31 août 2014
Chantage à la santé

Ce que les Chinois ont en tête en cherchant à voler des millions de dossiers médicaux occidentaux

La nouvelle tendance du monde de la cybercriminalité : le vol de données médicales. 4,5 millions de fichiers auraient ainsi été volés par des hackers chinois à un groupe hospitalier américain.

Avec Jean-Paul Pinte

Atlantico : Un groupe de hackers chinois a subtilisé 4,5 millions de données médicales au Community Health Centre (CHS), le deuxième réseau hospitalier américain. Quelles peuvent-être les motivations de ces hackers ? Que peuvent-ils bien faire de ces données personnelles ?

Jean-Paul Pinte : Nous ne sommes qu'au début d'une longue série d'épisodes cybercriminels dans le domaine de la santé et ce ne sont pas les applications E-santé comme les montres et les bracelets connectés qui pourront venir changer la donne. Cette fois-ci les hackers ont touché des données sensibles à chacun de nous, celles de la santé. Pas question ici de vol de numéros de cartes de crédit mais bien de données personnelles toutes aussi monnayables sur la toile aujourd'hui. Ce n'est pas non plus l'arrivée de l'Open Data ou libération des données par nos administrations croisées au phénomène du Big Data qui pourront arranger les choses. **La santé est aujourd'hui impactée par la cybercriminalité et ce secteur est appelé à devenir celui où les risques cybercriminels seront certainement les plus importants.**

Pour ces hackers, il s'agit avant tout, comme dans toute cyber-attaque, de prendre le pouvoir sur un système, une structure tout en s'en réjouissant. Il est ensuite question de pouvoir procéder à la manipulation d'informations et donc aussi de de travailler à une désinformation. **C'est aussi le moyen de pratiquer le chantage pour en obtenir en retour un avantage financier.**Enfin et surtout aussi une façon de pouvoir nuire à la réputation de chacun d'entre nous. Imaginons un instant que nos très personnelles données de santé soient demain à la portée du grand public ou d'institutions.

Quelles conséquences pour leurs propriétaires ? Et pour les hôpitaux ?

L'impact est loin d'être négligeable pour ces deux cibles.

Il en va avant tout de la réputation de ces derniers. Comme pour les propriétaires de données, les hôpitaux risquent de se voir salir leur image et voir naître la problématique de la fausse information véhiculée sur la toile. Elle pourrait nuire gravement à la santé des patients par exemple. Pour un particulier qui verrait divulguer des informations à son sujet cela pourrait par exemple lui poser problème dans le cadre de son emploi ou d'un recrutement à venir. **Apprendre que l'on suit une thérapie pour une maladie grave...** Le piratage des Dossiers médicaux personnels (DMP) qui peuvent aussi nuire à l'équilibre psychologique des patients.

Pour un hôpital, le simple fait de penser que son système d'information (SI) puisse être attaqué avec ses fichiers modifiés voire supprimés nous permet de réaliser l'impact sur les clients hospitalisés et aussi sur ceux passés par là et dans la nature aujourd'hui.

L'attaque du ver Conficker a paralysé plusieurs hôpitaux français. Son point d'entrée dans le réseau, les appareils de laboratoire et d'imagerie. "Aujourd'hui, les scanners et les IRM sont tous connectés", explique Philippe Loudenot, chargé de la sécurité informatique au ministère de la Santé.

Les problèmes liés à la confidentialité des données de santé : aux USA, 8 millions de dossiers médicaux ont été ainsi pris en otage contre une rançon. Il suffit d'imaginer que tout est, ou sera interconnecté dans les services hospitaliers pour mesurer le risque d'intrusion, d'interception de données, d'immobilisation, voire de pollution des données médicales via l'infection des SI.

Le département de la santé et des services sociaux des Etats-Unis indique dans son "Rapport annuel au Congrès sur les violations de données de santé mal protégées" que 14,7 millions de personnes ont été touchées par des violations de leurs données personnelles en 2011 et 2012. Pourquoi le vol de données médicales est-il en augmentation ? N'y a-t-il pas plus rentable ?

Si le phénomène est en hausse c'est que les données de santé nous sont plus que précieuses et sont indispensables à notre équilibre vital ! Elles sont en effet le seuls moyen de traçabilité, d'entretien et de suivi de notre santé. L'accès à des données sensibles touchant à la vie privée soulève aussi les questions importantes des garanties apportées à chacun de protection de sa propre intimité.

C'est aussi parce que l'identité de chacun est devenue l'une des marchandises les plus précieuses que les hackers s'y attaquent plus aujourd'hui. Quiconque se verrait attaquer à ce niveau serait prêt à payer le prix pour se voir supprimer des données diffusées sur la toile le concernant. C'est aussi parce que les hôpitaux n'ont pas mesuré dès le début que leurs données étaient parfois vulnérables et allaient bien au-delà du simple réseau sécurisé d'Intranet ou d'Extranet que le vol de données a profité aux pirates. **Le BYOD et le Cloud Computing sont venus aussi depuis ce temps se rajouter aux risques de fuite de données.**

Le département de la santé et des services sociaux des Etats-Unis indique dans son "Rapport annuel au Congrès sur les violations de données de santé mal protégées" que 14,7 millions de personnes ont été touchées par des violations de leurs données personnelles en 2011 et 2012.

Selon le Ponemon Institute, dans une étude sponsorisée par ID Experts, 94 % des établissements interrogés auraient rencontré au moins une fois le problème. Et 45% y auraient eu affaire plus de cinq fois dans les deux dernières années. L'un des problèmes, en plus de la sécurisation des données, est le coût : l'étude estime que cela pourrait coûter 7 milliards de dollars par an aux organisations. L'une des causes est que certains appareils qui contiennent des données ne sont pas sécurisés, comme les pompes à insuline (69% des institutions ne le feraient pas). Selon le rapport, le cloud et le mobile, qui font que de plus en plus de données sont hébergées sur de plus en plus de supports, pas forcément sécurisés, pourrait augmenter les risques.

Jennifer Leuer, directrice générale de ProtectMyID chez Experian, un service chargé de protéger les données d'identification dans le domaine de la santé signale que "Le secteur de la santé est beaucoup plus fragmenté que tout autre secteur. Il peut potentiellement faire appel à des dizaines de fournisseurs ou d'intervenants". Selon elle, c'est cette disparité qui favorise les incidents. **Çela a été le cas du fournisseur de services de santé Health Net qui a découvert que les données personnelles et les dossiers de 1,9 million de ses clients avaient disparu de ses serveurs.** La mutuelle conservait sur ses disques les noms, adresses, numéros de sécurité sociale, informations financières et données sur la santé des anciens adhérents et des adhérents actuels de Health Net, plus celles d'employés et de professionnels de soins de santé.

Pourquoi les hackers chinois s'attaquent-ils alors à des données américaines et non à des données chinoises ? Pour le Figaro, il s'agirait d'une tentative de la part d'Américains travaillant sous des adresses IP chinoises, de brouiller les relations sino-américaines...

Comme je l'expliquais précédemment nous n'en sommes qu'au début de ces attaques voire début de cyber-guerre sur les données entre pays. La société de sécurité informatique "Mandiant" qui a enquêté sur le phénomène a qualifié l'attaque Community Health Centre de : "Menace persistante avancée". **Des méthodes qui ne sont pas à la portée du premier quidam venu.**

Les objectifs de ces pirates restent à ce jour encore assez flous mais s'inscrivent à mon sens principalement plus dans l'extraction de données personnelles au sein de banques de données que dans un souci d'exploitation de données purement médicales.

Le phénomène ne se limitera pas à ces deux pays et les pratiques évolueront encore, nécessitant de plus en plus une surveillance stratégique déjà plus qu'entamée avec l'affaire Snowden.

Qu'en est-il de la situation en France ? Avons-nous déjà assisté à ce type de vol ?

Vers la fin de l'année 2009, le ver informatique Confiker, apparu en novembre 2008, a paralysé le système informatique de nombreux établissements de santé à Paris.

En dehors de cet événement, en France, on a pu assister ces dernières années plutôt à des vols de matériel et de dossiers médicaux (Ex : Michael Schumacher) au sein des hôpitaux qu'à des cyber-attaques visant à atteindre des banques de données.

Il y a fort à parier cependant qu'avec, par exemple, Bluebutton qui dématérialise le dossier médical de l'individu (DMP) et lui permet de le partager avec son médecin, les choses vont évoluer, comme avec le développement du "Bring Your Own Device" qui présente lui aussi déjà de nouvelles formes de risques aujourd'hui difficilement contrôlables.

Les dispositifs médicaux présentent également des risques considérables, vu que ceux-ci sont également des dispositifs actifs : appareils de surveillance, monitoring, Pacemaker, pompes à insuline… D'ailleurs, selon le site Anti-cybercriminalite.fr, le

hacker Jay Radcliffe a déjà prouvé que sa pompe à insuline de marque Medtronic pouvait être manipulée à distance par une autre personne, et que cette dernière pouvait avoir accès au dossier médical du patient, et en modifier ainsi les contenus.

Je vous invite ainsi à lire ce dossier sur l'Open Data et la santé car ce dernier pourrait se dessiner demain comme une nouvelle arme aux mains des pirates.

En attendant, ne perdez pas votre carte vitale car tout commence par là …