caractères de types différents
- ❑ Aucun lien perso
- ❑ Pas dans le dictionnaire
- ❑ ght5CD%E7am
- ❑ aE2LPLj2Géa!
- ❑ Pas d'outils de stockage des mots de passe
- ❑ Pas le même mot pour plusieurs



2. Mettre à jour régulièrement vos logiciels

- ❑ Faille IOS, Androïde, MacOs, Windows
- ❑ **Mettre à jour régulièrement**
- ❑ WannaCry, Adylkuzz, NotPetya



3 Bien connaître ses utilisateurs et ses prestataires

- ❑ Ne pas aller sur des **sites inconnus**
- ❑ Ne pas ouvrir des mails de **destinataires inconnus**
- ❑ Utiliser des **comptes utilisateurs pas administrateurs**



4 Effectuer des sauvegardes régulières

- Régulièrement
- Sauvegarde **externe**
- **En dehors** de l'entreprise
- Attention Cloud :
 - ▣ Confidentialité
 - ▣ Territorialité
 - ▣ Intégrité, disponibilité
 - ▣ Irréversibilité des contrats
 - ▣ Logiciel de cryptage avant le cloud



5 Sécurisé l'accès Wi-Fi de votre entreprise

- ❑ Préférer une **installation filaire** pour éviter le piratage,
- ❑ Borne d'accès : ne pas prendre Web mais **WAP2 ou WPA-AES**
- ❑ Activez **fonction pare-feu** de votre Box,
- ❑ Désactiver la borne d'accès lors qu'elle n'est pas utilisée.
- ❑ N'utilisez **pas les Wi-Fi public**: gare, hôtel, aéroport,
- ❑ **Antivirus et pare-feu**



6 Etre aussi prudent avec son smartphone, sa tablette

- Que les applis nécessaires,
- **Code Pin**,
- **Verrouillage** automatique
- Sauvegardes régulières extérieures
- Ne mettez **pas vos mots de passe** sur la fiche 1



7 Protéger ses données lors de ses déplacements

- ❑ Ne **pas prêter** son ordinateur
- ❑ Ne **pas brancher** un téléphone dessus.
- ❑ Ne voyager qu'avec les **données nécessaires**.
- ❑ **Pastille de couleur** pour le distinguer et éviter les échanges.
- ❑ Retirer la **carte SIM** et la **batterie** si vous êtes contraints de vous en séparer
- ❑ Ne **pas brancher** de **clefs USB**



8 Etre prudent lors de l'utilisation de sa messagerie

- Cohérent adresse **expéditeur connu**,
- **Pas** de demande **d'information personnelles**, ou confidentielles
- Attention attaque par **hameçonnage** , phishing
- Utilisez des **antivirus** dès que possible



9 Télécharger ses programmes sur des sites officiels des éditeurs

- Attention que des sites officielles, attention aux Copies.
- Une fois décharger lancer une analyse **antivirus**.



10 Etre vigilant lors d'un paiement sur Internet

- ❑ Site **sécuriser** uniquement
- ❑ Privilégiez l'envoi d'un **code SMS**



11 Séparer les usages personnels des usages professionnels

- **Différents ordinateurs.**
- **Pas d'ordinateur perso**
- **Il faut acheter des ordinateurs professionnelles**



12 Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

- Donnez le **minimum** d'information
- Garder deux adresses : **perso et pro**



Conclusion

- ❑ Laboratoires de biologie et centre de radiothérapie en première ligne mais cela va toucher tout le monde : **1 Mai 2018**
- ❑ PC > MAC
- ❑ Former le personnel
- ❑ Sauvegarder à l'extérieur
- ❑ Prendre un professionnel reconnu
- ❑ Interroger son Assureur
- ❑ Banque de données santé ??SISRA?



**Merci de votre attention
Didier Legeais
0685217995**

