Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de pilotage informatique de la Confédération UPIC
Service de renseignement de la Confédération SRC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
www.melani.admin.ch

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2014/II (juillet à décembre)

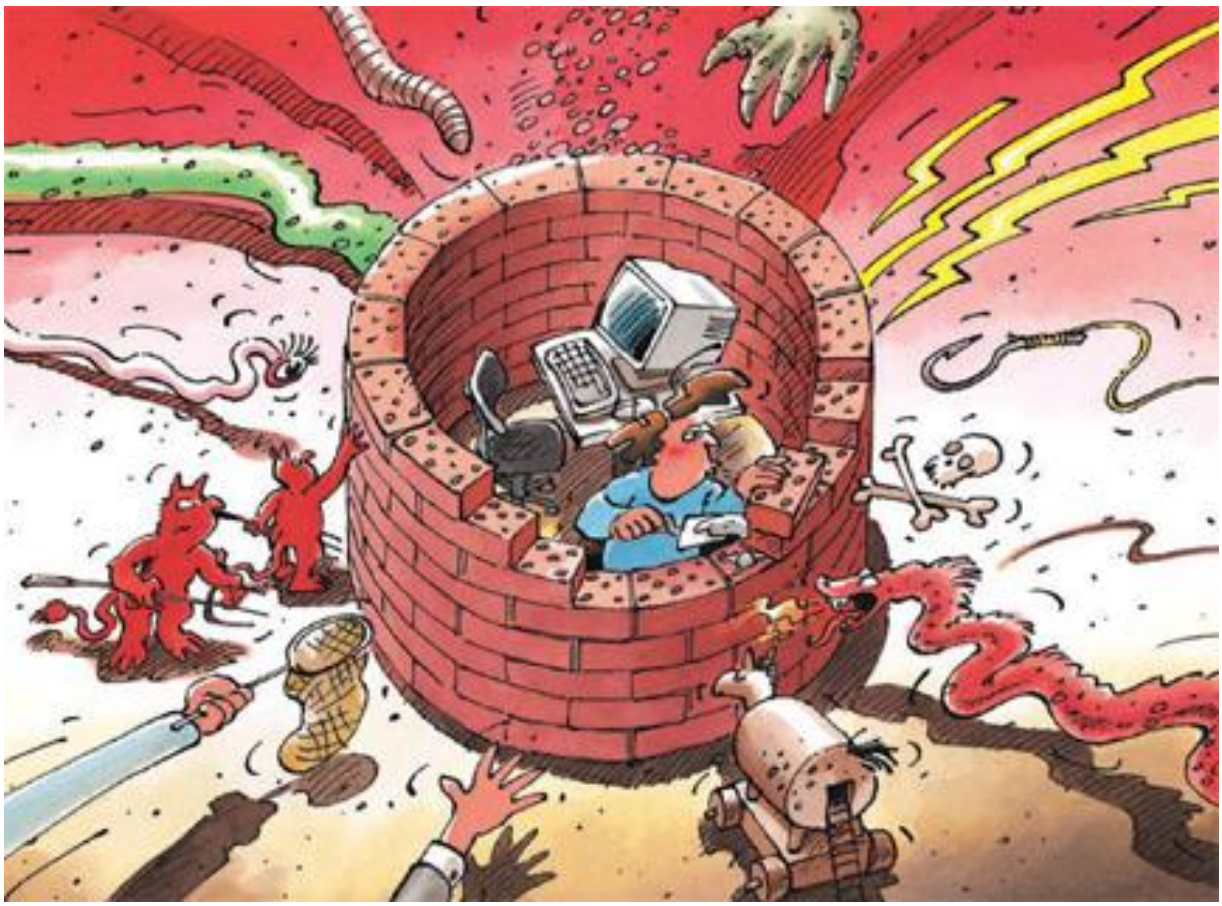

Table des matières

1 Temps forts de l'édition 2014/II

- **Dix ans de MELANI**

  La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a fêté ses dix ans le 1er octobre 2014. Les technologies de l'information et de la communication (TIC) ont connu un essor prodigieux en dix ans. Or les structures criminelles ont proliféré au même rythme que les plateformes, les services et le nombre d'internautes. Un véritable marché clandestin a vu le jour, où n'importe qui peut acheter tout ce qu'il faut pour lancer une cyberattaque. De même, certains Etats ont fortement développé et affiné leurs méthodes d'espionnage et de surveillance. Le chapitre 3.1 rappelle les temps forts de l'évolution d'Internet au cours des dix dernières années, avec d'utiles réflexions sur les perspectives.

  ► Situation en Suisse: chapitre 3.1

- **Nouvelles failles de sécurité dans le cryptage**

  Après Heartbleed, *SSL* a de nouveau subi une défaillance grave. Or à la différence de Heartbleed, la vulnérabilité connue sous le nom de Poodle n'était pas une erreur de programmation, mais une erreur de conception. Il a donc fallu désactiver la norme de cryptage défaillante. D'autres failles de sécurité, sérieuses parfois, ont encore été découvertes. La base de données où la société MITRE répertorie les lacunes de programmes rendues publiques signale au total 7945 vulnérabilités pour l'année 2014, un véritable record. D'où inévitablement la question des processus à suivre, lorsqu'une faille de sécurité a été découverte.

  ► Situation sur le plan international: chapitre 4.9, chapitre 4.10, chapitre 4.11
  ► Tendances / Perspectives: chapitre 5.5

- **Systèmes mal protégés – un danger pas seulement pour les exploitants**

  Les webcaméras accessibles, les réseaux sans fil mal protégés et les *systèmes de gestion de contenu (content management system, CMS)* désuets sont des cibles de choix. Si à première vue de telles agressions ne causent de préjudice qu'à l'exploitant négligent, elles ont souvent d'autres effets encore. Ainsi, les sites Web compromis peuvent servir à des opérations de *phishing* ou à la diffusion de *maliciels*, et les comptes de messagerie piratés à l'envoi de pourriels. Selon des calculs au prorata de la population, la Suisse s'est récemment hissée au troisième rang mondial pour l'envoi de pourriels.

  ► Situation en Suisse: chapitre 3.2, chapitre 3.4, chapitre 3.5

- **Espionnage – au travail, en déplacement et lors des communications**

  Les données sensibles suscitent un intérêt qui ne se relâche pas, et sont soumises à des pressions permanentes. Il ressort des exemples exposés dans le rapport que des actes d'espionnage peuvent être commis à tout moment et partout – au travail, en voyage d'affaires ou lors d'appels à partir d'un téléphone mobile.

  ► Situation sur le plan international: chapitre 4.5, chapitre 4.6, chapitre 4.10

- **Mise en réseau totale. Une solution intelligente et sûre?**

  Les téléphones ne sont plus seuls à être «intelligents»: les véhicules (smart car / smart drive), les logements (smart home) voire des bâtiments entiers (smart building), sans oublier les sites industriels (smart factory / smart manufacturing), sont en mesure de collecter ou recevoir des données, de les traiter et aussi d'en envoyer, de les traduire en commandes et d'exécuter des actions spécifiques. Les risques qui en découlent sont abordés au chapitre 5.2.

  ► Tendances / Perspectives: chapitre 5.2

2 Introduction

Le vingtième rapport semestriel (juillet à décembre 2014) de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI) commente les grandes tendances et les risques liés aux technologies de l’information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l’étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (*écrits en italique*) sont expliqués dans un **glossaire (chapitre 6)** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

Le **chapitre 1** esquisse certains thèmes du présent rapport semestriel.

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six derniers mois de l’année 2014. La situation nationale est analysée au **chapitre 3** et la situation internationale au **chapitre 4**.

Le **chapitre 5** décrit les tendances et donne un aperçu des développements à prévoir.

Le **chapitre 5.6** passe en revue les principales interventions parlementaires se rapportant à la sûreté de l’information.

A l’occasion des dix ans de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information, un tableau des principaux événements des dix dernières années se rapportant à Internet et à la sûreté de l’information est ajouté à ce rapport.

3 Situation en Suisse de l'infrastructure TIC

3.1 Rétrospective des dix ans d'activité de MELANI

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a fêté ses dix ans d'existence le 1er octobre 2014. Les technologies de l'information et de la communication (TIC) ont connu un essor prodigieux durant cette décennie. Un grand nombre de plateformes, de *protocoles* et d'appareils de communication ont vu le jour. Il suffit de penser à l'évolution des *médias sociaux* ou au développement fulgurant des *smartphones*. Rappelons que Facebook n'avait que huit mois, et donc n'en était qu'à ses balbutiements à la création de MELANI. Le service de messages courts Twitter n'est apparu qu'en 2006, et le premier iPhone a été commercialisé un an plus tard. Quant au nombre d'internautes, il a bondi de 900 millions en 2004 à trois milliards déjà en 2014.[1]

Il va de soi que les cybercriminels et autres acteurs hostiles suivent l'évolution technologique et sociétale, et n'ont pas manqué d'exploiter les nouvelles possibilités offertes. Tous ces internautes encore inexpérimentés constituaient autant de proies faciles. En outre, les nouveaux services ou applications ont donné aux escrocs des occasions supplémentaires de trouver des failles et d'en tirer parti. Par exemple, l'emploi de logiciels standardisés de gestion de contenu (*content management system, CMS*), qui bien souvent ne sont pas mis à jour, a multiplié les possibilités d'attaques.[2]

- *Réseaux de zombies*
  Indépendamment des possibilités quasiment illimitées d'attaques qu'un vaste réseau de zombies offre à ses propriétaires, le recours à des milliers d'ordinateurs familiaux et la complicité involontaire de leurs propriétaires constituent un véritable casse-tête pour les autorités de poursuite pénale, les services des renseignements et les spécialistes en TIC. Un changement de paradigme s'impose donc quant à la manière d'effectuer des attaques par Internet et de s'en protéger ou de les poursuivre en justice.

- *Recrudescence de la criminalité organisée*
  Alors qu'il y a peu encore les pirates informatiques avaient pour mobile principal la curiosité, les attaques dirigées contre les infrastructures TIC se font aujourd'hui par appât du gain. La criminalité organisée, d'Europe orientale notamment, joue désormais un rôle accru dans ces attaques.

- *Professionnalisation du piratage informatique*
  Outre l'accent mis sur les intérêts financiers, on assiste à une professionnalisation des pirates. Ils déclenchent parfois de véritables assauts de programmes malveillants, en recourant à des parasites hybrides toujours plus raffinés sur le plan technique, capables de combiner la puissance d'attaque et le potentiel de nuisance de plusieurs programmes.

- *Actes d'espionnage ciblés*
  Au premier semestre 2005, des entreprises ainsi que des systèmes étatiques ont été victimes d'actes d'espionnage ciblés. Les programmes malveillants utilisés étaient spécialement adaptés à la victime, dans le but de retarder la découverte du parasite. Ce dernier sévira d'autant plus longtemps qu'il est inconnu des fabricants d'antivirus.

Fig. 1 : Temps forts de la première édition du rapport semestriel de MELANI: réseaux de zombies, recrudescence de la criminalité organisée, professionnalisation du piratage informatique et actes d'espionnage ciblés.

[1] http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (état: le 28 février 2015).

[2] Voir présent rapport semestriel, chapitre 3.5.

Un coup d'œil au premier rapport semestriel MELANI, paru en 2005, révèle toutefois que les thèmes abordés n'ont guère changé. En 2005 déjà, il était question d'actes d'espionnage ciblés, de *phishing*, d'attaques *DDoS*, de défiguration de sites (*defacement*) et d'ingénierie sociale. Même les risques encourus par les usagers de la téléphonie mobile étaient abordés dans ce premier rapport MELANI, qui traitait aussi de la question toujours d'actualité de l'anonymat dans Internet. Or si les thèmes fondamentaux sont restés plus ou moins les mêmes, les agresseurs se sont considérablement professionnalisés et pratiquent une division toujours plus poussée des tâches. Aujourd'hui, les cybercriminels se spécialisent dans des domaines précis comme la détection des failles, la production de maliciels ou l'envoi de pourriels. Il y a dix ans, le passage du «piratage par pur plaisir» au «piratage avec un dessin d'enrichissement» ne faisait que s'amorcer, et il n'y avait encore que peu d'acteurs dans ce secteur. Entre-temps, un véritable marché clandestin a vu le jour, où n'importe qui peut acheter tout ce qu'il faut pour lancer une cyberattaque. De même, certains Etats ont fortement développé et affiné leurs méthodes d'espionnage et de surveillance.

Bien entendu, le nombre d'attaques a explosé. Les internautes ne sont plus confrontés comme en 2005 à des événements isolés; leurs données et leurs moyens de communication font l'objet de menaces permanentes. Les services qui, comme la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI et ses divers partenaires, opèrent dans le domaine de la sécurité des infrastructures d'information critiques, sont à tout moment confrontés à de nouveaux défis. D'où la nécessité d'étudier les contre-mesures possibles, et de les ajuster le cas échéant. De même, les entreprises doivent constamment intégrer dans leur stratégie de gestion des risques les connaissances existantes sur un contexte en rapide mutation, et adapter en conséquence leurs processus. D'un autre côté, une certaine routine et la sérénité se sont installées. Alors qu'en 2005 encore, p. ex., une vague de *phishing* visant la Suisse provoquait beaucoup d'émoi, que les médias en parlaient abondamment et qu'on ne savait pas comment réagir, la riposte à de telles attaques, qui aujourd'hui se produisent plusieurs fois par jour, est devenue une routine. De même, les médias ne s'intéressent plus qu'aux cas concernant des victimes illustres ou ayant provoqué des pertes spectaculaires.

Il reste encore à savoir si la population est devenue plus consciente des enjeux de sécurité des TIC. Or il ressort clairement des annonces parvenant quotidiennement à MELANI que les utilisateurs font preuve d'une prudence accrue. Mais il est non moins clair qu'il reste un grand potentiel de prévention pour déjouer les futures cyberattaques.

Connaissez-vous les diverses facettes de l'activité déployée depuis dix ans par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI?

- 20 rapports semestriels ont été publiés
- 33 workshops ont été organisés pour les exploitants d'infrastructures critiques
- 111 lettres d'information ont paru
- 141 exploitants d'infrastructures critiques font partie du cercle fermé de MELANI
- 1765 informations émanant d'exploitants d'infrastructures critiques ou leur étant destinées ont été traitées
- Plus de 3000 courriels ont été adressés à des fournisseurs d'accès, afin qu'ils désactivent des sites de *phishing*
- plus de 9000 questions de la population ont reçu une réponse
- plus de 27 000 annonces ont été effectuées à l'aide du formulaire prévu

Afin de rendre compte de ces tendances, MELANI a conçu un poster sous forme de chronologie articulée autour de trois thématiques – Internet, menaces, action de MELANI. Ce poster ne peut prétendre à l'exhaustivité, en raison des nombreux événements ayant marqué la décennie. Il aborde toutefois ces thèmes sous un angle dynamique et pose d'importants jalons. Le poster est ajouté au présent rapport.

3.2 Pourriels expédiés à des citoyens suisses – ou par eux

Outre les habituels *pourriels* vantant par exemple toutes sortes de médicaments ou de remèdes contre l'impuissance, qui inondent depuis plus de dix ans les boîtes aux lettres des internautes, un nombre croissant de pourriels accompagnés d'un *maliciel* en annexe ont circulé au deuxième semestre 2014. Mais à la différence des années précédentes, MELANI a relevé une augmentation des courriels contenant en annexe, à la place d'un fichier exécutable (contenant généralement l'extension *.exe*, *.pif*, *.scr* ou *.com*), un document de texte au format *Rich Text Format* (extension *.rtf*). Le maliciel est intégré dans le document de texte, et le destinataire est invité à ouvrir d'un double-clic le fichier accompagnant le courriel.

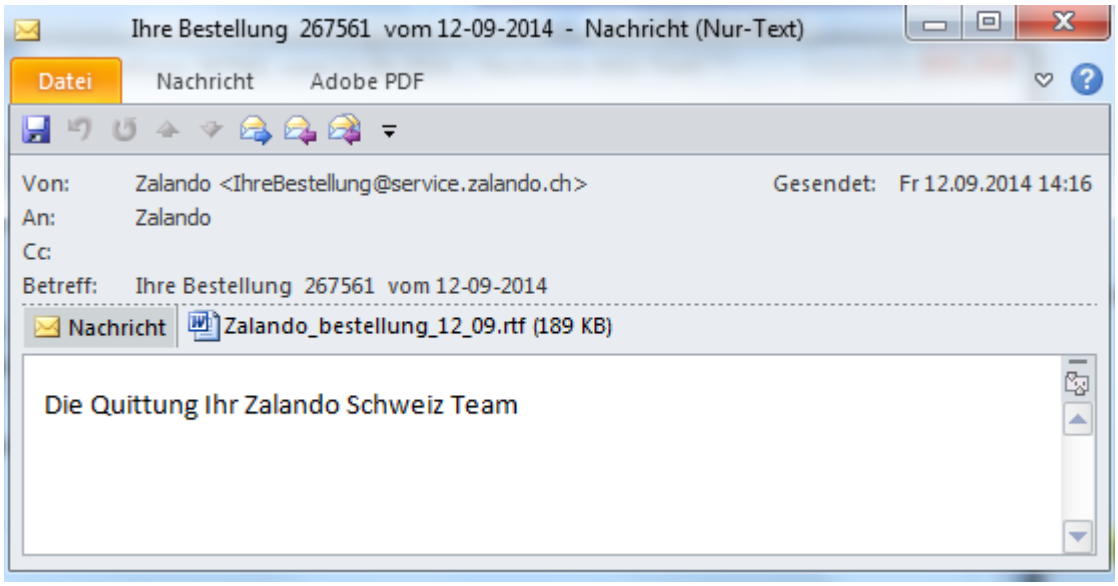

Fig. 2: Courriel falsifié prétendument expédié par Zalando, avec document RTF malveillant en annexe.

Beaucoup de ces campagnes de pollupostage étaient adaptées au marché suisse et prétendaient provenir de distributeurs en ligne réputés, comme p. ex. Zalando ou Le Shop. Ce qui a poussé beaucoup d'utilisateurs en Suisse à ouvrir le document malgré les maladresses de langage du courriel, à exécuter le code malveillant et ainsi à infecter leur machine avec un cheval de Troie spécialisé dans l'e-banking.

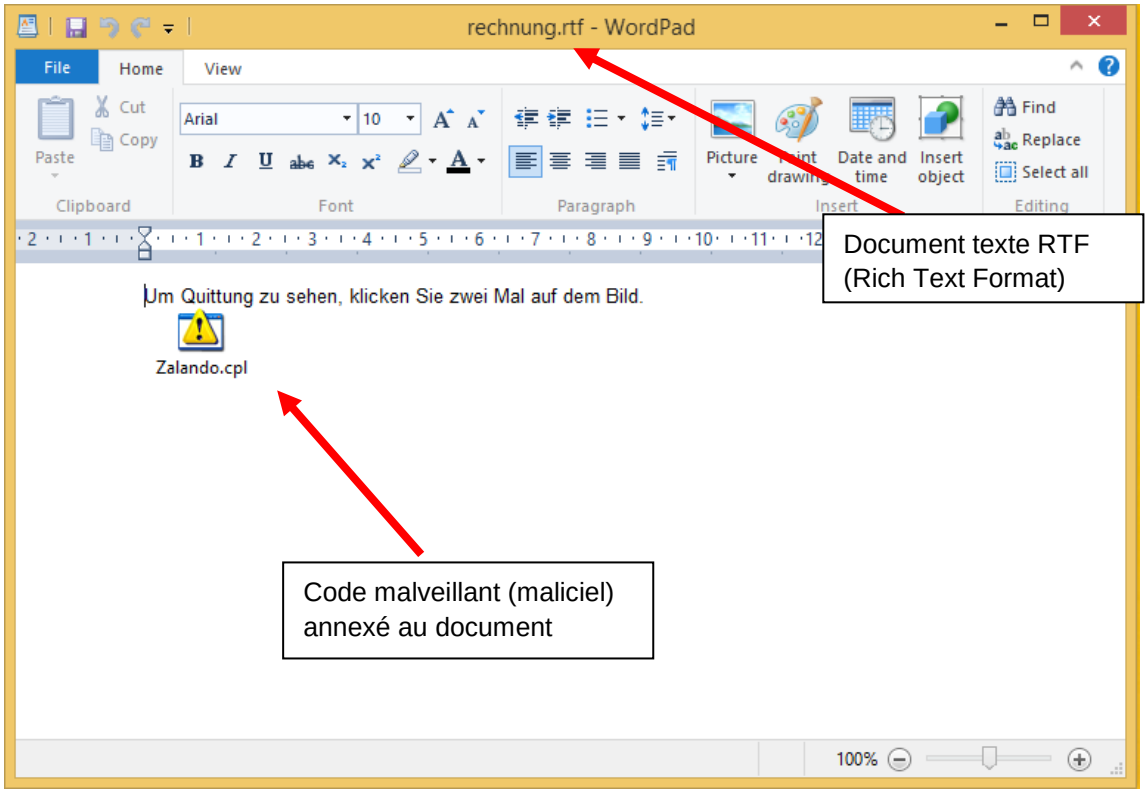

Fig. 3: Exemple de fichier RTF malveillant.

Les internautes suisses ne sont toutefois pas seulement la cible de pourriels, mais expédient souvent ce genre de messages non désirés. C'est du moins ce que révèle un rapport publié en juillet 2014 par le fabricant d'antivirus Sophos[3]. Le nombre de pourriels envoyés y est mis en relation avec la population des pays. Au deuxième trimestre 2014, la Suisse s'est ainsi hissée au troisième rang. MELANI a connaissance de différents cas où l'expéditeur des pourriels venait de Suisse. Dans l'un d'eux, plus de 18 000 pourriels ont été envoyés d'une adresse électronique suisse qui avait été piratée. Le plus souvent, les propriétaires imprudents de tels comptes ont révélé eux-mêmes leurs données d'ouverture de session, lors d'une attaque de *phishing*. Dans d'autres cas, un maliciel s'était glissé dans l'ordinateur à l'origine des pourriels.

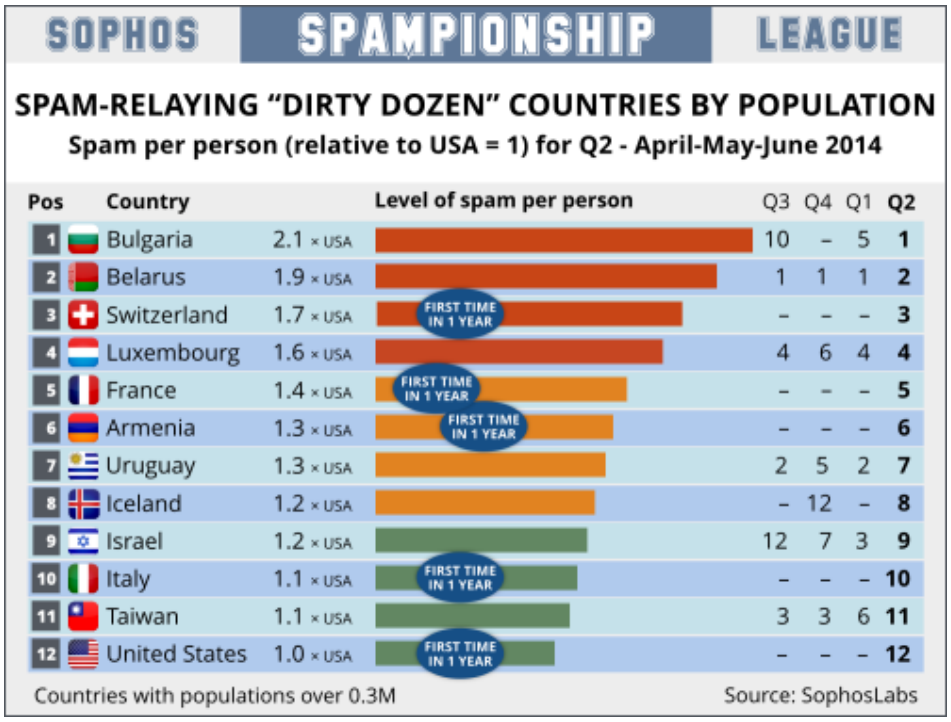

Fig. 4: Statistique (source: Sophos).

MELANI recommande de faire preuve de prudence avec les courriels, et rappelle les règles de comportement à suivre dans ce contexte:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=fr

Pour prévenir ou limiter les falsifications d'adresses d'expéditeurs, MELANI recommande aux fournisseurs de messagerie d'employer des technologies comme SPF ou DKIM:

Sender Policy Framework (SPF):
http://www.openspf.org/

DomainKeys Identified Mail (DKIM):
http://www.dkim.org/

[3] Sophos: Dirty Dozen Spampionship – which country is spewing the most spam? https://nakedsecurity.sophos.com/2014/07/22/dirty-dozen-spampionship-which-country-is-spewing-the-most-spam/ (état: le 28 février 2015).

3.3 Weltwoche: victime d'une cyberattaque

Les événements très polarisants ont toujours plus souvent des retombées sur Internet, a fortiori quand ils portent sur des thèmes religieux ou politiques. Internet joue régulièrement ici un rôle de soupape. Les réactions à l'attentat contre le magazine satirique Charlie Hebdo en sont le dernier exemple: à côté des déclarations de solidarité «Je suis Charlie» parues sur toutes sortes de plateformes de médias sociaux, d'innombrables cas de *défiguration de sites Web (defacement)* ont été signalés, avec publication de propagande islamiste. De telles pratiques ont beau ne pas exiger de grandes compétences informatiques, elles suscitent généralement un vif intérêt de la part des médias et donc ne manquent pas leur effet.

La Suisse également a déjà subi à plusieurs reprises de telles agressions à mobiles politiques ou religieux. Il convient de mentionner ici l'attaque *DDoS* lancée en 2010 contre Postfinance suite au blocage du compte de Julien Assange, fondateur de Wikileaks[4], ou la défiguration de plusieurs milliers de sites après l'adoption, en 2009, de l'initiative contre la construction de minarets[5].

La publication sous la plume d'Andreas Thiel d'un article critique sur le Coran, dans l'édition de la Weltwoche du 28 novembre 2014, a aussi déclenché une réaction de protestation dans le cyberespace: une attaque *DDoS* a longtemps paralysé le site de cet hebdomadaire.[6]

La recrudescence, depuis quelques mois, d'attaques *DDoS* d'une rare violence constitue une évolution préoccupante. A Noël, le groupe de pirates Lizard Squad a mis simultanément hors service, pendant au moins 24 heures, Sony Playstation Network et Xbox Live, deux des géants du divertissement en ligne. Le dommage causé est difficile à chiffrer. Il est dès lors recommandé à toutes les entreprises dont la marche des affaires serait compromise sans accessibilité en ligne et/ou connexion à Internet de tirer au clair, avec les responsables de leur site Web et de son hébergement, les risques de subir une telle attaque, ainsi que de définir des mesures de défense. Il s'agit non seulement de prévoir des mesures techniques pour identifier et déjouer de telles menaces, mais aussi d'évaluer l'aptitude du fournisseur en amont (*upstream provider*) et ses obligations contractuelles en cas d'incident.

3.4 Systèmes mal protégés, dont 141 webcams suisses

Toujours plus d'appareils possèdent une interface *Ethernet* ou *WLAN* et peuvent être raccordés à Internet. A commencer par les webcams, les archives de fichiers, les imprimantes, les scanners et les serveurs de musique ou vidéo. Et la palette devrait encore s'étoffer à l'avenir (voir chapitre 5.2 Mise en réseau totale. Une solution intelligente et sûre?). Or on oublie souvent que ces appareils sont généralement prévus et préconfigurés pour être utilisés dans un réseau interne. Ils ne sont nullement protégés, ou alors seulement par un mot de passe standard, aisé à deviner. D'où l'importance d'un *pare-feu* central ou d'un *routeur* empêchant tout accès direct à partir d'Internet. Si ce n'est pas le cas et si les appareils sont directement raccordés à Internet ou si un accès ouvert a été conçu à dessein,

[4] Voir MELANI, rapport semestriel 2010/2, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: le 28 février 2015).

[5] Voir MELANI, rapport semestriel 2009/2, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=fr (état: le 28 février 2015).

[6] http://www.tagesanzeiger.ch/schweiz/standard/Nach-KoranKritik-Weltwoche-ist-Opfer-einer-CyberAttacke/story/19607439 (état: le 28 février 2015).

n'importe qui peut les repérer et en théorie les consulter, si le mot de passe est faible ou a fortiori s'il n'y en a aucun.

Un tel incident a fait les gros titres en novembre 2014. De nombreux journaux ont signalé que des milliers de webcams avaient été piratées et qu'un site russe permettait de visionner leurs images en direct. Parmi elles, 141 webcams ont pu être localisées en Suisse.[7] Si certaines images, montrant p. ex. des entrées de garages, étaient peu spectaculaires, d'autres provenant p. ex. de caméras pour la surveillance de chambres d'enfants (baby cams) étaient sensibles. Une analyse plus approfondie a révélé que les cyberpirates s'étaient contentés d'utiliser des mots de passe standard. Les utilisateurs avaient négligé de modifier le mot de passe d'origine.

Les appareils directement reliés à Internet requièrent une protection particulière. Il s'agit non seulement d'y introduire des mots de passe conformes aux exigences les plus récentes, mais aussi de les mettre systématiquement à jour à l'aide des plus récents logiciels ou microprogrammes (*firmware*).

Ce cas relève donc moins du piratage que de la négligence de l'utilisateur au stade de la configuration. Il montre toutefois de manière exemplaire que même l'accès aux caméras intéresse les criminels. Cela tient notamment à ce qu'aujourd'hui, beaucoup d'appareils sont dotés de webcams (smartphones, tablettes, ordinateurs portables, divers téléviseurs). En outre, les utilisateurs ont rarement pris conscience des risques liés aux caméras intégrées. Au cas où un maliciel serait installé sur un appareil doté d'une caméra, son propriétaire s'expose à être espionné, ce qui peut entraîner de sérieux inconvénients, sachant qu'un smartphone est pris partout.

MELANI recommande de recouvrir d'un ruban adhésif les webcams inutilisées. Il existe désormais aussi des cache webcam, permettant d'obturer temporairement la lentille de la caméra.

Fig. 5: Cache webcam coulissant en position ouverte (à gauche) et fermée.[8]

[7] http://www.tagesanzeiger.ch/digital/internet/141-Schweizer-Webcams-gehackt-und-live-ins-Netz-gestellt/story/20973442 (état: le 28 février 2015).

[8] http://www.soomz.io (état: le 28 février 2015).

3.5 CMS – failles de sécurité et négligence des administrateurs Web

Une grande partie des pages de *phishing* et des *infections par drive-by download* sont placées sur des sites Web administrés par des systèmes de gestion de contenu (*content management system, CMS)* n'ayant pas été actualisés. En 2014, pas moins de 14 failles de sécurité ont été découvertes dans le logiciel Drupal, neuf dans Joomla! et même 29 dans Wordpress.[9] Il est donc essentiel que chaque exploitant de site Web actualise régulièrement son logiciel CMS – activité trop souvent négligée. On trouve encore beaucoup d'exploitants qui installent un CMS, puis omettent d'effectuer des mises à jour régulières. Or il existe des outils permettant de détecter et d'attaquer automatiquement les sites Web vulnérables. Les escrocs ont donc beau jeu de découvrir et de manipuler un nombre élevé de sites Web.

Un cas particulièrement grave a conduit Google à bloquer 11 000 pages de son index de recherche. Mais le maliciel Soak Soak avait selon différentes sources déjà infecté plus de 100 000 sites WordPress, s'introduisant par ce biais sur les ordinateurs des visiteurs des pages en question.

Dans un autre cas, les escrocs ont trouvé une alternative aux failles de sécurité. Ils offraient gratuitement aux exploitants de CMS un thème graphique piraté. Le plugiciel (*plug-in*) contenait un logiciel malveillant, livrant accès au serveur Web. CryptoPHP, maliciel conçu pour Drupal, WordPress ou Joomla, a infecté des dizaines de milliers de serveurs. Ses victimes pratiquent le *BHSEO (Black Hat Search Engine Optimization)*, opération consistant à ajouter des mots-clés ou des pages manipulées sur les sites compromis, afin d'en influencer le classement (*ranking*) dans les moteurs de recherche. Grâce à leur accès aux serveurs Web ainsi piratés, les escrocs peuvent également modifier le contenu des sites et y introduire des *infections par drive-by download* ou des *pages de phishing*, ou simplement diffuser de fausses informations. Les serveurs Web infectés par CryptoPHP agissent en outre comme un *réseau de zombies*.

Les corrections de programmes ou *patch*ing (consistant à reprendre régulièrement les mises à jour de sécurité) limitent fortement l'impact des attaques contre les CMS. Une panoplie d'autres mesures contribue à la sécurité des CMS. Des recommandations à ce sujet figurent sur le site MELANI, à la rubrique «Listes de contrôle et instructions».[10]

3.6 Essor des logiciels de chantage: méfaits de Synolocker

La liste des logiciels de chantage ne cesse de s'allonger. Alors qu'il y a quelques années de tels maliciels (*ransomware*) se contentaient de bloquer l'écran, que quelques manipulations suffisaient à débloquer, les versions actuelles ont un potentiel de nuisance bien plus élevé. Après Cryptolocker, analysé dans le dernier rapport semestriel, un nouveau maliciel appelé Synolocker est apparu dans la période sous revue. En Suisse aussi, de nombreux cas ont été signalés à MELANI. Toutes les données du serveur de stockage en réseau (*Network Attached Storage, NAS*) infecté sont cryptées, et la victime est priée de verser une rançon en échange de la clé privée requise. En effet, seule la clé publique nécessaire au cryptage en mode asynchrone a été installée sur son ordinateur, et il est pratiquement impossible de décrypter les données sans la clé privée correspondante. En l'occurrence, l'infection ne

9 http://www.cvedetails.com (état: le 28 février 2015).

10 http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=fr

nécessitait aucune interaction de l'utilisateur, mais exploitait de façon ciblée une faille de sécurité des appareils NAS de la société Synology. Il ne s'agissait toutefois pas d'une vulnérabilité inconnue, puisqu'un correctif (*patch*) est proposé depuis décembre 2013.[11] Un autre maliciel avait apparemment exploité la même faille de sécurité dès février 2014. A l'époque, les pirates avaient installé sur les appareils NAS des programmes de minage de bitcoins, et produit ainsi des crypto-monnaies.[12]

On a trop tendance à oublier que les routeurs, les serveurs de stockage en réseau et les appareils similaires nécessitent eux aussi des mises à jour (voir rapport semestriel 1/2014[13]). C'est particulièrement important si ces appareils sont directement raccordés à Internet.

Un autre cheval de Troie appelé CTB-Locker est apparu en août 2014. Il a pour particularité de communiquer sous forme cryptée avec ses serveurs de commande et de contrôle (C&C) et d'utiliser le *service d'anonymisation Tor* pour brouiller les pistes. D'où les réelles difficultés de la police et des entreprises de sécurité à localiser et analyser lesdits serveurs.

Il y a également eu de bonnes nouvelles au deuxième semestre 2014: les entreprises de sécurité informatique FireEye et Fox-IT ont mis à disposition un service gratuit, permettant aux victimes de Cryptolocker de récupérer leurs données verrouillées.[14] Une action lancée par le FBI contre ce *réseau de zombies* a en effet abouti à la découverte des clés privées. Il est ainsi possible de décrypter les données d'origine. Il n'est donc pas exclu que dans le cas de Synolocker aussi, les recherches et investigations aident à retrouver un jour les clés de cryptage correspondantes. Les propriétaires de données cryptées par Synolocker et non récupérables feraient donc bien de les garder malgré tout.

Il est indiqué de copier régulièrement ses données sur des supports de stockage externes (*backup*). Ces appareils ne seront reliés à l'ordinateur que pendant le processus de sauvegarde. En outre, il faut veiller à mettre systématiquement à jour tant les systèmes d'exploitation que la totalité des applications installées (p. ex. Adobe Reader, Adobe Flash, Sun Java, etc.). Dans la mesure du possible, la fonction de mise à jour automatique sera activée. La remarque vaut également pour les microprogrammes (*firmware*) des *routers*, des *NAS*, des serveurs de musique, etc.

3.7 Swiss Internet Security Alliance – collaboration pour plus de sécurité

Soucieux de combattre ensemble la cybercriminalité, des fournisseurs Internet, des banques et d'autres partenaires ont créé le 12 septembre 2014 la Swiss Internet Security Alliance (SISA). A travers ce partenariat intersectoriel, les membres soulignent leur engagement pour la sécurité de leurs prestations ainsi que de leurs clients. La SISA s'appuie sur l'expertise de différents représentants du secteur, afin de favoriser les échanges d'informations entre concurrents. Elle mise sur le savoir, l'expérience et les compétences techniques de ses

[11] http://www.heise.de/security/meldung/Jetzt-updaten-Aeltere-Synology-NAS-Geraete-anfaellig-fuer-Ransomware-2287427.html (état: le 28 février 2015).

[12] http://www.synology-forum.de/showthread.html?50468-Aktive-Hackangriffe-auf-DSM-Versionen-kleiner-4-3-3810-Update-3 (état: le 28 février 2015).

[13] Voir MELANI, rapport semestriel 2014/1, chapitre 4.13: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=fr (état: le 28 février 2015).

[14] https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html (état: le 28 février 2015).

membres, qui constituent son véritable capital. Parmi ses membres figurent l'asut, Centralway, Credit Suisse, cyscon Suisse, la Haute école spécialisée lucernoise, Hostpoint, la Banque Migros, PostFinance, Raiffeisen, Sunrise, Swisscard, Swisscom, SWITCH, UBS, upc cablecom et Viseca. Tous jouissent d'une longue expérience en matière de sécurité sur Internet. L'association reste ouverte aux autres acteurs intéressés.[15]

[15] https://www.swiss-isa.ch/ (état: le 28 février 2015).

4 Situation internationale de l'infrastructure TIC

4.1 Cyberattaque contre le réseau de Sony Pictures Entertainment

Le 24 novembre 2014, les salariés de Sony Pictures Entertainment (SPE) ont appris en allumant leur ordinateur qu'un groupe de pirates se faisant appeler Guardians of Peace avait piraté leur réseau d'entreprise. Le groupe se vantait d'avoir copié des données internes et menaçait de les publier. Non seulement le maliciel était capable de dérober des données, mais il posséderait une routine d'effacement des données. Le réseau entier est ensuite resté inaccessible plusieurs jours. Les Guardians of Peace prétendaient détenir 100 terabytes de données, soit l'équivalent de 150 000 CD-ROM. Ils auraient copié des données sensibles, comme la liste des salaires des 6000 collaborateurs et des cadres au plus haut niveau, de la correspondance interne, mais aussi des films pas encore sortis. Cinq films ont en effet circulé au début de décembre sur des bourses d'échange, et une version du scénario du nouveau James Bond «Spectre» est parue sur le réseau. Le 21 novembre 2014 déjà, la direction de SPE avait reçu un message de chantage demandant une grosse rançon. Un autre groupe nommé God's Apostls l'y menaçait de déclencher une «attaque totale», en l'absence de compensation du grave préjudice – non précisé – causé par SPE. Le délai signalé à la direction était le 24 novembre, date à laquelle la cyberattaque a été rendue publique.[16] Le lien entre les groupes Guardians of Peace et God's Apostls n'a toutefois pu être élucidé.

Le rapprochement n'a pas tardé à être fait entre l'attaque et le lancement imminent du film «L'Interview qui tue!». Il s'agissait d'une comédie satirique sur un complot de la CIA visant à supprimer Kim Jong-un, leader nord-coréen, dont la sortie en salle était prévue à Noël. En juillet déjà, l'ambassadeur nord-coréen aux Nations Unies s'était plaint auprès du Secrétaire général des Nations Unies du scénario du futur film. Le 1er décembre 2014, des experts américains ont soupçonné la cyberattaque contre Sony d'être d'origine nord-coréenne.[17] Le 8 décembre, un message des Guardians of Peace publié sur le site du service d'hébergement GitHub a exigé explicitement de renoncer à publier le film: «Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!».

Le FBI, mandaté pour élucider l'affaire, a publié ses premiers résultats le19 décembre.[18] Les enquêteurs ont signalé avoir récolté suffisamment d'informations pour conclure que le gouvernement nord-coréen était à l'origine de cette attaque. Par exemple, le maliciel ayant détruit les données était apparenté à un maliciel antérieur développé par la Corée du Nord. Des similitudes auraient été découvertes dans le code de programmation, dans les algorithmes de cryptage et les mécanismes de destruction des données. En outre, des recoupements frappants étaient possibles entre les infrastructures utilisées et des attaques antérieures attribuées à ce pays. Ainsi, les adresses IP programmées dans le maliciel avaient communiqué avec des infrastructures nord-coréennes déjà connues. De même, il y avait des similitudes avec les attaques de mars 2013 ayant pris pour cibles des banques et

16 http://www.hotforsecurity.com/blog/leaked-emails-reveal-that-hackers-demanded-money-from-sony-pictures-before-attack-10964.html (état: le 28 février 2015).

17 http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202 (état: le 28 février 2015).

18 http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (état: le 28 février 2015).

des stations de radio sud-coréennes (DarkSeoul)[19], que le FBI avait également attribuées à la Corée du Nord.
Le Ministère des affaires étrangères nord-coréen a aussitôt réfuté les accusations, en se disant en mesure de prouver que l'attaque n'avait rien à voir avec son gouvernement. Il a également invité les Etats-Unis à mettre en place une équipe commune d'enquête.
Le 7 janvier 2015 James Comey, patron du FBI, a répété lors d'une conférence sur la cybersécurité organisée à New York que les services secrets américains considéraient que les attaques avaient été lancées par la Corée du Nord.[20] Il n'a pas fourni de détails. Mais le FBI aurait découvert de graves erreurs commises par les pirates. Le groupe Guardians of Peace avait ainsi posté divers messages sur son compte Facebook et aurait utilisé des adresses IP nord-coréennes pour se connecter.[21] Après avoir réalisé son erreur, il s'était servi d'ordinateurs installés à l'étranger pour brouiller les pistes.
Selon plusieurs sources, la Corée du Nord ne serait pas le seul acteur à l'origine de cette cyberattaque. Quelques experts ont soupçonné un délit d'initié. Un ex-collaborateur de Sony licencié en mai 2014 aurait été mêlé à l'attaque.[22]

Les Etats-Unis ont durci le ton avec la Corée du Nord suite à cette attaque contre Sony Pictures Entertainment. Des sanctions pénales ont été prononcées contre dix responsables du régime de Pyongyang, ainsi que contre trois organisations ou entreprises.

En réaction aux cyberattaques répétées visant des entreprises ou le gouvernement fédéral, les Etats-Unis prévoient de créer une nouvelle autorité, intitulée Cyber Threat Intelligence Integration Center. Le CTIIC sera chargé de canaliser et d'analyser les informations issues de différentes sources.

Cet incident montre l'extrême difficulté, dans le cyberespace, d'apporter des preuves concluantes d'agressions attribuées à un Etat. Il est vrai que contrairement aux attaques conventionnelles, il existe de multiples possibilités de dissimuler l'origine d'une attaque et de lancer de fausses pistes. D'un autre côté, on aurait tort de croire que des fonctionnaires sont seuls assis à leur écran, en cas de cyberattaque d'origine étatique. La frontière est sans doute ténue entre les attaques étatiques et celles commanditées ou simplement tolérées par un Etat. Dans le meilleur des cas, on découvrira des cyberpirates résidant dans un pays précis. Or la preuve de l'implication étatique est encore loin d'être faite, et il faudrait enquêter sur place pour pouvoir l'apporter – ce qui est impensable dans de telles circonstances.
Par conséquent, les recherches portent fréquemment sur les mobiles des agresseurs. En l'absence d'enjeu monétaire, on a tôt fait de conclure à une attaque professionnelle, d'origine étatique. Or déjà avant la mise en circulation de CD contenant des données bancaires intéressant les autorités fiscales, des individus ont dérobé de leur propre chef des données sensibles, afin de les écouler auprès de gouvernements. La structure du marché cybercriminel est bien trop complexe pour se laisser réduire à une formule simple et généralisable. En l'occurrence, il se peut très bien que plusieurs acteurs soient en cause, et que leur interaction ait contribué à l'ampleur de l'incident survenu.

---

19 Voir MELANI, rapport semestriel 2010/2, chapitre 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 28 février 2015).

20 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (état: le 28 février 2015).

21 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (état: le 28 février 2015).

22 http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/ (état: le 28 février 2015).

4.2 Piratage d'installations industrielles

Les installations industrielles sont toujours plus connectées au réseau. Même si elle simplifie les contrôles et la maintenance, une telle situation accroît les risques d'accès indésirable et de manipulations. Après les acteurs étatiques aux visées stratégiques qui, le cas échéant, s'intéressent à ce genre d'installations pour des raisons militaires, la curiosité des experts en sécurité et des pirates amateurs est en éveil. C'est ainsi qu'au 31e congrès du Chaos Computer Club, organisé en décembre 2014, il a été question des systèmes *SCADA* et des systèmes de contrôle industriels.[23] Des simulateurs de systèmes de pilotage comme ceux utilisés dans l'industrie chimique ont été mis au point et permettent aux amateurs de tester leurs aptitudes au cyberpiratage. En outre, des kits (*exploit-kit*) ont été spécialement programmés pour identifier et exploiter les failles de sécurité des installations industrielles.

Un rapport publié en décembre 2014 par l'Office fédéral allemand de la sécurité dans la technologie de l'information (BSI)[24] fait état d'une attaque ciblée survenue outre-Rhin contre une aciérie, qui aurait infligé des dégâts à un haut fourneau. Grâce à un courriel de phishing ciblé (*spear phishing*) et à des méthodes raffinées d'ingénierie sociale (*social engineering*), les escrocs auraient accédé au réseau administratif de l'entreprise, d'où ils se seraient glissés par étapes dans les réseaux de production. La défaillance de plusieurs composants ou d'une installation complète a empêché l'arrêt contrôlé d'un haut fourneau, endommageant l'infrastructure. Selon le BSI, non seulement les pirates disposaient de capacités techniques très avancées, mais ils maîtrisaient encore les processus de production et de contrôle industriels. Le rapport du BSI reste factuel et n'émet aucune hypothèse sur les auteurs possibles de l'attaque.

Les auteurs d'actes de pur sabotage sont souvent mus par les mêmes mobiles: tantôt un concurrent cherche à se procurer un avantage compétitif, tantôt un (ancien) collaborateur mécontent veut nuire à son employeur en tirant parti de son savoir d'initié, ou encore des tiers visent à prouver tout ce qu'il est possible de faire. Dans le cas d'espèce, il paraît peu probable qu'un Etat étranger ait voulu saboter la production d'acier allemande. Encore que les stratégies militaires et les scénarios de guerre examinent de plus en plus le potentiel du cybersabotage.

La menace de sabotage s'avère pour les escrocs un intéressant moyen de chantage contre les exploitants d'installations.[25] Avec des chances de succès d'autant plus réelles que l'installation est tributaire de ses liens à d'autres réseaux ou systèmes, et qu'il n'est pas possible de la déconnecter sur-le-champ. On peut également imaginer qu'un maliciel soit entré clandestinement et sévisse à un moment donné, indépendamment de la connexion à Internet. En pareil cas, il ne servirait à rien de retirer le système du réseau, puisqu'il faudrait trouver le maliciel et le rendre inoffensif. Ce qui peut être un casse-tête, si le système est d'une grande complexité et faute de savoir précisément où chercher.

Il est important d'étudier l'aspect sécuritaire, avant tout raccordement de systèmes physiques au réseau. Les principaux vecteurs d'attaque des systèmes de contrôle sont le réseau administratif, les *médias amovibles* et les failles de sécurité des accès à distance. D'où l'utilité de dûment segmenter les réseaux (en séparant hermétiquement du réseau destiné à l'administration les systèmes de contrôle et, si des échanges de données s'avèrent nécessaires, en les contrôlant bien), d'utiliser des périphériques amovibles adéquats et soumis à des contrôles réguliers, ainsi que de sécuriser les accès à distance par des

[23] https://events.ccc.de/congress/2014/wiki/

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[25] Voir aussi chapitre 5.3 du présent rapport semestriel.

méthodes d'authentification robustes et en cryptant les échanges de données. Voir la liste de contrôle de MELANI «Mesures de protection des systèmes de contrôle industriels (SCI)».[26]

4.3 Cyberattaques contre le secteur énergétique et pétrolier

En août 2014, on a appris que près de 300 entreprises norvégiennes du secteur énergétique et pétrolier avaient été victimes d'une cyberattaque. Les agresseurs avaient obtenu un certain succès avec des méthodes d'ingénierie sociale (*social engineering*). Aux dires des autorités de sécurité norvégiennes, des recherches leur avaient servi dans un premier temps à identifier pour chaque entreprise les fonctions-clés et les personnes responsables, puis à envoyer à ces dernières des courriels sur mesure, en apparence légitimes mais renfermant des maliciels en annexe. En cas d'ouverture d'une telle annexe, un *kit d'exploit* s'installait, analysait le système à la recherche de vulnérabilités, puis importait le cas échéant un logiciel d'espionnage hautement spécialisé. Cette approche permettait de repérer les secrets de fabrique, ainsi que les données d'accès à d'autres systèmes.

Depuis longtemps déjà, les entreprises du secteur énergétique – notamment celles assurant l'approvisionnement en pétrole et en gaz – sont sujettes aux cyberattaques.[27] Cela peut être dû à l'importance politique et plus encore économique du secteur. En effet, certains acteurs tentent de s'assurer par l'espionnage un avantage en matière d'information face à la concurrence – étatique ou privée. D'autres cherchent de manière ciblée à saboter l'activité d'entreprises énergétiques, pour pouvoir ensuite profiter directement de l'arrêt de production ou des fluctuations du cours des actions. Il convient enfin de rappeler l'enjeu stratégico-militaire – pour l'approvisionnement en carburants notamment– des agents énergétiques fossiles, enjeu amenant les acteurs étatiques à intervenir dans un but offensif ou défensif.

4.4 Attrait des terminaux de paiement (*point of sale*)

Nous avons déjà eu par le passé l'occasion de thématiser la problématique des attaques visant les terminaux de *points de vente*, comme celle ayant touché le distributeur nord-américain Target[28]. La finalité principale de ces attaques est d'obtenir des données de cartes de crédit, même si d'autres données personnelles sont parfois dérobées en parallèle. La fin de l'année 2014 a vu un nouveau cas similaire faire la une des journaux: le 14 septembre, le distributeur américain Home Depot a admis avoir été victime d'un vol des données de 56 millions de cartes de crédit et débit de clients, perpétré entre avril et septembre 2014. Cette communication confirmait et précisait les nombreuses informations publiées les semaines précédentes par des journaux ou blogs spécialisés. La méthode utilisée pour l'attaque rappelle fortement ce qui avait été observé dans le cas de Target: un maliciel de type *Ram Scraper* a été installé sur les points de vente, après une compromission initiale ayant touché un fournisseur de l'entreprise.

Ce mode opératoire n'est d'ailleurs pas le seul utilisé par les criminels pour compromettre des terminaux de points de vente. En juillet 2014 déjà, l'entreprise de sécurité FireEye a

[26] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=fr (état: le 28 février 2015)

[27] Voir MELANI, rapport semestriel 2014/1, chapitre 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=fr (état: le 28 février 2015).

[28] Voir MELANI, rapport semestriel 2013/2, chapitre 4.4, Attaques visant les points de vente Target: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 28 février 2015).

attiré l'attention sur le maliciel BrutPOS. Ce dernier cherche à exploiter des interfaces d'administration à distance de terminaux, protégées par des mots de passe faibles. Pour identifier les systèmes vulnérables, BrutPOS utiliserait selon FireEye un réseau de zombies composé de plus de 5500 machines infectées. Pour ce faire, des mots de passe standards sont essayés, p. ex. «admin», «client» ou «password». Une fois le système pénétré, les criminels cherchent à obtenir des données de cartes de crédit par Ram Scraping.

Ces exemples prouvent que les terminaux de points de vente restent au cœur des préoccupations de certains gangs criminels. D'importants moyens sont investis pour accéder à de tels systèmes, dans l'espoir de réaliser de gros profits. Les données de cartes de crédit saisies sont bien souvent revendues sur des forums clandestins, et au final utilisées pour réaliser des achats à l'insu du propriétaire de la carte. Si les entreprises américaines sont surtout attaquées, c'est qu'il s'agit de cibles intéressantes. Outre qu'elles réalisent un gros volume d'affaires, leur niveau de protection laisse souvent à désirer. En effet, alors qu'il est largement répandu en Europe, le système de paiement par carte de crédit avec puce et PIN («chip and pin») n'est guère utilisé aux Etats-Unis[29]. Même si des attaques de prestataires utilisant ce dernier système sont aussi envisageables, les systèmes n'intégrant pas cette norme présentent pour l'instant un rapport coût-bénéfice plus favorable.

Plus spécifiquement, le cas du réseau de zombies BrutPOS rappelle la nécessité de protéger toute interface permettant d'accéder à distance à un appareil ou système. MELANI a signalé à maintes reprises les risques que comporte la tendance à raccorder au réseau toujours plus d'appareils de pilotage des processus physiques, dans l'industrie productive comme en domotique. Car les appareils ou systèmes concernés ont beau être différents, les règles de sécurisation de l'accès à distance restent en grande partie les mêmes.

4.5 Espionnage – incidents du deuxième semestre

Regin – indices relatifs au créateur probable

Plusieurs incidents d'espionnage ont été révélés au dernier semestre également. Les rapports publiés en novembre 2014 par Symantec, Kaspersky et F-Secure à propos d'un maliciel du nom de Regin ont fait grand bruit.[30] Pendant plusieurs années, le cheval de Troie Regin aurait discrètement espionné diverses victimes, dont des cibles basées en Russie et en Arabie saoudite, mais aussi en Europe de l'Ouest, comme en Belgique et en Autriche. Regin offrirait à ses programmeurs des possibilités de surveillance à grande échelle, et aurait servi tout à la fois contre des organisations gouvernementales, des exploitants d'infrastructures, des entreprises, des instituts de recherche et des particuliers. Les activités d'espionnage visant les prestataires télécom méritent une mention spéciale: un cas sur quatre aurait touché de tels opérateurs. Symantec a ainsi découvert une fonction ciblant les stations de base GSM. Kaspersky, qui s'intéressait aussi à ce maliciel, a précisé qu'en avril 2008, Regin avait dérobé des codes d'accès d'administrateurs permettant de manipuler des réseaux GSM au Moyen-Orient. Peu après, le site «The Intercept» a signalé que Regin aurait notamment été utilisé contre l'opérateur Belgacom. Les documents publiés par le lanceur d'alerte Edward Snowden ont conduit ce site à soupçonner les services secrets

[29] Aux Etats-Unis comme dans beaucoup d'autres pays, la plupart des cartes de crédit en circulation renferment des données enregistrées sur une bande magnétique.

[30] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance (état: le 28 février 2015).
http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks (état: le 28 février 2015).

britanniques (GCHQ). En janvier 2015, Kaspersky a publié de nouveaux éléments de preuve. Cette entreprise de sécurité a découvert des similitudes entre Regin et un maliciel du nom de Qwerty. Or l'hebdomadaire allemand «Der Spiegel» avait publié peu de temps avant le *code source* de Qwerty, qui figurait dans la masse de documents copiés par Edward Snowden. Qwerty constituerait le module d'enregistreur de frappes (*keylogger*) de Regin.[31]

A la fin de 2014, plusieurs journaux ont signalé la découverte du maliciel Regin sur un ordinateur de la Chancellerie fédérale allemande. Il semblerait que l'infection résulte de l'utilisation d'une clé USB. Cette clé aurait servi auparavant sur le système privé d'un collaborateur de la Chancellerie. Une porte-parole du gouvernement a souligné que le réseau n'avait pas été contaminé.[32]

«Red October reloaded»

L'entreprise de sécurité Bluecoat a découvert en décembre 2014 une attaque d'espionnage ciblé, qui avait pour particularité de se propager aussi aux appareils mobiles fonctionnant sous Android ou iOS, ainsi qu'aux Blackberry. Or pour qu'un iPhone ou un iPad puisse être infecté, il faut d'abord que ses restrictions à l'utilisation aient été désactivées (*jailbr*eak, ou débridage). Le maliciel utilisait en outre un mécanisme de commande et contrôle peu répandu. Toutes les machines infectées communiquaient via https et WebDav avec le même serveur de CloudMe, service suédois de stockage dans le nuage (*cloud*). Le maliciel, baptisé Inception, a surtout servi à espionner des cadres dirigeants dans les secteurs du pétrole et du gaz, dans les milieux financiers et la défense militaire, au niveau étatique ainsi que dans les ambassades. Il était diffusé par des courriels de *spear phishing*, dans des documents contenant un cheval de Troie. Kaspersky, qui a également publié des informations sur cette campagne d'espionnage intitulée Cloud Atlas[33], considère qu'il pourrait s'agir d'une nouvelle version du maliciel Red October – réseau d'espionnage ayant cessé toute activité aussitôt après la publication, en janvier 2013, d'un rapport de Kaspersky à son sujet. En effet, les traces laissées par Cloud Atlas font penser à la campagne Red October. Non seulement le cercle de victimes est identique, mais le document utilisé pour une des attaques de *spear phishing* était quasiment le même.

Cloud Atlas est un bon exemple d'attaque de type APT (*advanced persistent threat).* Outre son grand professionnalisme (*advanced*), elle fait surtout preuve de durabilité (*persistent*). Lorsqu'un acte d'espionnage ciblé est découvert et donc neutralisé, il faut s'attendre à ce que les agresseurs soient déjà présents ailleurs dans le système, ou sinon à ce qu'ils récidivent plus tard.

---

31 http://www.spiegel.de/netzwelt/netzpolitik/nsa-trojaner-kaspersky-enttarnt-regin-a-1015222.html (état: le 28 février 2015).
http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html (état: le 28 février 2015).

32 http://www.heise.de/newsticker/meldung/Offenbar-Spionagesoftware-Regin-auf-Rechner-im-Kanzleramt-entdeckt-2507042.html (état: le 28 février 2015).

33 https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (Stand: 28. Februar 2015)

Sandworm – attaques visant l'OTAN et des membres du gouvernement ukrainien

L'entreprise de sécurité iSight a rendu publique à la fin d'octobre 2014 une campagne d'espionnage ciblé menée contre des membres du gouvernement ukrainien, de l'Union européenne ainsi que de l'OTAN, en tirant notamment parti d'une faille de Windows.[34] Les autres cibles étaient une société de télécommunications française et une compagnie énergétique polonaise. L'utilisation d'une vulnérabilité jour zéro de Microsoft Windows et de Windows Server (CVE-2014-4114) atteste du très grand professionnalisme de son auteur.[35]

Les attaques contre des fonctionnaires du gouvernement ukrainien, incessantes depuis l'été 2014, auraient été commises grâce à l'envoi ciblé aux victimes de documents PowerPoint utilisant la faille de sécurité susmentionnée. Les premières activités du groupe d'espions identifiées par iSight remontent toutefois à 2009. Même si les centres d'intérêt et certains éléments textuels indiquent une origine russe, il n'a pas été possible dans ce cas de déterminer sans ambiguïté l'agresseur.

Attaques présumées contre des sociétés israéliennes

A fin juillet 2014, le journaliste indépendant Brian Krebs a publié qu'en 2011 et en 2012, des documents ayant trait au Dôme de fer, le système de protection anti-missile israélien, avaient été dérobés à plusieurs reprises.[36] Krebs se référait à l'agence de sécurité américaine CyberESI, qui a examiné la campagne. Trois fabricants d'armes israéliens seraient concernés – Rafael Advanced Defense Systems, Israel Aerospace Industries et le groupe Elisra. Les soupçons se sont portés sur le groupe de cyberespions APT1, aussi connu sous le nom d'Unité 61398 de l'armée populaire de Chine. Les entreprises touchées n'ont pas confirmé les attaques.

Autorité de sûreté nucléaire américaine

La Commission de réglementation nucléaire des Etats-Unis aurait subi, ces trois dernières années, au moins trois cyberattaques réussies. Une implication étatique est soupçonnée. Dans deux cas, les traces remonteraient à un pays précis, dont le nom n'a toutefois pas été dévoilé. Selon Nextgov[37], des méthodes usuelles comme le *phishing* et le *spear-phishing* ont été employées. Il est intéressant de noter que pour la troisième agression, le compte de messagerie d'un collaborateur avait servi à transmettre un fichier PDF compromis à seize autres collaborateurs. Il est d'autant plus difficile au destinataire de reconnaître un courriel malveillant. Il s'agit d'une astuce fréquente pour accéder à des ordinateurs «intéressants» d'une entreprise, à partir de postes de travail plus faciles à infiltrer.

Les actes d'espionnage ciblés ne sont pas des événements isolés. Les données sensibles suscitent un intérêt qui ne se relâche pas et sont soumises à des pressions permanentes. Or il est toujours difficile d'en déterminer l'auteur. Même si pour la plupart des attaques de type APT (*advanced persistent threat)*, le choix des victimes alimente l'hypothèse d'un acteur étatique, la ligne de démarcation entre les pirates employés par l'Etat et les criminels agissant pour leur propre compte est souvent floue.

---

34 http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/ (état: le 28 février 2015)

35 http://www.isightpartners.com/2014/10/cve-2014-4114/ (état: le 28 février 2015).

36 http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ (état: le 28 février 2015).

37 http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/ (état: le 28 février 2015).

Amnesty International propose un outil de détection des logiciels d'espionnage

En novembre 2014, Amnesty International a mis à disposition un programme censé reconnaître les logiciels espions. Tel FinFisher, qui permet notamment d'effectuer un suivi des conversations sur Skype, d'enregistrer les courriels et même de prendre des photos en utilisant la caméra de l'appareil. Ce logiciel est notamment utilisé contre les militants des droits de l'homme et les dissidents, dans les pays soumis à des régimes autoritaires et où la liberté d'expression est muselée. On ignore toutefois jusqu'à quel point le nouvel outil permet de détecter les divers types de logiciels de surveillance.[38]

4.6 Espionnage lors de voyages d'affaires

Depuis longtemps déjà, la prudence s'impose en cas d'utilisation de réseaux sans fil publics (*WLAN*). L'exemple le plus connu d'attaque contre un tel réseau porte le nom de Firesheep: il permettait de détourner aisément les sessions de navigation (*session hijacking*) dans un réseau non sécurisé, et donc ouvert (p. ex. cybercafé), pour dérober les données d'utilisateur comme les mots de passe. Une telle attaque ne fonctionne qu'en cas de transmission non cryptée des données, sans protocole de transfert sécurisé https. La société Kaspersky a publié en novembre 2014 un rapport sur la campagne baptisée Darkhotel: un groupe de pirates s'en serait pris aux réseaux sans fil de grands hôtels, bien au-delà des attaques connues jusque-là.[39] Depuis quatre ans, des top managers auraient fait l'objet d'attaques systématiques lors de voyages d'affaires en Asie. Ce qui suggère une affaire d'espionnage économique. Il est vrai que d'autres personnes ont aussi été attaquées de manière aléatoire. L'agression intervient dès que la victime, après s'être enregistrée, utilise son ordinateur et veut se connecter au WLAN de l'hôtel. Elle est informée qu'un programme spécifique a besoin d'une mise à jour (p. ex. la barre d'outils Google, Adobe Flash ou Windows Messenger). Il s'agit bien entendu d'un virus capable de dérober ses données.

Par ailleurs, les Services secrets américains ont signalé au semestre dernier la présence d'enregistreurs de frappes (*keylogger*) sur les ordinateurs proposés au public dans les hôtels ou les aéroports. Ils invitaient la branche de l'hôtellerie à contrôler leurs ordinateurs en libre accès. Ce communiqué faisait suite à l'arrestation de personnes soupçonnées d'avoir installé des enregistreurs de frappes (*keylogger*) sur les ordinateurs de plusieurs hôtels de congrès de Dallas/Fort Worth.[40]

Une saine prudence s'impose en cas de navigation sur des réseaux locaux sans fil (WLAN) publics. Il faut se garder d'accepter les programmes cherchant à s'installer lors d'une demande d'accès au réseau mobile. En outre, une extrême vigilance doit être apportée à l'actualisation régulière de son ordinateur. Il risque sinon d'être vulnérable aux simples *infections de sites Web*. Les personnes obligées de traiter en déplacement des données critiques feraient bien de se demander s'il ne vaudrait pas mieux partager la connexion de leur téléphone mobile et utiliser sa fonction d'itinérance (*roaming*). Même si cette solution génère d'importants coûts.

Il faudrait s'abstenir d'utiliser sur des ordinateurs publics des services nécessitant un nom d'utilisateur ou un mot de passe. Il est conseillé de n'utiliser cette prestation fournie par les hôtels que pour s'informer p. ex. des curiosités d'une ville.

---

38 http://www.amnesty.ch/fr/themes/autres/liberte-dexpression/docs/2014/amnesty-lance-detekt-un-outil-de-detection-des-logiciels-despionnage (état: le 28 février 2015).

39 http://blog.kaspersky.com/darkhotel-apt/ (état: le 28 février 2015).

40 http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/ (état: le 28 février 2015).

4.7 Vol de données à grande échelle

Cette année aussi, plusieurs cas de vol de données ont fait les gros titres. L'un d'eux surtout a été très remarqué – en raison moins de la quantité de données subtilisées que de son contexte. En août, un des principaux exploitants d'hôpitaux américains a signalé que les données de 4,5 millions de patients lui avaient été dérobées. Les patients s'attendent à ce qu'une grande attention soit accordée à la protection de leurs données médicales. Or la numérisation avance à grands pas dans le secteur de la santé. Cette situation offre certes des avantages et contribue à réduire les erreurs, mais n'est pas sans risques.

Dans le cas d'espèce, le système de santé communautaire d'une des principales chaînes d'hôpitaux américains avait annoncé en août 2014 une intrusion dans son système informatique. L'opération aurait permis de faire main basse sur les données de 4,5 millions de patients traités au cours des cinq années précédentes dans un établissement du groupe. La société Mandiant a attribué ce forfait à des pirates chinois. De l'aveu même de la victime, qui gère 206 hôpitaux dans 29 Etats fédéraux, les pirates auraient volé le nom et l'adresse, le numéro de téléphone, la date de naissance et le numéro de sécurité sociale des patients. L'enquête n'a hélas permis de déterminer ni le but précis des pirates, ni si des acteurs étatiques étaient mêlés à l'opération.

Le secteur financier n'a pas été ménagé au semestre dernier. Les médias ont surtout parlé d'une vaste opération lancée contre la grande banque américaine J.P. Morgan. Les données de 76 millions de ménages et de sept millions d'entreprises auraient été copiées lors de l'attaque découverte à la mi-août 2014. Les escrocs ont obtenu des données de clients (nom, adresse, n° de téléphone, adresse électronique) sur les serveurs de cet établissement financier. Rien n'indique toutefois qu'ils aient subtilisé des données sensibles (n° de compte, date de naissance, mot de passe ou n° de sécurité sociale). Le vecteur d'attaque a été identifié, aux dires de la banque J.P. Morgan: une faille de sécurité connue depuis juin 2014 aurait été utilisée. Rien n'a toutefois filtré sur la nature de cette vulnérabilité. Les comptes menacés ont été désactivés et les mots de passe de tous les techniciens informatiques modifiés. Sur la base des indices collectés, les autorités penchent pour des professionnels de haut vol, peut-être basés en Russie. L'hypothèse d'une réaction aux sanctions américaines a certes été avancée, mais il n'a pas été possible d'en apporter la preuve.

Au début d'août 2014, la société Hold Security a annoncé un incident d'une ampleur sans précédent: des cyberpirates russes auraient dérobé 1,2 milliard d'identifiants – nom et mot de passe. Les données d'accès proviendraient de plus de 420 000 sites Web, appartenant parfois à des entreprises connues. Autre particularité de ce cas, la société Hold Security signalait dans la foulée qu'elle allait fournir un nouveau service, permettant de savoir si l'on avait soi-même été victime de cet incident ou d'autres vols de données.[41]

Souvent, les entreprises de sécurité informatique s'adressent aux services étatiques compétents ou aux fournisseurs d'accès impliqués, pour qu'ils puissent informer les victimes. La question de l'usage responsable de telles informations se posera toujours plus à l'avenir, et le chapitre 5.5 l'aborde en détail.

[41] http://www.forbes.com/sites/kashmirhill/2014/08/05/huge-password-breach-shady-antics/ (état: le 28 février 2015).

4.8 iCloud piraté – photos de célébrités dans Internet

A la fin du mois d'août 2014, des photos volées de célébrités dénudées ont été rendues publiques, d'abord sur le site 4chan, puis sur plusieurs autres plateformes. Il s'est vite avéré que ces photos étaient issues de différents comptes iCloud, le service de stockage dans le nuage (cloud) d'Apple. Plusieurs pistes ont été avancées quant à la méthode utilisée pour accéder aux photos. Puis très vite le logiciel Find My iPhone, servant à localiser les appareils égarés ou volés, a été pointé du doigt. Selon de nombreux comptes rendus d'experts, ce programme aurait été vulnérable à une attaque par force brute (*brute-force attack*), qui consiste à essayer, de manière automatisée, un grand nombre de mots de passe pour accéder à un service. Ce soupçon a été nourri par le fait qu'une démonstration de faisabilité (*proof of concept*, *POC*) consacrée à cette méthode avait paru peu avant le scandale sur le site GitHub. Une mesure de sécurité classique pour se prémunir des attaques par force brute consiste à bloquer le service après un certain nombre de tentatives d'accès infructueuses. Ce dispositif n'était pas prévu à l'époque pour Find My iPhone, mais a été implémenté peu après le scandale des photos volées. Il faut encore préciser qu'Apple a réfuté l'hypothèse d'une vulnérabilité de Find My iPhone ou d'un autre de ses services. Dans une déclaration officielle, l'entreprise attribue la fuite à une attaque très ciblée visant les noms d'utilisateurs, mots de passe et questions de sécurité de certains comptes[42].

L'affaire n'est pas la seule à avoir suscité des doutes quant à la sécurité des services de stockage dans le nuage. Dropbox a par exemple aussi été visé: des données d'accès à ce service ont été postées sur le site Pastebin, une application web qui permet aux utilisateurs de publier des morceaux de textes, en octobre 2014. Ces différents cas relancent le débat sur la sécurité des données enregistrées dans le nuage. Ce mode de stockage offre en effet à un pirate la possibilité de s'emparer de nombreuses données personnelles, à travers la compromission d'un système ou compte vulnérable. Dans le cas d'iCloud ou de services similaires, il convient de préciser que de nombreux utilisateurs n'ont pas réalisé que les photos qu'ils prennent sont automatiquement synchronisées avec un compte dans le nuage. Ce paramètre peut en effet être activé par défaut. Il est donc primordial de vérifier si tel est le cas pour chaque «app», et de désactiver la synchronisation automatique si l'on n'en veut pas.

Il est par ailleurs recommandé aux utilisateurs du stockage en nuage de respecter les règles de sécurité s'appliquant aux autres comptes en ligne, tels les comptes de messagerie. Il convient de choisir, pour chaque service, un mot de passe complexe et comportant différents types de caractère. MELANI recommande encore, lorsque c'est possible, de recourir à l'*authentification à deux facteurs*[43]. Enfin, comme le rappelle l'incident des photos de célébrités dénudées mises en circulation, le meilleur moyen d'éviter toute fuite reste de ne pas produire de matériel compromettant, ou du moins de ne pas le stocker sur un support numérique connecté.

[42] http://www.bbc.com/news/technology-29039294 (état: le 28 février 2015).

[43] Une liste des sites permettant une authentification à deux facteurs est disponible sous: https://twofactorauth.org (état: le 28 février 2015).

4.9 Graves failles de sécurité dans des composants logiciels importants

Outre les nombreuses lacunes d'applications comme Flash, Acrobat, Java et Office, de graves vulnérabilités ont été découvertes au semestre dernier dans les systèmes d'exploitation et les bibliothèques logicielles.

Poodle

Déjà victime dans le passé de Heartbleed, le protocole *SSL*, qui a pour objectif d'assurer la protection du caractère confidentiel des données échangées, a connu un nouveau problème technique. Or à la différence de Heartbleed, la faille baptisée Poodle[44] n'était pas une erreur de programmation, mais une erreur du protocole lui-même, plus précisément de la version 3 de *SSL*. La faille tient au fait que *SSL/TLS* s'assure de l'intégrité des données avant de les crypter. Comme le cryptage consiste généralement en blocs de longueur fixe, chaque ligne comporte à la fin le nombre de caractères nécessaires pour que le bloc ait la longueur voulue. Le dernier *byte* indique la taille du bloc. C'est là que réside le problème. Les données aléatoires complétant le bloc et le dernier *byte* ont beau être aussi cryptés, leur intégrité n'est pas vérifiée. Un pirate peut donc y insérer discrètement toutes sortes de caractères, dont des éléments de la ligne qu'il souhaite décrypter. L'auteur d'une attaque de l'intermédiaire (*man-in-the-middle attack*, MIDM) s'immisce à cet effet dans le canal de communication des partenaires. Ce qui est par exemple possible dans un réseau mobile ouvert.[45]

MELANI recommande aux exploitants de sites Web de désactiver complètement SSLv3 et de n'utiliser autant que possible que les protocoles de cryptage TLS 1.1 ou TLS 1.2. La plupart des navigateurs actuels ne supportent plus entre-temps SSLv3.

Shellshock

La vulnérabilité Shellshock[46] concernait notamment la quasi-totalité des systèmes d'exploitation Unix. Cette faille critique permet d'exécuter sans contrôle du code de programme. Elle a été découverte dans un logiciel fréquemment utilisé, nommé «Bash Shell». Outre les serveurs et les clients, des appareils comme les *routeurs* ou les *passerelles de sécurité* sont vulnérables. Les lacunes découvertes ont été corrigées au fur et à mesure. La défaillance tient à ce que les variables d'environnement soumises ne font pas l'objet de vérifications adéquates. D'où la possibilité d'ajouter à une variable du code malveillant.

```
$ env x='() { :;}; echo VULNERABLE' bash -c ""
```

[44] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 (état: le 28 février 2015).

[45] Une description détaillée du mode opératoire de la faille de sécurité de Poodle figure ci-après: https://nakedsecurity.sophos.com/2014/10/16/poodle-attack-takes-bytes-out-of-your-data-heres-what-to-do/ (état: le 28 février 2015).

[46] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271, ainsi que les numéros CVE 2014-7169, 2014-7186, 2014-7187, 2014-6277 et 2014-6278 (état: le 28 février 2015).

Différents scénarios d'attaque sont envisageables:

- serveur HTTP / Web, via l'interface CGI
- SSH
- DHCP
- SIP
- et bien d'autres encore.

Après la révélation de cette lacune, MELANI a constaté une hausse spectaculaire des opérations de scan et d'exploit, qui entre-temps se poursuivent avec une moindre intensité.

Kerberos

Une autre lacune (MS14-068[47]) susceptible d'avoir de graves conséquences pour les entreprises réside dans la configuration de Kerberos dans le service d'annuaire (*active directory*) de Microsoft. Un simple utilisateur de compte peut exploiter cette faille pour obtenir des privilèges supérieurs (droits d'administrateur) et s'approprier tout un service d'annuaire. Autrement dit, il suffit en principe à un agresseur de lancer une attaque fructueuse (basée p. ex. sur un maliciel) contre un utilisateur interne pour prendre le contrôle de la totalité des ressources Windows de l'entreprise. MELANI recommande non seulement de combler la lacune, mais aussi de prévoir des plans d'urgence en vue de la restauration des *active directories*, et d'en tester régulièrement le fonctionnement. En outre, il importe de veiller spécialement à la sécurisation des comptes à privilèges.

SChannel

Une autre faille de sécurité de Windows (MS14-066)[48] concernait Secure Channel. SChannel est la librairie SSL/TLS de Microsoft, permettant d'échanger de manière cryptée des informations sensibles sur un réseau public. Selon Microsoft, un agresseur peut exécuter à distance, grâce à cette vulnérabilité, n'importe quel code malveillant sur le système pris pour cible, en envoyant des paquets spécialement conçus à un serveur Windows. Cisco a encore mentionné, dans un article de son blog, plusieurs débordements de tampon (*buffer overflow*).[49] Ce patch a donné du fil à retordre à Microsoft, qui a dû l'améliorer à plusieurs reprises pour en éliminer les effets secondaires, comme les problèmes de performance.

De façon générale, MELANI observe que les pirates s'intéressent de près aux logiciels couramment utilisés dans Internet, comme Flash, Acrobat et Java. Dès qu'un programme correctif (patch) paraît, ils analysent la vulnérabilité éliminée et complètent leurs *kits d'exploits* afin de pouvoir attaquer les appareils n'ayant pas encore été protégés. L'opération s'effectue généralement en quelques jours. Certains *kits d'exploits* exploitent même des lacunes inédites (*0-day-exploit*). Par conséquent, MELANI recommande aux utilisateurs à domicile et aux PME d'automatiser les mises à jour, et aux grandes entreprises de mettre en place une gestion très rapide des patchs, avec des processus clairement définis et un degré de priorité élevé.

47 https://technet.microsoft.com/fr-FR/library/security/ms14-068.aspx (état: le 28 février 2015).

48 https://technet.microsoft.com/fr-fr/library/security/ms14-066.aspx (état: le 28 février 2015).

49 http://blogs.cisco.com/security/talos/ms-tuesday-nov-2014 (état: le 28 février 2015).

4.10 Faille de la norme de télécommunication mobile

Les experts réunis autour de Karsten Nohl, spécialiste berlinois de la sécurité informatique, ont révélé en décembre 2014 une faille du réseau de téléphonie mobile permettant de déjouer le cryptage réputé sûr du réseau *UMTS*, afin d'intercepter des *SMS* notamment. Le protocole de signalisation SS7 (signalling system 7), où cette lacune de sécurité a été découverte, sert aux opérateurs téléphoniques à échanger des informations entre eux, p. ex. pour acheminer les SMS ou les appels sur différents réseaux. Le protocole lui-même remonte aux années 1980, et donc s'avère relativement âgé. Même s'il a été modernisé à deux reprises et doté à cette occasion de nouvelles fonctions, le grave problème de l'absence d'authentification entre les partenaires n'a jamais été résolu. Du temps où il n'y avait qu'un petit nombre de grands opérateurs, qui en outre se connaissaient et se faisaient mutuellement confiance, cela ne posait guère problème. Entre-temps, de multiples opérateurs plus ou moins fiables se partagent le marché mondial de la téléphonie mobile, et certains d'entre eux revendent encore à d'autres entreprises l'accès au protocole SS7.

Concrètement, cette faille de sécurité comporte les vecteurs d'attaques suivants pour un agresseur potentiel:

- géolocalisation d'un appareil:
  Chaque appareil est annoncé auprès de la plus proche cellule radio. Il suffit à l'agresseur d'indiquer le numéro de téléphone de la personne à surveiller, pour connaître la cellule radio qu'elle utilise à ce moment. Un coup d'œil à une banque de données donnera ensuite l'emplacement de cette cellule radio. Dans les régions densément peuplées et possédant de nombreuses cellules radio, un individu peut être localisé avec une assez grande précision. En outre, la connaissance de l'identité internationale de l'abonné mobile (*international mobile subscriber identity, IMSI)* et de son adresse unique utilisée pour le routage des appels (global title, GT) livre des vecteurs d'attaque supplémentaires, exploitables même si l'opérateur verrouille certaines fonctions de journalisation.

- interception et écoute des conversations:
  Lorsqu'un appareil se trouve dans un autre réseau, des événements spécifiques aboutissent à une demande auprès de l'opérateur d'origine. Si un pirate remplace les coordonnées d'envoi par sa propre adresse, l'appareil s'annoncera le cas échéant à ce réseau malveillant. D'où la possibilité de détourner et d'épier les conversations. L'attaque de l'intermédiaire (*man-in-the-middle attack*) a lieu à l'insu de la victime.

- interception de numéros mTAN:
  D'autres opportunités d'attaque s'offrent lors de la mise à jour des informations sur l'atteignabilité d'un appareil, qui ne sont pas non plus authentifiées. Un pirate peut ainsi prétendre que sa victime se trouve dans son réseau, et le signaler à l'opérateur d'origine. Celui-ci lui acheminera alors par son réseau les appels ou les SMS. Un agresseur peut ainsi intercepter un numéro mTAN, lors des séances d'e-banking où l'authentification repose sur l'envoi d'un code par SMS.

- interception du numéro IMSI:
  Pour signaler à un appareil qu'un appel lui est destiné, une identité lui est temporairement attribuée (TIMSI) et circule sur le réseau sans cryptage. Une fois interceptée, il suffit de s'adresser au centre de commutation pour connaître le véritable numéro d'identification (IMSI). Et dès lors qu'un agresseur connaît l'IMSI, il peut p. ex. apprendre le numéro de téléphone effectif ou obtenir la clé de cryptage de la conversation en cours.

Ces scénarios sont relativement simples à mettre en œuvre, et il est très probable que des acteurs étatiques ou assimilables à l'Etat y recourent. D'où l'importance de ne pas échanger par téléphone mobile des informations hautement confidentielles, comme p. ex. des secrets commerciaux, a fortiori si l'un des interlocuteurs se trouve à l'étranger et qu'il s'agit donc d'un appel en itinérance. MELANI a pris contact avec les opérateurs de téléphonie mobile suisses, afin de corriger autant que possible ces vulnérabilités.[50]

4.11 Failles – également dans MacOSX

MELANI constate que les failles du système d'exploitation MacOSX sont toujours plus souvent utilisées pour lancer des attaques ciblées, et plus généralement pour diffuser des maliciels. Par analogie à Windows, les pirates tirent parti des vulnérabilités de Java ou des plugiciels pour navigateurs, comme Acrobat Reader ou Flash.

Deux familles de maliciels ont suscité une vive attention au cours des derniers mois:

- iWorm[51] est une porte dérobée (*backdoor*) pouvant être utilisée dans divers buts. Il est intéressant de noter la manière dont ce maliciel se procure des informations sur les serveurs C&C avec lesquels il doit communiquer. Il utilise des indications publiées par les agresseurs sur le forum communautaire Reddit, afin de générer les adresses URL correspondantes. La diffusion d'iWorm se fait principalement par des copies pirates compromises qui sont proposées via le logiciel BitTorrent.[52]

- Wirelurker[53] est un maliciel qui renferme à la fois une composante MacOSX et une composante iOS. S'il est en activité sur une machine OSX, il attend qu'un appareil iOS (iPhone, iPad) se connecte par liaison *USB*. Le maliciel copie alors différentes informations (numéro de téléphone, données de l'iTunesStore, etc.), qu'il envoie à un serveur C&C. Comme la liaison USB est jugée fiable, il peut se faire passer pour une app normale. Il lui faut un certificat d'entreprise et un profil d'approvisionnement, afin que sa signature soit reconnue valable. La procédure comporte une requête auprès de l'utilisateur. Avec son feu vert, le maliciel s'installe. Cette étape s'avère même superflue en cas de désactivation des restrictions à l'utilisation (*jailbr*eak, débridage). De tels certificats d'entreprise permettent à une compagnie d'installer ses propres applications sur ses appareils iOS. Comme iWorm, le maliciel destiné à OSX est diffusé par des copies pirates de logiciels commerciaux.

A côté d'attaques basées sur des maliciels, MELANI constate que les comptes iTunes et iCloud sont toujours plus souvent la cible d'attaques de *phishing*. Les internautes sont invités – de façon tout à fait classique – par des courriels en apparence authentiques à saisir leurs données d'ouverture de session sur un serveur des agresseurs. Ceux-ci obtiennent ainsi l'accès convoité aux comptes de leurs victimes.

En outre, l'interface Thunderbolt présente une lacune à prendre au sérieux dans le contexte des attaques ciblées[54]. Cette lacune permet à un agresseur ayant physiquement accès à un

[50] Source: Tobias Engel, http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf (état: le 28 février 2015).

[51] http://news.drweb.com/show/?i=5977&lng=en (état: le 28 février 2015).

[52] http://www.thesafemac.com/iworm-method-of-infection-found/ (état: le 28 février 2015).

[53] https://www.paloaltonetworks.com/resources/research/unit42-wirelurker-a-new-era-in-ios-and-os-x-malware.html (état: le 28 février 2015).

[54] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4498 (état: le 28 février 2015).

appareil de modifier directement le programme interne (*firmware)* EFI des machines Mac, en y connectant un appareil Thunderbolt modifié – p. ex. un adaptateur Gigabit. Un maliciel répandu par ce biais sera d'autant plus difficile à découvrir qu'il s'installe en amont du système d'exploitation, et peut ainsi se dissimuler tant du système que des antivirus. Apple a publié un patch qui comblera la lacune au moins pour OSX Yosemite (10.10.2).

5 Tendances / Perspectives

5.1 Collecte et échange d'informations à l'ère du Big Data

A la fin du 20e siècle déjà, on assimilait les données et l'information à un nouvel eldorado. D'innombrables start-up d'Internet ont vu le jour, avec des plans d'affaires se contentant d'indiquer comme source de revenus la collecte de données et d'informations. Elles éludaient soigneusement la question de savoir comment les données seraient transformées en argent. D'où un brutal rappel à la réalité quand il a fallu présenter, à côté de toutes les informations et données collectées, des chiffres bien souvent rouges. A l'esprit pionnier a succédé la gueule de bois, et la bulle Internet a éclaté en mars 2000, presque aussi vite qu'elle était apparue. Quinze ans plus tard, les sociétés Internet ont visiblement fait leurs devoirs. Soit elles se font payer les prestations fournies en ligne, soit il faut leur fournir des données personnelles pour accéder à leurs offres gratuites. Tel est notamment le cas de Facebook, Google ou Twitter – qui tirent entre-temps de juteux profits de la collecte et de l'exploitation des données et informations à leur disposition.

La collecte de données et d'informations a ceci de bon qu'elle permet d'analyser les profils, d'afficher une publicité individualisée et d'offrir aux clients des services toujours mieux adaptés. Dans leur propre interprétation des faits et leur souci de fournir de la façon la plus rationnelle possible le produit sécurité, certains services de renseignement soulignent volontiers qu'«on a besoin de toute la botte de foin pour trouver l'aiguille» (en pensant généralement au terrorisme). Au niveau international et interétatique également, la collecte de données et d'informations et les échanges correspondants sont toujours plus considérés comme une solution miracle, p. ex. dans la lutte contre les excès en matière de soustraction fiscale ou en vue d'une harmonisation des listes de personnes recherchées. On peut toutefois supposer, du moins dans le cas de la collecte et de l'analyse des données personnelles par l'Etat, ainsi que de leur échange au niveau international, que le cadre juridique est très strict, ce qui est loin d'être le cas avec les initiatives du secteur privé.

Dans tous les cas, cette évolution s'avère problématique à double titre. Premièrement, la collecte centralisée de données et d'informations débouche sur des vols spectaculaires. Ce n'est pas un hasard si lors des cyberattaques lancées contre des entreprises, la quantité de données dérobées ne cesse d'augmenter. Alors qu'il y a dix ans, les médias signalaient encore le vol de quelques milliers d'adresses électroniques, un incident doit entre-temps porter sur des millions de données, mot de passe compris, pour attirer leur attention. Il n'est guère étonnant que les pertes surviennent régulièrement dans des entreprises auxquelles la victime n'avait pas directement fourni de données. En effet, les données et les informations font l'objet d'échanges intenses. Généralement avec l'autorisation implicite du propriétaire qui, un jour ou l'autre, avait accepté des conditions générales ou une disposition relative à la protection des données, afin de pouvoir commander un livre convoité ou se créer un compte sur un réseau social. Le principe du maillon le plus faible s'applique tout particulièrement à la sécurité informatique. Un accord ou un traité sur les modalités de la collecte et des échanges techniques de données ont beau être très précis et stricts, il n'est jamais exclu qu'au bout du compte, des données ne tombent entre les mauvaises mains. Cette règle ne vaut d'ailleurs

pas que pour le secteur privé, mais concerne aussi les institutions étatiques, comme le rappelle la mésaventure du Système d'information Schengen (SIS) au Danemark.[55]

Deuxièmement, la question de la finalité de cette masse de données se pose. Dans le secteur privé, on peut considérer que leur usage répond en premier lieu à des considérations commerciales. En transmettant des données, leur propriétaire espère en tirer un avantage. Il peut être utile de fournir des données à un tiers, pour obtenir en retour l'offre la mieux adaptée. Il en va différemment si elles sont transmises aux autorités chargées de la sécurité dans un autre pays. D'où la nécessité de dûment préciser la destination des données dans les relations interétatiques. Il peut être judicieux de simplifier la lutte contre l'évasion fiscale en instaurant l'échange automatique de renseignements (EAR). Mais il est également urgent de fixer la manière exacte dont ces informations seront exploitées par l'Etat qui les reçoit. La Suisse s'est notamment battue au sein de l'OCDE pour que la réglementation sur l'EAR ne porte pas seulement sur la nature des données à collecter, mais qu'elle précise encore l'usage pouvant en être fait. Or il n'est visiblement pas garanti que l'Etat partenaire se conforme à ses engagements, comme le montre une décision rendue en 2014 par le Tribunal administratif fédéral.[56]

Dans le cas d'espèce, où un citoyen suisse était soupçonné de délit d'initié, les autorités pakistanaises avaient sollicité en été 2012 l'assistance administrative de l'Autorité fédérale de surveillance des marchés financiers (FINMA). Cette dernière y ayant consenti, l'accusé suisse avait déposé auprès du Tribunal administratif fédéral un recours, où il expliquait en substance que l'autorité pakistanaise compétente n'était pas en mesure de garantir le respect du principe de la spécialité et de la confidentialité. En effet, des courriels internes de l'autorité pakistanaise, de même que la communication interne entre la FINMA et elle avaient été envoyés à la presse pakistanaise. La violation du secret de fonction était donc avérée. La FINMA a aussitôt suspendu la procédure d'assistance administrative.

L'apparition de mégadonnées (big data), avec leurs avantages et inconvénients, ne soulève pas seulement des questions relevant de la sécurité technique et de la responsabilité des exploitants d'une telle masse d'informations. Des questions se posent également quant à la «due diligence» requise en amont de l'exploitation et de l'utilisation de ces données. Les premiers concernés sont ici les propriétaires de données, qui mettent volontairement à disposition leurs données et qui doivent être au clair sur ce qui en sera fait. Or les autorités étatiques ont également un rôle à jouer: il leur incombe de veiller à ce que les données perçues et transmises légalement ne soient réellement utilisées que dans le but prévu au départ. La mise au point de processus efficaces d'audit et de contrôle pour s'en assurer constitue sans doute un des principaux défis à relever dans un proche avenir.

5.2 Mise en réseau totale. Une solution intelligente et sûre?

Internet – le réseau des réseaux – relie entre eux les systèmes basés sur les TIC et permet le transfert d'informations et de données. Il ne se limite toutefois pas au World Wide Web et aux sites Web que les internautes consultent. En tant qu'infrastructure de télécommunication implantée au niveau mondial, Internet permet également aux gens de communiquer avec des machines et de leur donner des instructions ayant un impact sur le monde physique.

[55] Voir MELANI, rapport semestriel 2013/2, chapitre 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 28 février 2015).

[56] http://www.bvger.ch/publiws/download;jsessionid=F01EA73D27D15FF364A9203975D0B648?decisionId=f736b6ed-38ba-4d10-bf8f-c0312d05030f (état: le 28 février 2015).

Entre-temps, les machines sont également en mesure d'interagir – à condition bien entendu d'avoir été dûment programmées. Des micro-ordinateurs aptes à communiquer jouent un rôle croissant dans divers domaines. L'enregistrement de la situation par des capteurs et l'exécution, par des actionneurs, de commandes produisant un effet spécifique permettent une automatisation poussée des processus de soutien, dont tout un chacun bénéficie non plus seulement dans le monde virtuel, mais dans le monde physique également.

De nombreux néologismes reflètent cette évolution, comme l'Internet des objets (internet of things), l'informatique omniprésente (pervasive computing, ubiquitous computing) ou les ordinateurs vestimentaires (wearable computing), conçus pour être intégrés à un vêtement ou à un accessoire qu'on peut porter. Entre-temps, les téléphones ne sont plus seuls à être qualifiés d'intelligents. Les véhicules (smart car / smart drive), les logements (smart home), voire des bâtiments entiers (smart building) et des sites industriels (smart factory / smart manufacturing)[57] sont en mesure de collecter et de recevoir des données, de les traiter, de les envoyer, de les traduire en commandes et d'exécuter des actions spécifiques.

Le succès rencontré par la technologie sous-jacente à Internet et le besoin d'interopérabilité font que toujours plus d'applications ayant besoin d'échanger des données recourent au protocole Internet. C'est ainsi que dans les maisons dites intelligentes, les capteurs et les actionneurs de la domotique sont intégrés au réseau local sans fil (WLAN). En effet, cette infrastructure est déjà en place et les habitants souhaitent pouvoir contrôler leur domicile avec leur smartphone déjà relié au réseau domestique. D'où inévitablement des interfaces entre Internet, conçu pour les échanges de données et d'informations au niveau mondial, et les appareils locaux comme le capteur de température du chauffage ou l'ampoule du salon reliée au réseau. Or s'il peut être utile d'enclencher par smartphone le chauffage et le chauffe-eau de l'appartement de vacances avant son arrivée, il paraît moins indispensable de pouvoir allumer ou éteindre l'éclairage en son absence, et à fortiori d'actionner l'écran de projection d'un home-cinéma. Bien que les fabricants de tels systèmes ne proposent que très rarement des fonctions de domotique basées sur Internet (préconisant plutôt l'usage du réseau interne), de telles possibilités existent du moins en théorie.[58] Le cas échéant, il faut protéger tous ces systèmes non seulement contre les attaques lancées à partir d'Internet, mais aussi contre les menaces locales. Outre le WLAN, d'autres interfaces sans fil (p. ex. *Bluetooth*, *NFC*) peuvent servir de porte d'entrée si elles sont mal configurées ou sécurisées.

Les utilisateurs assimilent toujours plus leur smartphone à un dispositif d'identification et de commande, ainsi qu'à un outil de collecte et d'analyse des données. On le voit p. ex. aux apps en plein essor dans le secteur de la santé. D'où la nécessité de prendre dûment en compte la sécurité de son smartphone, pour des raisons de sûreté de l'information et de protection des données. Par ailleurs, il importe de réfléchir à la meilleure façon d'agir en cas de compromission ou de perte de son smartphone, pour prévenir tout abus par des tiers non autorisés et pour pouvoir transférer sans perte les fonctions et données habituelles sur un appareil de remplacement.

En dépit de tous les avantages qu'offre un environnement «intelligent», il ne faut jamais oublier de s'interroger sur la collecte, le traitement et le stockage des données, et de se demander si et comment on parviendrait à se débrouiller sans accessoires connectés – si

---

[57] Le gouvernement fédéral allemand parle dans sa stratégie high tech d'*Industrie 4.0*, où l'accent est mis sur l'informatisation des techniques de fabrication: http://www.bmbf.de/de/9072.php

[58] Voir les scénarios décrits dans MELANI, rapport semestriel 2013/2, chapitre 5.5: Attaques contre les routeurs domestiques: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=fr (état: le 28 février 2015).

p. ex. on dispose de WC intelligents[59] qui ne rincent plus tant qu'on n'a pas remis du papier ou parce que la liaison Internet est interrompue, il faudrait qu'une solution manuelle soit prévue. Enfin, il importe de penser au risque de manipulation malveillante des processus physiques pilotés à distance par des tiers non autorisés. Des individus éprouvant un malin plaisir à nuire peuvent causer de sérieux préjudices, voire même se servir des appareils et services qu'ils contrôlent comme d'une arme de chantage face à leurs utilisateurs légitimes.

5.3 Variantes de chantage

Parmi les différents moyens utilisés par les criminels pour valoriser leurs attaques, il en est un qui a connu un essor spectaculaire au cours des dernières années: le rançonnage. Les criminels cherchent toujours plus à extorquer de l'argent, la plupart du temps en utilisant comme moyen de pression des données appartenant à leur victime.

Dans un premier type de modus operandi, les criminels accèdent à des données sensibles afin d'opérer un chantage à la divulgation. Si une somme ne leur est pas versée, les données seront publiées. Plusieurs cas de ce type visant des entreprises ont été rendus publics au cours des six mois sous revue. On peut notamment citer les agissements du groupe de pirates Rex Mundi, qui a fait plusieurs victimes avec un mode opératoire identique. Une *injection sql* sur le site de l'entreprise permet tout d'abord d'accéder à une base de données, contenant typiquement des informations concernant des clients et les échanges qu'ils ont eus avec l'entreprise. Par la suite, les pirates contactent l'entreprise victime: si un versement n'est pas effectué, les données volées seront publiées. Des attaques plus sophistiquées ayant également comme finalité un chantage à la divulgation d'informations sensibles ont aussi été révélées. On pense ici notamment à l'attaque ayant touché Sony Pictures Entertainment (voir chapitre 4.1). Dans ce type de cas, les criminels espèrent que le dommage à l'image risqué incitera la société piratée à payer afin que la faille ne soit pas ébruitée.

Si des menaces s'appuyant sur une atteinte à la confidentialité des données sont utilisées comme levier pour obtenir de l'argent, une tendance encore plus marquante, tout particulièrement pour les individus, est celle des ransomware, qui eux visent la disponibilité des données. Les différentes familles identifiées, des premiers cas bloquant l'ordinateur de la victime à Cryptolocker et autres maliciels chiffrant les données contenues sur la machine infectée, s'avèrent être une source de revenus inépuisable pour les criminels. De nombreux experts s'accordent à dire que cette tendance va s'inscrire dans la durée. Le succès des ransomware s'explique bien entendu par la propension des victimes à payer pour récupérer l'accès à leurs données ou à leur machine. Cette dernière semble élevée si l'on en croit une étude de l'Université du Kent, qui précise que 40% des victimes de Cryptolocker paient dans l'espoir de récupérer leurs données[60]. Pour le criminel, ce n'est donc pas la valeur intrinsèque des données visées et les possibilités de revente ou d'utilisation qui importent, mais plutôt la valeur que la victime accorde à ses données, ce qui l'amène à payer dans l'espoir de les récupérer. Ainsi, les particuliers auraient tort de négliger la protection de leurs données personnelles sous prétexte qu'elles ne présentent pas de valeur pour un attaquant potentiel. A partir du moment où ces données ont une valeur (même sentimentale) pour l'utilisateur, un potentiel «maître chanteur» les juge intéressantes.

---

[59] http://www.heise.de/newsticker/meldung/31C3-Hacker-nehmen-vernetzte-Toiletten-ins-Visier-2507287.html (état: le 28 février 2015).

[60] http://www.kent.ac.uk/news/science/528/cryptolocker-victims-pay-out (état: le 28 février 2015).

Les criminels à l'œuvre derrière ces méthodes de rançonnage ont de beaux jours devant eux. Un exemple récent attire l'attention sur la possibilité de cibler des sites Web mal sécurisés. Dans ce cas[61], le mode opératoire consiste à chiffrer la base de données du site, puis à demander une rançon à l'administrateur souhaitant récupérer l'accès aux données. Une autre perspective inquiétante est liée au développement de l'Internet des objets (Internet of things) et à la mise en réseau de plus en plus d'appareils, qui semble ouvrir aux «maîtres chanteurs» des potentialités d'attaques infinies. N'importe quel système de contrôle ménager, outil ou appareil relié à Internet devient en effet vulnérable. On peut tout à fait imaginer des scénarios où des criminels cherchent à rendre un appareil ménager inaccessible, puis demandent de l'argent à la victime pour lui permettre de le réutiliser. Même si dans bien des cas, il existe des moyens de débloquer l'appareil soi-même, ou alors d'actionner son mode de fonctionnement «physique», le désagrément occasionné et l'ignorance pourraient inciter de nombreuses personnes à payer, notamment lorsqu'il s'agit de petites sommes.

Ces quelques exemples récents, de même que les perspectives évoquées, rappellent l'importance de ne pas négliger les attaques menées sous l'angle de la disponibilité. Parmi le trio du modèle classique «confidentialité – intégrité – disponibilité», les comptes rendus des attaques actuelles ou les évaluations de nouveaux produits et services ont trop tendance à se focaliser sur la confidentialité. Il convient donc de garder à l'esprit qu'il est très profitable pour les escrocs de compromettre la disponibilité de données ou de services, à condition de bien cibler les utilisateurs. Cet enjeu actuel – avec les différents ransomware en circulation – deviendra toujours plus brûlant, en raison de la mise en réseau croissante de différents services ou appareils. D'où l'importance de ne pas s'intéresser qu'au problème des données personnelles susceptibles d'être prélevées et utilisées, et d'examiner systématiquement les possibilités de rendre ces services inaccessibles à des fins de rançonnage.

5.4 Navigation par satellite dans l'aviation

Le *Global Positioning System (GPS)* est un système mondial de localisation permettant, à un moment précis, de déterminer une position géographique (latitude, longitude et altitude) en captant, à l'aide d'un récepteur, les signaux émis par des satellites. On trouve désormais presque partout des récepteurs GPS – dans les smartphones, les appareils photo numériques et jusqu'aux automobiles. En particulier, toujours plus d'applications importantes pour la sécurité recourent à la navigation par satellite.

Le cas de l'aviation civile l'illustre bien. L'Office fédéral de l'aviation civile (OFAC) a approuvé pour la première fois en Suisse, le 17 février 2011, une procédure d'approche assistée par satellite pour la piste 14 (approche par le nord) de l'aéroport de Zurich.[62] Le 18 octobre 2012, l'exploitant de l'aéroport introduisait avec la société de contrôle aérien Skyguide le décollage assisté par satellite sur la piste 34. C'était la première fois en Suisse que la procédure de départ définissait aussi le rayon de virage à effectuer. Puis le 14 octobre 2014, un appareil de Swiss effectuait à Zurich la première approche de précision par GPS.[63] Il n'est toutefois prévu d'équiper toute la flotte de cette nouvelle technologie que lorsque la plupart des aéroports desservis seront outillés pour la procédure d'approche assistée par satellite.

---

61 https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html (état: le 28 février 2015).

62 Voir MELANI, rapport semestriel 2011/1, chapitre 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=fr (état: le 28 février 2015).

63 http://www.swiss.com/corporate/de/medien/newsroom/medienmitteilungen/medienmitteilung20141015 (état: le 28 février 2015).

Cette évolution ne doit pas faire oublier que la navigation par satellite n'a pas été expressément conçue pour l'aviation civile, et qu'il suffit de peu de chose pour la perturber, à dessein ou involontairement. Les dysfonctionnements du système GPS de l'aéroport de Newark aux Etats-Unis en sont la preuve. Après plusieurs mois d'investigations, il s'est avéré que ces perturbations étaient dues à un chauffeur de poids lourds, qui faisait régulièrement des haltes à proximité de l'aéroport et disposait d'un perturbateur (*GPS jammer*).

Il n'est donc pas possible de se limiter à utiliser les signaux GPS. Il faut un second système, qui vérifie l'intégrité des données et qui serve à reconnaître les pannes ou manipulations. Le signal GPS normal, spécifié pour une précision de 9 à 17 mètres, est d'ailleurs trop inexact pour les approches de précision. Sans compter que des facteurs extérieurs, comme le rayonnement ionisant ou un changement de satellite GPS, peuvent provoquer des écarts. D'où la mise en place à Zurich de la procédure GBAS (Ground Based Augmentation System), système d'augmentation des performances basé au sol. Quatre stations de référence dont la position exacte est connue calculent la correction différentielle à appliquer au «GPS normal», autrement dit l'erreur de mesure du signal GPS actuel. L'écart est ensuite communiqué par radio à l'avion.[64] Une grande attention est apportée à l'intégrité des données, et la correction différentielle fait l'objet d'une transmission sécurisée.

Un autre système de renforcement, baptisé EGNOS (European Geostationary Navigation Overlay Service), s'utilise en Europe dans la navigation aérienne.[65] Là aussi, des points de référence répartis dans toute l'Europe accroissent la précision du signal GPS, tout en vérifiant son intégrité. A supposer que le système GPS envoie des données fausses, l'erreur sera découverte en six secondes et signalée au pilote. La correction différentielle parvient aux avions par satellite géostationnaire. Le signal est également transmis par Internet. Les récepteurs GPS peuvent recevoir et exploiter le signal, et du même coup l'erreur est bien inférieure à 10 mètres. EGNOS est un projet commun de l'Agence spatiale européenne (ASE), de l'UE et de l'Organisation européenne pour la sécurité de la navigation aérienne (Eurocontrol), conçu comme première étape vers le système européen de navigation par satellite Galileo. Le système EGNOs coûte moins cher que GBAS, faute d'équipements techniques au sol. Outre sa précision accrue, il se distingue du GPS exploité par des Etats non européens par le fait qu'il est soumis au contrôle des exploitants susmentionnés, et donc que la qualité du signal est surveillée en permanence.

Dans le cas d'EGNOS, le signal de correction est transmis par satellite géostationnaire aux avions, et peut être capté par tout le monde. EGNOS n'est rien d'autre qu'une extension et un affinement du signal GPS existant. Autrement dit, des manipulations ont beau sembler difficiles, on ne peut entièrement les exclure, comme pour n'importe quel système technique. La sécurité, qui dépend des diverses composantes et de leurs fabricants, s'avère ici prioritaire. Les entreprises fournissant des composantes destinées à EGNOS doivent dès lors répondre à des exigences particulières en matière de sécurité. A ce titre, les experts en matière de sécurité du Département fédéral de la défense, de la protection de la population et des sports (DDPS) contrôlent minutieusement les sociétés suisses désireuses de participer au programme Galileo et EGNOS. [66]

---

64 http://www.skyguide.ch/fileadmin/user_upload/publications/Factsheets/1201_Factsheet_Satellitennav_System e_Verfahren_fr.pdf (état: le 28 février 2015).

65 http://www.esa.int/Our_Activities/Navigation/The_present_-_EGNOS/What_is_EGNOS (état: le 28 février 2015).

66 https://www.news.admin.ch/message/index.html?lang=fr&msg-id=53264 (état: le 28 février 2015).

Les systèmes TIC modernes sont souvent favorisés, même dans les domaines où la sécurité est un impératif absolu. Dans de nombreux cas, il s'agit de moderniser les systèmes ou de recourir à des systèmes dont l'exploitation serait plus efficace, sans absorber de ressources supplémentaires. Or le gain d'efficacité souhaité ne devrait pas intervenir dans l'évaluation des risques et être mis en relation avec les considérations de sécurité. Les systèmes TIC peuvent en revanche utilement compléter d'anciens systèmes de sécurité. Le défi posé par l'usage de tels systèmes ne réside toutefois pas seulement dans l'intégrité des données transmises, et tient aussi à la disponibilité des systèmes. Une perturbation du signal GPS oblige les avions en phase d'approche à poursuivre leur atterrissage avec d'autres systèmes à disposition. Cela ne pose aucun problème tant que les régimes d'atterrissage n'opèrent pas de distinction entre les systèmes à disposition, ou que d'autres systèmes restent proposés, comme le système d'atterrissage aux instruments (ILS). S'il s'agit d'un système spécifique à un aéroport précis, des perturbations auraient un caractère local, comme pour le système ILS. A contrario, une panne d'EGNOS affecterait l'ensemble du trafic aérien au niveau européen.

5.5 Failles de sécurité – divulgation responsable

Les internautes sont constamment exposés à des failles de sécurité – soit directement, soit de manière indirecte. L'utilisateur moyen connaît surtout les lacunes des produits Microsoft, ainsi que celles d'Acrobat-Reader et de Flash-Player. Les défaillances des composantes de sécurité ou de cryptage font également les gros titres. L'exemple le plus célèbre dans ce domaine est Heartbleed, dont il a été question dans le précédent rapport semestriel. Pour la période sous revue, il convient de mentionner les vulnérabilités Poodle et Kerberos (voir chapitre 4.9). La base de données où la société MITRE répertorie les lacunes de programmes rendues publiques signale au total 7945 failles de sécurité pour l'année 2014, un véritable record[67]. En réalité, la palette est bien plus grande, allant des sites vulnérables aux mauvaises configurations, qui n'apparaissent pas dans la base de données MITRE. Il s'avère donc que pratiquement tout logiciel utilisé comporte au moins une faille de sécurité. Cette évolution amène toujours plus à s'interroger sur les processus à suivre, lorsqu'une vulnérabilité a été découverte.

Par exemple, la plupart des internautes s'imaginent que le découvreur fournit (gratuitement) les informations en sa possession à l'entreprise concernée, afin qu'elle propose au plus vite une mise à jour. Or le marché de la sécurité est âprement disputé, et la gestion des informations dans ce secteur s'apparente toujours à un exercice de corde raide. Des intérêts divergents, y c. financiers, y jouent toujours un rôle important. Quiconque découvre une vulnérabilité rend service au fabricant, qui aurait dû s'en apercevoir lors de ses contrôles de qualité. Tout indique que différentes entreprises sont actives sur ce marché et qu'elles sont à l'affût des lacunes de sécurité des programmes, pour en tirer des profits monétaires. Un exemple ayant fait les gros titres en 2012 vient de la société maltaise ReVuln, dont le modèle d'affaires consiste non pas à signaler aux fabricants les failles encore inconnues des produits SCADA, mais à les vendre aux gouvernements et à d'autres «clients solvables».[68] Dans le secteur des infrastructures critiques notamment, une telle opération peut être lucrative, en raison des attentes de fonctionnement irréprochable et parce que les gouvernements sont bien obligés de garantir la sécurité de leurs systèmes vitaux. Or cette

[67] http://cvedetails.com/browse-by-date.php (état: le 28 février 2015).

[68] http://www.computerworld.com/article/2493333/malware-vulnerabilities/security-firm-finds-scada-software-flaws--won-t-report-them-to-vendors.html (état: le 28 février 2015).

commercialisation risque d'aboutir à ce que des failles de sécurité ne soient pas corrigées pour des raisons financières, ou alors à ce que des criminels solvables apprennent l'existence d'une vulnérabilité. En outre, en payant pour connaître les lacunes de sécurité, les Etats prennent des risques que l'on connaissait déjà avant la publication des documents de Snowden. La même année 2012 Chaouki Bekrarder, CEO et expert en cyberpiratage de la société VUPEN, confiait dans une interview qu'il ne vendrait pas les failles de sécurité du navigateur Chrome pour un million de dollars à la société Google, préférant se tourner vers les clients de cette société, à commencer par les Etats membres ou partenaires de l'OTAN.[69]

Par ailleurs, les fabricants ne prennent pas au sérieux certaines failles de sécurité, ce qui est frustrant pour leurs informateurs. Tant qu'elle n'est pas de notoriété publique, ils ne voient aucune urgence à corriger la vulnérabilité. Il s'est ainsi avéré après coup, dans de nombreux cas, que le fabricant connaissait la faille des mois avant sa divulgation, mais qu'il avait négligé à ce moment-là de lui trouver une solution. De guerre lasse, l'auteur de la découverte menace parfois de révéler la lacune à une certaine date, pour obliger le fabricant à agir. Dans le pire des cas, elle sera publiée avant la mise à jour correspondante.

Alors que seule une réglementation étatique pourrait remédier le cas échéant à l'incurie des entreprises, le second problème peut parfaitement être résolu. Aux Pays-Bas, le National Cyber Security Center a publié par exemple un guide expliquant comment les découvreurs et les victimes de failles de sécurité doivent agir. Le Security Center fait office de centrale d'enregistrement, à laquelle les lacunes de sécurité découvertes peuvent être signalées. L'auteur de la découverte est instamment prié de ne publier aucune information. En contrepartie, il lui est promis que le sérieux de son rapport sur une vulnérabilité sera évalué dans les trois jours ouvrables, et un délai est fixé en vue de la résolution du problème. En outre, il est informé de l'avancement des travaux entrepris. Une fois la faille de sécurité publiée, il est dûment remercié et reçoit au moins un T-Shirt en souvenir.[70]

5.6 Objets politiques

Objet	N°	Titre	Déposé par	Date de dépôt	Conseil	Dépt	Etat des délibérations et lien
Po	14.3739	Control by Design. Renforcer les droits de propriété pour empêcher les connexions indésirables	Schwaab Jean Christophe	17.09.2014	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143739
Po	14.3782	Des règles pour la «mort numérique»	Schwaab Jean Christophe	24.09.2014	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143782
Ip	14.3884	Des groupes d'électricité envisagent de mettre en vente leur participation dans Swissgrid	Killer Hans	25.09.2014	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20143884
Qst.	14.5642	Services Internet. Démantèlement de groupes d'entreprises qui dominent le marché	Glättli Balthasar	03.12.2014	CN	DEFR	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20145642
Ip	14.4138	Procédure d'adjudication pour les infrastructures TIC critiques de l'administration fédérale	Noser Ruedi	10.12.2014	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20144138

69 http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ (état: le 28 février 2015).

70 https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html (état: le 28 février 2015).

Ip	14.4123	Développement de l'infrastructure des TIC. Créer un environnement plus favorable aux investissements	Guhl Bernhard	10.12.2014	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20144123
Ip	14.4194	Mégadonnées (big data). Potentiel et perspectives de développement de l'économie de l'information en Suisse	Graf-Litscher Edith	11.12.2014	CN	DFI	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20144194
Po	14.4294	Index Web pour un Internet libre et ouvert. La Suisse ne figure qu'au 18^{e} rang	Glättli Balthasar	12.12.2014	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20144294

6 Glossaire

0-day exploit	Exploit paraissant le jour même où une faille de sécurité est rendue publique.
Active Directory	Active Directory (AD) est le nom du service d'annuaire de Microsoft Windows Server.
Advanced Persistent Threat	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.
Attaque par force brute	Méthode consistant à tester une à une toutes les combinaisons possibles pour trouver un mot de passe ou une clé (brute-force attack).
Authentification à deux facteurs	Au moins deux des trois facteurs d'authentification sont exigés : un élément que l'on connaît (p. ex. mot de passe, code PIN, etc.) un élément que l'on détient (p. ex. certificat, jeton, liste à biffer, etc.) un élément qui nous est propre (p. ex. empreinte digitale, scanner rétinien, reconnaissance vocale, etc.)
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Black Hat Search Engine Optimization (BHSEO)	L'optimisation pour les moteurs de recherche (search engine optimization, SEO) est un ensemble de techniques visant à augmenter la visibilité d'un site Web dans les résultats des moteurs de recherche. Les pratiques «black hat» (BHSEO) consistent à manipuler par tous les moyens le référencement.
Bluetooth	Technologie permettant d'établir une communication sans fil entre deux équipements terminaux, mise en œuvre surtout dans les téléphones mobiles, les ordinateurs portables, les PDA (assistants numériques personnels) et les périphériques d'entrée (p.ex. la souris).
Byte	Plus petite unité adressable d'un ordinateur, composée généralement d'une suite de 8 bits.

Classement dans les moteurs de recherche	Positionnement d'un site dans les résultats des outils de recherche suite à une requête.
Cloud	Le cloud computing (informatique en nuage) désigne l'utilisation de serveurs distants pour traiter ou stocker l'information. Les logiciels eux-mêmes peuvent y être déportés.
Code source	Le code source (angl. source code) est un ensemble d'instructions écrites dans un langage de programmation informatique évolué, qui se présente sous la forme d'un texte lisible par un utilisateur.
Content Management System (CMS)	Un système de gestion du contenu (CMS, acronyme de content management system) est une solution flexible et dynamique permettant aux entreprises ou organisations de corriger et ajouter sur des sites Web des textes, des photos et des fonctions multimédias. Un auteur peut actualiser un tel système sans connaissances préalables en programmation ou en langage HTML. Les informations gérées dans ce contexte sont appelées contenu (content).
Cookie	Témoin de connexion. Petit fichier texte enregistré sur l'ordinateur de l'internaute à l'occasion de sa visite sur une page Web. Les témoins permettent par exemple de mémoriser les réglages personnels pour un site Internet. Il est cependant aussi possible de les utiliser abusivement, notamment pour établir un profil détaillé des habitudes de l'internaute.
DDoS	Attaque par déni de service distribué (Distributed Denial-of-Service attack) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Débordement de tampon	Fréquente faille de sécurité des logiciels, dont les pirates profitent pour glisser dans la mémoire tampon des codes permettant de faire exécuter des programmes d'accès (en anglais buffer overflow).
Defacement	Défiguration de sites Web.
Ethernet	Ethernet est un protocole de réseau local, où un câble diffuse les données à toutes les machines connectées.

Firewall	Un pare-feu (firewall) protège les systèmes informatiques en surveillant et, éventuellement refusant, les connexions entrantes ou sortantes. Un pare-feu personnel (personal firewall ou desktop firewall) est en revanche installé pour protéger un ordinateur unique; il est directement installé sur le système à protéger, c'est-à-dire sur votre ordinateur.
Firmware	Microprogrammes. Instructions enregistrées dans une puce pour commander un appareil (p.ex. numériseur, carte graphique, etc.). Elles sont en général modifiables par des mises à jour.
Global Positioning System (GPS)	Global Positioning System (GPS), dont le nom offi-ciel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Global System for Mobile Communications (GSM)	Le réseau GSM (Global System for Mobile Communications, au départ Groupe spécial mobile) constitue un standard de téléphonie mobile entièrement numérique, permettant de transmettre la voix ainsi que des messages texte (SMS) ou multimédia.
GPS-Jammer	Appareil servant à brouiller les données GPS.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le server.
International Mobile Subscriber Identity (IMSI)	L'IMSI est un numéro unique, qui permet à un réseau mobile GSM ou UMTS d'identifier un usager.
Jailbreak	Le jailbreaking (de l'anglais: évasion), ou débridage, est une opération consistant à outrepasser une restriction à l'utilisation

	des produits Apple, à l’aide de logiciels adéquats.
Keylogger	Appareil ou programme intercalé entre l'ordinateur et le clavier qui permet d'enregistrer toute saisie au clavier.
Kit d’exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d’accéder au système.
Malicious Code	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Man in the Middle	Man-in-the-Middle attack, attaque de l’intermédiaire Attaque où le pirate s’immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
Média amovible	Mémoire de masse conçue pour être insérée et retirée d’un ordinateur sans devoir éteindre ce dernier.
Message Authentication Code (MAC)	Un code d’authentification de message permet de vérifier l’intégrité de données ou messages.
Near Field Communication (NFC)	La communication en champ proche (near field communication) est une norme internationale d’échange de données entre des périphériques à courte portée et à haute fréquence.
Network Attached Storage (NAS)	Un serveur de stockage en réseau (serveur NAS) désigne une mémoire de masse autonome, accessible par l’intermédiaire d’un réseau local.
Passerelle de sécurité	Nom générique de tous les systèmes servant à garantir la sécurité informatique au sein d’une organisation.
Patch	Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d’erreurs et remédie ainsi p.ex. à une lacune de sécurité.
Phishing	Via l'hameçonnage, des pirates tentent

	d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées.
Plug-in	Plugiciel. Logiciel complémentaire qui étend les fonctions de base d'une application. Exemple : les plugiciels Acrobat pour navigateurs Internet permettent un affichage direct des fichiers PDF.
Point of Sales	Un terminal EFT/POS est un terminal de point de vente (POS, point of sale) acceptant le paiement sans numéraire (EFT, electronic funds transfer).
Porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
Proof of concept (POC)	Démonstration de faisabilité.
Proof of concept (POC)	Proof of Concept Démonstration brève, et pas nécessairement complète, du bien-fondé d'une idée ou d'une méthode A titre d'exemple, les exploit codes sont souvent publiés sous forme de PoC, pour souligner les conséquences d'une faille de sécurité.
Protocole réseau	Protocole de communication utilisé par toutes les stations échangeant des données sur le réseau.
RAM scraper	Maliciel parvenant à copier les données contenues sur la bande magnétique d'une carte de crédit, dans les instants qui suivent son utilisation sur le terminal de paiement, alors qu'elles sont contenues en clair dans la mémoire vive (*RAM*)

Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Requête	Message transmis par un client à un serveur, dans un modèle client-serveur.
Réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis.
Réseautage personnel	Traduction du concept américain de «social networking». Un profil ou page de membre permet aux utilisateurs d'une plateforme d'échanger et d'établir des relations entre eux. Des données personnelles y sont souvent publiées (nom, date d'anniversaire, photos, intérêts professionnels, loisirs, etc.).
Rich Text Format	Le Rich Text Format (RTF) est un format de fichier développé pour les textes.
Roaming	L'itinérance ou *roaming* permet à l'abonné d'un réseau mobile d'utiliser son appareil dans celui d'un autre opérateur.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Service d'anonymisation Tor	Tor est un logiciel d'anonymisation en ligne. Tor protège l'utilisateur de l'analyse du trafic.
Session	Période de temps continue s'écoulant entre la connexion et la déconnexion d'un client à un serveur.

Session Hijacking	Détournement de session; un pirate réussissant cette attaque pourra prendre possession de la connexion pendant toute la durée de la session.
Short Message Service (SMS)	Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
Signature	Mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur à l'aide d'une clé publique.
Smartphones	Un smartphone est un téléphone mobile doté des fonctions d'un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
Spear-Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
SSL	Secure Sockets Layer Protocole permettant de communiquer en toute sécurité sur Internet. SSL s'emploie aujourd'hui p. ex. pour les transactions financières en ligne.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Universal Mobile Telecommunications System (UMTS)	L'UMTS est l'une des technologies de téléphonie mobile de troisième génération, optimisée pour le transfert de données.
Universal Serial Bus Serieller Bus (USB)	Universal Serial Bus Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus

	et configurés automatiquement.
Upstream-Provider	Un fournisseur en amont (upstream provider) permet aux fournisseurs d'accès de se connecter à Internet.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.