A GIS plugin to model the near surface air temperature from urban meteorological networks

Najla Touati, Thomas Gardes, Julia Hidalgo

Rubrique : Sécurité et hôpital

CYBERATTAQUES ET HOPITAL

CYBER ATTACKS AND HOSPITAL

Didier Mennecier

Médecin Général. Directeur des systèmes d'information et du numérique du service de santé des Armées.

Auteur correspondant : Médecin Général Didier Mennecier, DSIN, 69, avenue de Paris, 94160 Saint-Mandé. E-mail : docteur@mennecier.net

L'auteur déclare ne pas avoir de liens d'intérêts.

Résumé

Les cyberattaques visant les systèmes et réseaux hospitaliers sont en nette progression dans le monde et vont probablement augmenter. Le procédé des *Ransomwares*, qui est de chiffrer les données de la cible pour obtenir une rançon, apparaît de plus en plus dans les structures hospitalières. Il faut savoir que les données de santé sont le nouvel eldorado des Hackers. Les numéros de sécurité sociale se vendent plusieurs centaines de dollars chacun aujourd'hui, contre quelques dollars pour un numéro de carte bancaire qui ne vaudra plus grand chose une fois le vol signalé.

Mots-clés : cyberattaque, hôpital, donnée de santé, *Ransomware*, Hacker

Summary

Cyber attacks on hospital systems and networks are on the rise worldwide and are likely to increase. The Ransomware process, which is to encrypt target data to obtain a ransom, appears more and more in hospital structures. You should know that health data is the new Eldorado for Hackers. Social security numbers are sold for several hundred dollars each today, compared to a few dollars for a bank card number that will not be worth much once the theft is reported.

Keywords : Cyber attacks, Hospital, Health Data, Ransomware, Hacker

Pour comprendre l'ampleur des cyberattaques, l'entreprise américaine NORSE (http://norse-corp.com), spécialisée en sécurité informatique, a créé une carte du monde interactive qui montre en temps réel, les attaques que subit des *honeypots* ou pot de miel qui sont des leurres informatiques pour attirer des attaques sur des serveurs.

Cette carte objective une infime fraction des cyberattaques sur Internet et sur la capture ci-dessous nous pouvons voir une attaque dite par dénis de service ou *DDoS* (*distributed denial of service attack*) en juin 2014 de Facebook (Figure 1). Cette attaque a rendu indisponible le service pendant une heure.

Une attaque par *DDoS* a pour principe de rendre indisponible un service par inondation du réseau par exemple lors d'une demande d'accès à une page Web.

Figure 1. Attaque par dénis de service (DDoS) en juin 2014 de Facebook.

CYBERATTAQUE VIA LES OBJETS CONNECTES

Une attaque informatique d'une ampleur sans précédent a eu lieu le 22 Octobre 2016 aux États-Unis. Cette attaque s'est servie d'une faille de sécurité présente sur des objets connectés (webcams, imprimantes, thermostats…). Ainsi environ dix millions d'objets connectés, ont été infectés par un virus, qui par la suite, a envoyé automatiquement des requêtes pour submerger les serveurs et provoquer un déni de service auprès de la société américaine DYN.

Cette société héberge la plupart des sites web américains. Ainsi la société DYN a été submergée de requêtes automatiques et ne pouvait plus faire face aux demandes des internautes qui, tapant une requête dans leur barre d'adresse Internet, n'étaient pas redirigés vers le bon site. Cette attaque qui a duré plusieurs heures a rendu inaccessible de nombreux sites comme PayPal, Twitter etc.

Actuellement il existe environ six milliards d'objets connectés dans le monde, contre seulement plusieurs centaines de millions d'ordinateurs. La puissance d'une attaque par déni de service dépend essentiellement du nombre de périphériques piratés ce qui confirme l'intérêt actuel des hackers de passer par la case *IoT* (*Internet of Things*) ou objet connecté.

CYBERATTAQUE CONTRE DES APPAREILS MEDICAUX

Pirater une pompe à perfusion est ainsi possible

Ainsi la FDA (*Food and Drug Administration*) en juillet 2015 ordonnait le retrait du marché des pompes à perfusion Symbiq de l'américain Hospira. Cet équipement possédait en effet une faille de sécurité qui permettait de modifier à distance les doses de médicament injectées via le réseau Wifi de l'hôpital…

Pirater une pompe à insuline, pourquoi pas

Le fabricant Animas du groupe Johnson & Johnson a averti en octobre 2016 les utilisateurs de ses pompes à insuline OneTouch Ping qu'une faille de sécurité pourrait permettre à un pirate d'accéder de manière non autorisée à la pompe. Jay Radcliffe, expert en sécurité (diabétique de type I) a mis en évidence que la communication entre le lecteur qui envoie le taux de glycémie à la pompe à insuline n'était pas chiffrée. Il a pu ainsi usurper l'identité du lecteur et envoyer à la pompe de fausses informations.

Pirater un stimulateur cardiaque à distance est donc aisé

Ainsi Barnaby Jack en 2012, alors qu'il était expert en sécurité informatique chez IO Active, installé à une dizaine de mètres de l'appareil médical, et muni uniquement d'un ordinateur portable a pu envoyer plusieurs décharges de 830 volts. Il était parvenu à se procurer les données pour rentrer dans l'appareil pour ensuite implanter un virus. La série Homeland a utilisé cette possibilité dans un de ses épisodes (Figure 2).

Figure 2. Homeland saison 2 épisode 10 : Le vice-président décède après que le code Wifi de son Pacemaker est découvert et qu'un virus attaque le système - source : *https://www.incrementalhealthcare.com*

Appareils médicaux accessibles sur le Web

En fait, la plupart des appareils médicaux sont accessibles sur le web. Le site Shodan est un site web spécialisé dans la recherche d'objets connectés à Internet et qui possèdent une adresse IP visible sur le réseau (Figure 3). Ce site a été conçu pour permettre aux entreprises de traquer l'utilisation de leurs logiciels.

Les pirates peuvent ainsi rechercher des dispositifs mal sécurisés et peuvent prendre ainsi le contrôle à l'aide d'un seul navigateur Web en tapant l'adresse IP et en utilisant un login et un mot de passe qui peuvent ne pas avoir été changé. Ainsi il existe encore de nombreux appareils qui conservent les login/mot de passe d'usine comme admin*/admin* ou admin/1234. Ainsi, à condition d'envoyer les requêtes adéquates à Shodan, vous pouvez trouver des milliers de dispositifs médicaux exposés sur Internet.

Les hackers peuvent ainsi identifier des appareils IRM, des équipements de cardiologie, de radiologie ou d'autres dispositifs associés connectés à Internet. De plus il faut savoir qu'un bon nombre de ces dispositifs fonctionne toujours sous Windows XP et compte donc des dizaines d'anciennes vulnérabilités bien connues.