N° 852 – Du 2 au 15 novembre 2016

01net

3,90€

LE MAGAZINE DE LA HIGH-TECH

LEADER DE LA PRESSE TECHNO

TRANSHUMANISME
LE GRAND MENSONGE ?

M 05367 - 852 - F: 3,90 €

PIRATES
ILS ATTAQUENT DÉSORMAIS NOS HÔPITAUX

SYNDIC
CES LOGICIELS DE GESTION POUR REPRENDRE LA MAIN

SIMPLISSIME
LES RECETTES POUR DOPER VOTRE TÉLÉ

10 PAGES PRATIQUES

TEST
YOGA BOOK, UNE PIÈCE D'ORFÈVRERIE À 499 €

COMPARATIF
HUIT CAMÉRAS QUI FILMENT À 360 DEGRÉS

Belgique : 4,50 € > Suisse : 6,50 FS > Luxembourg : 4,50 € > Guyane : 7,60 € > DOM AVION : 5,10 € > TOM AVION : 1 300 CFP > Maroc : 39 DH > Canada : 7,25 CAD > Tunisie : 3,20 TND > Portugal : 4,70 €

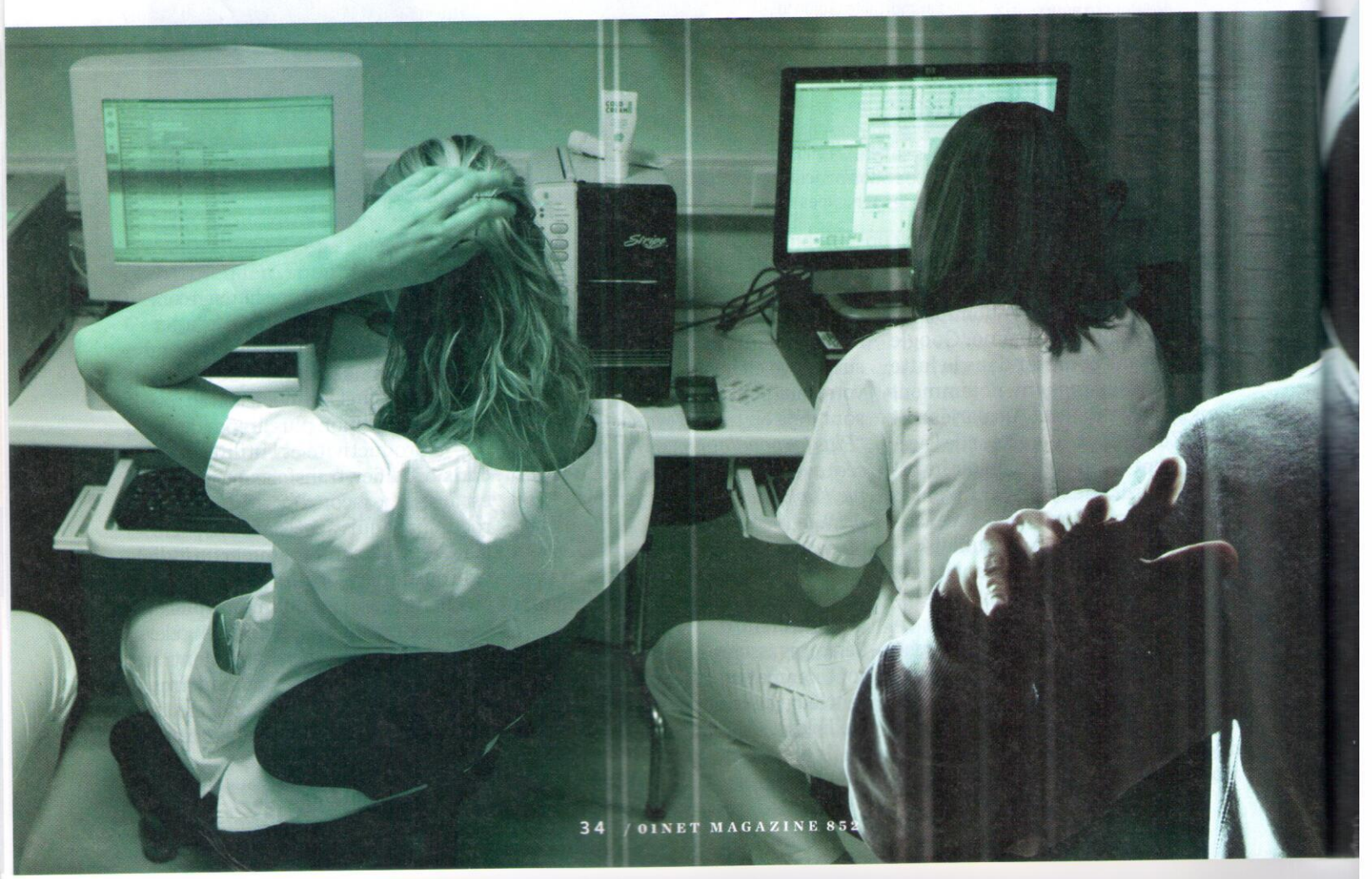
CONTRE-ENQUÊTE

Les pirates À L'ABORDAGE des hôpitaux

Mal protégés, nos établissements de santé sont une proie idéale pour les hackers. Les cyberflibustiers pillent nos dossiers médicaux pour les revendre sur le Web. Ils pourraient bientôt saboter à distance le matériel de soins.

Branle-bas de combat ! L'an dernier, un pirate a obligé les médecins du centre de radiothérapie de Valence, dans la Drôme, à reporter tous leurs rendez-vous. Après avoir pénétré les serveurs de l'établissement de santé, le hacker avait accédé aux données médicales des patients, qui incluaient les doses précises de rayons pour les soigner. Ensuite, il a tout effacé...

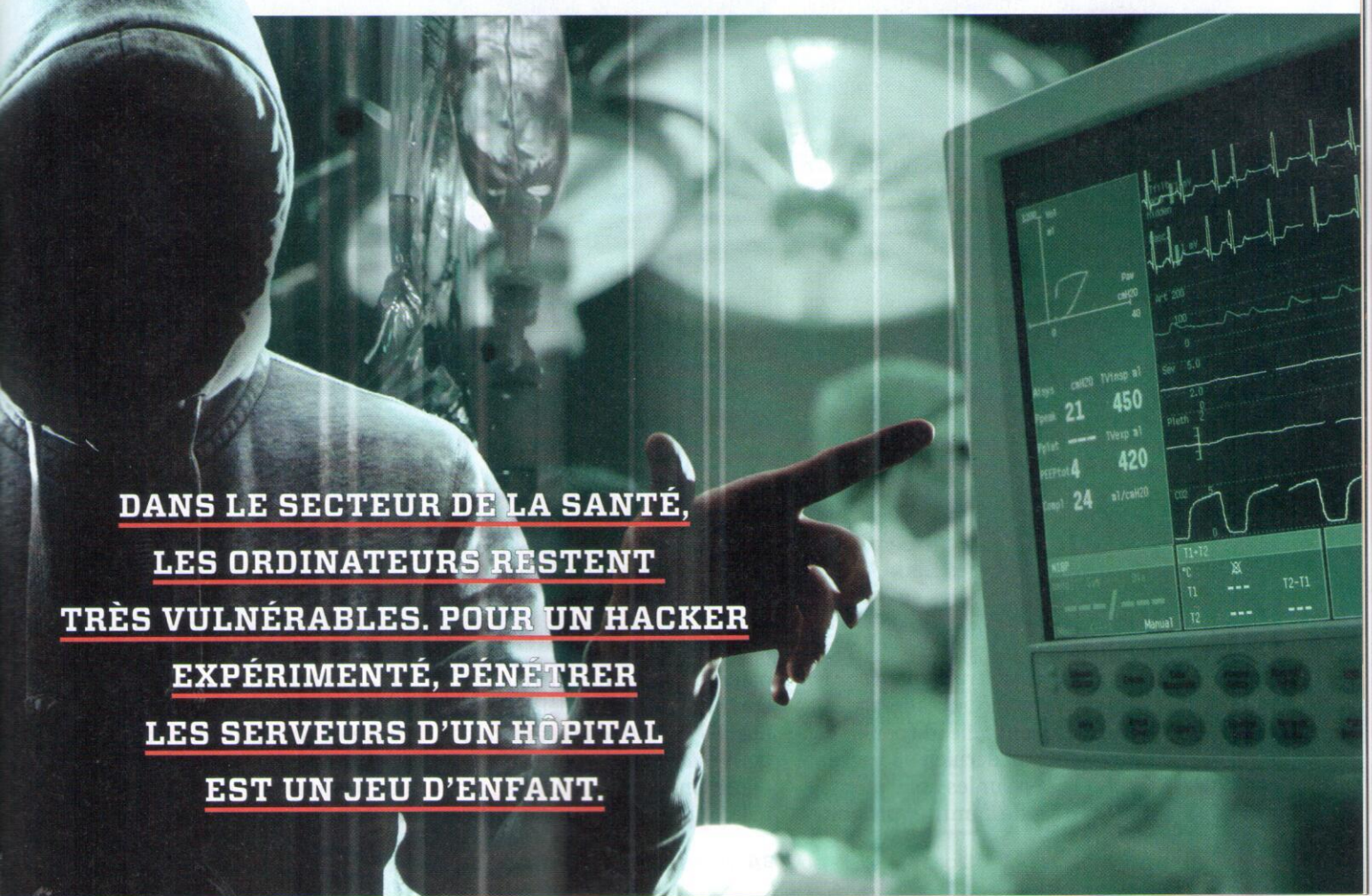
Il y a de quoi s'inquiéter, car cet acte de malveillance est loin d'être un cas isolé. *"L'an dernier, déjà, 1500 attaques de ce genre ont été recensées dans nos hôpitaux"*, s'alarme Stéphane Pasquier, fonctionnaire de sécurité des systèmes d'information adjoint pour le ministère des Affaires sociales et de la Santé.



Depuis, cette menace numérique n'a pas faibli. Chaque jour, en moyenne, six attaques toucheraient les établissements de santé français, devenus les nouveaux souffre-douleur des pirates pour les extorsions de dossiers médicaux, chiffrement de données, demandes de rançons et autres actes de cybersabotage. *"Les hôpitaux sont des proies faciles pour les hackers,* explique Vincent Trély, président de l'Association pour la promotion de la sécurité des systèmes d'information de santé (Apssis). *Contrairement aux banques, qui sont devenues des forteresses numériques, les ordinateurs des professionnels de la santé restent très vulnérables."* La sécurité informatique demeure pourtant le cadet des soucis des responsables des hôpitaux et de leur personnel, qui suent déjà sang et eau pour soigner leurs malades, dans un contexte marqué par les restrictions budgétaires. Pour un pirate expérimenté, pénétrer les serveurs d'un hôpital est donc un jeu d'enfant, comme l'a encore récemment démontré un expert en sécurité. En avril, à l'occasion du congrès national de l'Apssis, il n'a pas fallu plus de cinq minutes à ce gentil hacker pour prendre le contrôle d'un hôpital, puis mettre la main sur des milliers de dossiers médicaux, devant les yeux ébahis des 150 responsables informatiques présents dans la salle.

Chantage et rançon. Les pirates ont plusieurs façons de tirer profit de ces intrusions malveillantes. L'une des plus répandues consiste à injecter dans le système un rançongiciel. Ce programme malveillant se camoufle dans une pièce jointe. Il suffit qu'un salarié ouvre le document pour le répandre à travers tout le système et déclencher le chiffrement des données, qui deviennent dès lors inutilisables. La seule solution pour de nouveau les exploiter, c'est d'obtenir la clé de déchiffrement. Et pour ça, il faut payer une rançon. En février dernier, le Hollywood Presbyterian Medical Center de Los Angeles a ainsi déboursé 17 000 dollars afin de récupérer l'accès à son système d'information, bloqué pendant dix jours par un cybervoyou. Céder au chantage n'offre cependant aucune garantie. Voilà quelques mois, un hôpital du Kansas a versé une rançon de 13 000 euros deux fois de suite sans jamais recevoir la clé de déchiffrement. À l'inverse, en France, l'hôpital Duchenne de Boulogne-sur-Mer (Pas-de-Calais), attaqué à trois reprises en début d'année, a refusé d'entrer dans le jeu de ses maîtres-chanteurs. Grâce aux sauvegardes que ses services opèrent régulièrement, il a pu restaurer les fichiers qui avaient été visés.

Refuser le chantage ? C'est conseillé, mais ce n'est pas non plus la panacée. L'an dernier, le laboratoire français d'analyses médicales Labio avait refusé de verser les 20 000 euros réclamés par le groupe de pirates Rex Mundi. Les



WILFRID MAISY/REA - FOTOLIA

DANS LE SECTEUR DE LA SANTÉ, LES ORDINATEURS RESTENT TRÈS VULNÉRABLES. POUR UN HACKER EXPÉRIMENTÉ, PÉNÉTRER LES SERVEURS D'UN HÔPITAL EST UN JEU D'ENFANT.

hackers ont fini par diffuser sur le Net une partie des informations qu'ils avaient confisqué.

Car les cyberflibustiers ne se contentent plus de chiffrer les données. Ils les dérobent, pour ensuite les revendre sur le Dark Web. Sur cet Internet souterrain, un dossier médical rapporte désormais bien plus qu'un numéro de carte de crédit. *"Un dossier médical avec données personnelles, adresses mails et mots de passe se vend au bas mot 20 euros, alors qu'un code de carte de banc aire se monnaye à moins de 2 euros"*, susurre un expert. La pêche aux dossiers médicaux est même en passe de devenir une véritable ruée vers l'or. La division de recherche en cybersécurité de Cisco évalue le pactole à 100 millions de dollars, pour la seule année 2016. De quoi susciter bien des vocations !

Extorsion de fonds. Cet été, un hacker connu sous son pseudo Dark Overlord a mis en vente sur le Net une base de données de 2 gigaoctets, recensant les informations confidentielles de plus de 9 millions de patients américains. *"Ces données proviennent d'une grande organisation américaine de santé"*, précise-t-il en substance dans sa petite annonce publiée sur The Real Deal, une boutique du réseau Tor, bien connu des aficionados du Web sulfureux. Pour mieux valoriser sa base de données, (noms, adresses, mails, numéros de téléphone et de Sécurité sociale) Dark Overlord promet qu'elle ne sera vendue qu'une seule fois. L'acheteur pourra donc les acquérir en exclusivité pour en tirer profit à son tour. Par exemple, en vendant chaque enregistrement au détail, à des personnes qui voudraient s'en servir pour usurper l'identité des patients enregistrés. Dark Overlord réclame 750 bitcoins, soit environ 450 000 dollars.

Et quand les pirates ne parviennent pas à mettre la main sur les informations médicales des patients, ils s'arrachent celles du personnel. Ainsi, en juin dernier, un hacker a mis la main sur les nom, adresse, situation de famille, parcours professionnel et même montant de la rémunération des quelque 2 400 salariés du centre hospitalier Princesse-Grace de Monaco.

Mais il est probable que les pirates n'en resteront pas là. Comme n'importe quel ordinateur, les instruments médicaux, presque tous reliés à Internet, pourraient devenir les

450 000 DOLLARS POUR LES DONNÉES DE 9 MILLIONS D'AMÉRICAINS

ERIC DULIERE/PHOTOPQR/MAXPPP

Le centre hospitalier Princesse-Grace de Monaco où, en juin dernier, un cyberpirate a mis la main sur la totalité des informations personnelles des quelque 2 400 salariés.

prochaines cibles des hackers. Début octobre, un chercheur en sécurité américain a découvert qu'il était possible de prendre le contrôle à distance de pompes à insuline. Par un signal radio, un pirate serait capable d'administrer une dose mortelle à un patient. L'an dernier, les autorités américaines avaient déjà retiré du marché 400 000 pompes à morphine qui présentaient des failles informatiques. Un hacker aurait pu les manipuler à distance pour déclencher des surdoses. Alors que notre pays est l'un des plus touchés par le cybercrime, comme le confirme l'étude "Global Economic Crime Survey 2016" publiée par le cabinet PwC, ce danger ne semble toujours pas inquiéter les politiques ni les dirigeants des hôpitaux publics et privés. *"Pour un hôpital qui n'aurait pas encore été frappé, la question n'est plus de savoir si l'attaque va avoir lieu, mais quand, et surtout, comment s'y préparer"*, résume Nathalie Devilliers, docteur en droit, dans sa chronique publiée voilà quelques mois sur le site Theconversation.com. La tâche est dantesque.

"Il faut commencer par cartographier les systèmes d'information, puis isoler les postes d'administration, cloisonner les réseaux, mettre en place et vérifier le plan de continuité informatique sans oublier les fondamentaux comme la bonne gestion des mots de passe", énumère Stéphane Pasquier. Las, les moyens humains restent bien insuffisants. Les 1 200 établissements de santé français comptent en tout à peine 50 responsables à plein-temps de la sécurité informatique.

Voilà qui fait de nos dossiers médicaux et de nos équipements de santé un gibier bien tendre pour les meutes de cyberloups aux dents longues et affûtées. ■ **JEAN-BERNARD GALLOIS**