Bitdefender : Les malwares s'attaques aux cardiaques et aux diabÃ©tiques
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 23/10/2012 14:00:00

Lâ□□Ã©diteur de solutions antivirus **Bitdefender** indique que le risque dâ□□attaques contre des appareils mÃ©dicaux tels que les dÃ©fibrillateurs, les pacemakers, les pompes Ã insuline et autres Ã©quipements commandÃ©s par des logiciels est en hausse en raison de lâ□□Ã©volution Â« cybercriminelle Â» des techniques de piratage.

Des patients, cardiaques et diabÃ©tiques, menacÃ©s par des malwares ciblant les appareils mÃ©dicaux. Les attaques contre les hÃ´pitaux sont inÃ©vitables si la sÃ©curitÃ© nâ□□est pas renforcÃ©e.

En septembre, The Government Accountability Office (GAO), l'Ã©quivalent amÃ©ricain de la Cour des comptes franÃ§aise, signalait des vulnÃ©rabilitÃ©s au sein des appareils mÃ©dicaux informatisÃ©s en raison de logiciels et de firmwares non mis Ã jour. Sans parler des attaques ciblant lâ□□Ã©quipement mÃ©dical et les hÃ´pitaux, qui elles, reprÃ©sentent un risque encore plus grand, puisque la sÃ©curitÃ© sur place est toujours insuffisante face Ã ce type dâ□□attaques.

Comptent parmi les cyber-attaques mÃ©dicales les plus courantes, le piratage Wifi, les spywares installÃ©s via des prises rÃ©seau dans les hÃ´pitaux ainsi que les malwares pouvant Ã©craser ou endommager des donnÃ©es.

Â« *La rÃ¨gle tacite qui rÃ©git la sÃ©curitÃ© informatique, est que toute vulnÃ©rabilitÃ© finira par Ãªtre exploitÃ©e Ã un moment ou Ã un autre. Les patients risquent donc de perdre leurs donnÃ©es personnelles et en cas dâ□□infection, les systÃ¨mes des hÃ´pitaux peuvent Ãªtre ralentis*

ou mÃªme, ne plus rÃ©pondre du tout ! Â» dÃ©clare **Alexandru Balan**, Responsable des Recherches en SÃ©curitÃ© des Laboratoires Bitdefender. Â« *Cela pourrait entraÃ®ner des scÃ©narios dignes des plus noirs polars. Les hackers pourraient attenter Ã la vie des patients, dÃ©rober des informations sur des personnalitÃ©s de premier plan ou concernant des anonymes et les utiliser pour des attaques dâ□□ingÃ©nierie sociale ciblÃ©es. Un autre scÃ©nario possible (comprenez rentable) consisterait Ã rÃ©cupÃ©rer tout simplement la base de donnÃ©es dâ□□un hÃ´pital et Ã lâ□□utiliser pour envoyer du spam Ã ses patients, afin de leur proposer directement des mÃ©dicaments et de faux traitements* Â».

Il est recommandÃ© aux centres mÃ©dicaux de :

â□¢ Renforcer les mesures de sÃ©curitÃ©, en maintenant leurs systÃ¨mes dâ□□exploitation et leurs logiciels de sÃ©curitÃ© Ã jour.

â□¢ Surveiller leurs politiques BYOD (Â« Bring your own device Â») dans les hÃ´pitaux et les services de numÃ©ros dâ□□urgence pour empÃªcher les brÃ¨ches de donnÃ©es.

â□¢ Dâ□□utiliser un chiffrement fort pour toutes les communications via des services VPN puisquâ□□il suffit de quelques dollars pour pirater les rÃ©seaux privÃ©s virtuels basiques.

â□¢ De corriger les failles courantes de Windows pouvant conduire au piratage des appareils mÃ©dicaux, la plupart dâ□□entre eux fonctionnant sous Windows.

â□¢ De maintenir tous les rÃ©seaux Wifi Ã lâ□□extÃ©rieur du rÃ©seau principal, car le piratage Wifi est accessible Ã tous en tÃ©lÃ©chargeant simplement un outil sur Internet.

â□¢ De placer des systÃ¨mes de dÃ©tection dâ□□intrusion absolument partout et de recevoir des alertes lors de tentatives dâ□□accÃ¨s au rÃ©seau ou Ã un appareil mÃ©dical.

Pour retrouver Bitdefender en ligne Â