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
http://www.melani.admin.ch

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2015/II (juillet à décembre)

28 AVRIL 2016

CENTRALE D'ENREGISTREMENT ET D'ANALYSE POUR LA SÛRETÉ DE L'INFORMATION MELANI
http://www.melani.admin.ch

1 Aperçu / Sommaire

2 Editorial

MELANI: Perpétuer les efforts engagés et renforcer les partenariats transverses avec l'économie!

Jean-Pierre Therre, Executive Vice President / Head of Technology Risk & Business Continuity, Banque Pictet & Cie SA, Associate Fellow GCSP, Lead Lecturer UniGE.

Dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), les objectifs stratégiques dévolus à MELANI sont la détection précoce des menaces et des dangers dans le cyberespace, la réduction des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage**,** ainsi que le renforcement de la capacité de résistance des infrastructures critiques.

Dans ce contexte essentiel pour favoriser la bonne résilience opérationnelle de tous les acteurs économiques publics ou privés, l'équipe MELANI, malgré des ressources qui restent encore trop limitées, s'attache avec diligence à répondre aux objectifs fixés. Mais MELANI s'efforce aussi de consolider des initiatives sectorielles visant à renforcer le partage d'informations pertinentes ainsi que des échanges structurés entre les acteurs des principaux secteurs économiques. Par exemple les rencontres semestrielles regroupant un grand nombre de représentants du secteur bancaire et financier (Information Exchange Financial Sector) sont devenues des évènements de référence. C'est l'occasion pour les experts présents de découvrir de manière condensée le spectre des menaces cyber, parfois spécifiques, observées en Suisse et aussi à l'étranger.

S'inscrivant dans la même volonté d'échanges et de collaboration, la journée « Swiss Cyber Risks 2015 » orchestrée par MELANI au Stade de Suisse le 02.11.2015, en présence de nombreux professionnels de l'économie et autorités politiques et militaires, a permis d'établir des ponts inattendus et très appréciés entre le secteur public et l'économie privée.

De fait, ces efforts s'inscrivent en excellente intelligence avec le renforcement d'un vrai partenariat transversal public-privé (PPP) souhaité par tous les professionnels concernés du fait de la multiplication avérée, de la complexité grandissante et du caractère toujours plus international des menaces cyber. Les actions de prévention, détection et réaction, ainsi que les principes de gestion de crise, ne peuvent plus être anticipés par des institutions isolées mais plutôt par des initiatives concertées et structurées entre tous les acteurs de la communauté nationale. En ce sens le partenariat entre MELANI et l'association «Swiss Cyber Experts (SCE)»[1] qui permet de regrouper les connaissances des experts dans le but de fournir un diagnostic efficace en cas de grave attaque cybernétique, est bien exemplaire.

Que les équipes de MELANI, sous la direction de Pascal Lamia, soient remerciées pour leurs multiples initiatives d'informations et leurs efforts louables de coordination intersectorielle !

[1] https://www.swiss-cyber-experts.ch/ (état: 29 février 2016).

3 Thème prioritaire: gestion des lacunes de sécurité

Les internautes sont constamment exposés à des failles de sécurité – soit directement, soit de manière indirecte. La banque de données de MITRE, organisation à but non lucratif enregistrant systématiquement les lacunes de sécurité, a répertorié au niveau mondial 6419 vulnérabilités durant 2015[2]. Très peu d'entre elles ont toutefois fait les gros titres. On peut de même considérer qu'une partie des lacunes de sécurité sont absentes de cette banque de données car pour toutes sortes de raisons, il arrive qu'elles ne soient pas signalées aux fabricants.

D'un autre côté, la palette des appareils raccordés à Internet pour accéder aux composantes d'un système d'exploitation et aux *bibliothèques logicielles* correspondantes ne cesse de s'agrandir. Cette situation accroît encore les effets et l'impact des lacunes de sécurité. En outre, beaucoup de ces systèmes ne font généralement pas l'objet d'actualisations automatiques. Honnêtement, quand avez-vous mis à jour pour la dernière fois le *firmware* (microprogramme) de votre *routeur* ou le logiciel de votre radio Internet? Les mises à jour absentes ou non exécutées sont à l'origine d'une augmentation constante du nombre des systèmes vulnérables.

3.1.1 Absence de politique de gestion des mises à jour

Dans de nombreux domaines, les mises à jour automatiques sont devenue la norme. Cependant cela n'est pas encore le cas partout : La faille de sécurité Stagefright, rendue publique en juillet 2015, a montré de manière exemplaire l'absence de processus efficaces et rapides de mise à jour pour le système Android. Il n'est donc guère étonnant qu'une étude de 2011 ait abouti à la conclusion que 56% des smartphones Android possèdent un système d'exploitation désuet.[3] Bien souvent, il faut énormément de temps pour que les mises à jour parviennent aux utilisateurs. Car Google est tributaire aussi bien des fabricants de smartphones, comme Samsung ou LG, que des opérateurs de téléphonie mobile. Avant toute distribution, ces derniers doivent d'abord tester et certifier les mises à jour que leur proposent les fabricants. Par contre, Apple peut directement distribuer ses mises à jour aux clients. Google a annoncé après cet incident un cycle mensuel de mises à jour. Quelques fabricants de téléphones mobiles souhaitent suivre cette pratique, et sont en discussion avec les exploitants de réseaux. Des compléments d'information sur Stagefright figurent au chapitre 5.6.1.

Un autre problème tient aux systèmes de gestion de contenu (*content management system,* CMS) de sites Web. D'habitude, des mises à jour sont rapidement disponibles pour les grands CMS. Or bien souvent, les exploitants ne sont guère motivés à les reprendre. MELANI l'a déjà montré de manière frappante dans son précédent rapport semestriel.[4]

---

2 http://www.cvedetails.com/ (état: 29 février 2016).

3 https://www.carbonblack.com/files/info-graphic-orphan-android/ (état: 29 février 2016).

4 Voir rapport semestriel 1/2015, chap. 3 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-1.html (état: 29 février 2016).

3.1.2 Failles de sécurité: un marché lucratif

Avant qu'une lacune de sécurité ne soit comblée et que le *patch* (programme correctif) correspondant ne voie le jour, il faut que le fabricant en ait connaissance. Cela paraît banal à dire, et pourtant c'est loin d'être toujours le cas. 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 compris financiers, y jouent toujours un rôle majeur.

La cyberattaque menée en été 2015 contre Hacking Team, entreprise italienne vendant des logiciels servant à l'espionnage et à la surveillance, et la publication subséquente de données commerciales confidentielles l'ont clairement montré. Outre des logiciels de surveillance et des courriels personnels, les données dérobées comprenaient diverses vulnérabilités *zero-day* que la société Hacking Team avait acquises. Dans un cas concret, elle avait payé 45 000 dollars à un hacker russe pour obtenir une faille de *Flash*.[5] On ignore à qui ce hacker russe a encore vendu la faille en question.

Ni les transactions concrètes liées aux logiciels de surveillance, ni les cas d'espionnage ou les aspects opérationnels de la politique nationale d'armement numérique ne sont discutés sur la place publique. Il est par conséquent difficile de cerner la portée exacte et la quantité des failles zero-day en circulation. Chaouki Bekrar, ancien CEO et expert en cyberpiratage de la société VUPEN, rompt toutefois avec ce principe de discrétion. Dès 2012, il expliquait dans une interview que même si on lui proposait un million de dollars, il ne vendrait pas les failles de sécurité découvertes au fabricant du logiciel, mais exclusivement à ses propres clients – en l'occurrence les Etats membres ou partenaires de l'OTAN. Entre-temps, Chaouki Bekrar a créé la société Zerodium, elle aussi spécialisée dans la surveillance des appareils informatiques. En 2015, il a lancé au nom de cette compagnie un concours doté d'un million de dollars, invitant les hackers à lui annoncer une méthode permettant de contourner les restrictions à l'utilisation (*jailbreak*) des iPads et iPhones dotés du tout récent système d'exploitation iOS 9.1[6]. Le succès a été au rendez-vous. Comme le montre cet exemple, le marché des vulnérabilités zero-day obéit aux règles économiques usuelles. Plus une faille est exclusive, plus elle se monnaie à un prix élevé.

Il faut définir certaines règles du jeu et créer des incitations adéquates, afin que les chercheurs divulguent les failles de sécurité aux fabricants de logiciels, au lieu de les vendre au plus offrant. Parmi les spécialistes de la sécurité informatique, un grand nombre de personnes s'engagent pour développer de bonnes pratiques (*Best Practices*) en la matière, sans chercher à en tirer un profit financier. Du côté des fournisseurs, à qui l'on annonce des failles et qui devraient mettre en place les patchs (correctifs) nécessaires, il n'y a pas encore une approche généralement admise. Mais si les fabricants ne prennent pas au sérieux les vulnérabilités signalées ou, pire encore, menacent leurs informateurs de porter plainte contre eux, il n'est guère étonnant qu'elles soient publiées à leur insu ou qu'on les retrouve sur le marché des failles zero-day, avant même que de la mise à jour correspondante ne soit disponible.

---

5 http://arstechnica.com/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/ (état: 29 février 2016).

6 https://www.zerodium.com/ios9.html (état: 29 février 2016).

L'affaire survenue entre FireEye, prestataire de sécurité informatique basé aux Etats-Unis et ERNW, homologue ayant son siège à Heidelberg, montre à quel point les rapports portant sur la vulnérabilité sont sensibles. Un chercheur d'ERNW ayant découvert cinq failles de sécurité dans le système de protection contre les maliciels de FireEye les a annoncés à cette entreprise. ENRW prévoyait de publier ces lacunes dans un délai de 90 jours. Or il en est résulté un litige sur la notification qu'ERNW comptait publier. FireEye craignait que cette publication n'en dise trop sur le fonctionnement de son produit. De son côté, ERNW faisait valoir que de tels détails étaient nécessaires pour comprendre les vulnérabilités. En outre, ERNW prévoyait de présenter le fonctionnement desdites failles de sécurité à Londres, à la conférence 44CON sur la sécurité informatique. FireEye avait toutefois obtenu une décision de justice, ce qui fait que seule une version expurgée a été dévoilée.

3.1.3 Divulgation responsable

Divers pays ainsi que des éditeurs de logiciels ont reconnu l'absence de règles du jeu et de processus, et y ont réagi. Par souci d'une divulgation responsable des lacunes de sécurité, ils ont conçu des processus ad hoc (*responsible disclosure process*) et ont lancé des initiatives visant à identifier, corriger et signaler les erreurs logicielles, appelées *bug bounty programs*. On peut signaler ici le programme bug bounty de Microsoft, ou le programme de divulgation responsable du gouvernement néerlandais déjà évoqué dans le rapport semestriel 2/2014 de MELANI[7]. Le site government.nl[8] décrit en détail les étapes du traitement des vulnérabilités signalées, et ce à quoi le découvreur peut s'attendre. De grandes entreprises comme Google, Facebook et Twitter mènent également de tels programmes. Or au-delà des règles du jeu définies entre les chercheurs, les auteurs d'annonces et la société touchée (délai de correction des erreurs, aspects financiers et idéels, etc.), leur bon fonctionnement nécessite d'abord d'établir un solide rapport de confiance.

3.1.4 Situation juridique en Suisse

Outre les règles de conduite déjà indiquées à caractère facultatif, un cadre légal clair s'impose. Il devrait en particulier rester possible aux chercheurs en sécurité de traquer de telles vulnérabilités, car c'est l'unique moyen d'améliorer la sécurité des programmes. Une solution à cet égard consisterait à légalement se concentrer non sur la recherche de lacunes, mais sur l'exploitation ultérieure qui en est faite. Le droit pénal suisse se base sur la motivation des acteurs: est punissable «quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction […]»[9], ou alors «aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles

---

7 Rapport semestriel 2/2014, chapitre 5.5 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2014-2.html (état: 29 février 2016).

8 https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure (état: 29 février 2016).

9 Art. 143bis, al. 2, CP: https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a143bis (état: 29 février 2016).

des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une [détérioration de données], ou qui aura fourni des indications en vue de leur fabrication […]»[10]. Autrement dit, il n'est pas punissable en droit suisse de rechercher des failles de sécurité pour les signaler au fabricant. Les échanges entre chercheurs de sécurité devraient également être autorisés. Par contre, quiconque publie des vulnérabilités sera puni, car il doit s'attendre à ce qu'un tiers s'en serve pour commettre des faits répréhensibles. D'où le reproche d'avoir pris sciemment en compte un tel risque, et donc agi par dol éventuel. Il s'ensuit qu'il n'est pas permis en Suisse de menacer un fabricant de la publication (détaillée) d'une vulnérabilité, pour l'inciter à la combler. Un chercheur est par contre libre de signaler en termes généraux sur Internet l'existence d'une faille de sécurité identifiée, et d'y fustiger le cas échéant la négligence du fabricant.

Il n'existe toutefois (encore) aucune règle établie sur l'indemnité qu'un fabricant est censé verser à l'auteur de la découverte et de l'annonce d'une vulnérabilité, et la jurisprudence devrait sans doute préciser ce point. Il serait notamment possible d'invoquer ici la «gestion d'affaires sans mandat»[11], ou la naissance d'une obligation résultant de l'enrichissement illégitime[12], puisque le fabricant reçoit une prestation. On peut toutefois douter qu'un chercheur ouvre un litige avec un fabricant et qu'un tribunal ait l'occasion de se prononcer sur un tel cas d'espèce. De leur propre avis, les chercheurs en sécurité ont mieux à faire que de se battre avec les avocats et la justice.

---

10 Art. 144bis, ch. 2, CC: https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a144bis (état: 29 février 2016).

11 Art. 419 ss CO: https://www.admin.ch/opc/fr/classified-compilation/19110009/index.html#id-2-14 (état: 29 février 2016).

12 Art. 62 ss CO: https://www.admin.ch/opc/fr/classified-compilation/19110009/index.html#id-1-1-3 (état: 29 février 2016).

4 Situation nationale

4.1 Cyber espionnage en Suisse

Le présent chapitre ne révèle pas de détails permettant d'identifier des opérations ou des cibles précises. En raison de l'anonymat que l'on doit la plupart du temps accorder à la victime et à la source de l'information, mais également du point de vue de la défense des intérêts de la place économique et de l'Etat, il serait contreproductif de révéler aux attaquants le niveau de connaissance. Néanmoins, notre vue d'ensemble des cas en cours nous permet de fournir un état des lieux de la situation du cyber espionnage en Suisse.

Avant de prétendre établir une typologie des cibles d'attaques, il convient de déterminer quel type d'information peut présenter une valeur aux yeux d'un éventuel attaquant. Comme nous nous limitons ici aux agressions profitant à un Etat, il s'agit d'informations l'aidant à atteindre ses objectifs stratégiques. Bien des agressions visent à connaître des agendas politiques (en particulier: négociations à venir, surveillance d'opposants politiques à l'étranger), sécuritaires (terrorisme), militaires voire économiques (innovation, savoir-faire, détails de relations commerciales notamment).

La Suisse est un champ privilégié pour des opérations cyber, car elle compte sur son territoire un grand nombre d'organisations possédant des informations très recherchées. A l'instar des représentations étrangères, des organisations internationales ou des communautés qui présentent un intérêt politique pour de nombreux Etats. Il en va de même pour des pans entiers de son activité économique, où le savoir-faire ou des informations sur des relations commerciales ou des offres actuelles permettraient aux acteurs économiques d'autres pays de bénéficier d'un avantage compétitif conséquent. On notera encore que pour de nombreux pays, l'espionnage économique nourrit un agenda politique plus large, et qu'il se justifie même parfois pour des raisons sécuritaires.

Dans le cadre d'opérations visant à acquérir ce type d'informations, on retrouve différents types de victimes. L'agresseur peut faire le choix d'attaquer directement la cible les détenant. Mais si par exemple cette dernière s'avère trop résiliente, il arrive qu'il adopte une stratégie en deux phases. Il cherchera ainsi à compromettre un fournisseur, pour accéder de là à sa cible finale. C'est notamment dans cette optique que des réseaux d'hôtels de la région lémanique ont été victimes de cyber espionnage. En effet l'agresseur ne s'intéressait pas aux hôtels, mais aux délégations qui y séjournaient pendant les négociations sur l'accord nucléaire iranien de 2014 et 2015[13]. Dans d'autres cas, ce sont des entreprises de maintenance ayant accès au périmètre sécurisé d'une société ou des prestataires en

[13] MELANI, rapport semestriel 1/2015, chap. 4.1.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-1.html (état: 29 février 2016).

télécommunications qui peuvent être ciblés en premier. L'attaque ayant visé BICS BELGACOM et révélée en 2013[14] illustre bien ce dernier cas de figure.

Dans d'autres cas, des entreprises ou des individus peuvent être des victimes collatérales d'enjeux les dépassant et ne les concernant pas. Il arrive en effet que les opérations infectent des tiers, à la suite d'une erreur de ciblage ou d'autres effets non voulus. En 2015, une entreprise du secteur viticole s'est ainsi trouvée infectée par un maliciel lors d'une campagne de cyber espionnage. Après vérification, et connaissant les centres d'intérêt des attaquants, l'incident a été rapidement ramené à sa dimension de «dommage collatéral».

[14] MELANI, rapport semestriel 2/2013, chap. 4.1
https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2013-2.html

Conclusions et recommandations :

Le cyber espionnage contre des intérêts helvétiques est une réalité. Il a déjà été question de plusieurs cas dans de précédents rapports semestriels de MELANI. Le rapport annuel du Service de renseignement de la Confédération (SRC) donne également un aperçu de la situation. En la matière, la prévention est une composante importante si ce n'est la plus importante afin de se protéger contre des tentatives d'espionnage. Pour une entreprise, la première étape nécessaire consiste à reconnaître l'existence d'un danger bien réel et non hypothétique. Les nombreux cas portés à la connaissance de MELANI attestent de cette prise de conscience. Pour combattre efficacement l'espionnage, il faut que les informations circulent et donc que les cas soient annoncés. Cette démarche permet aux autorités de prendre des mesures et de tirer les enseignements nécessaires au niveau législatif ou politique. Mais plus encore, en signalant ce type d'informations, les victimes permettent à d'autres organisations de détecter d'éventuelles intrusions dans leur réseau. Le traitement strictement confidentiel de telles données est ici primordial aux yeux des autorités.

MELANI joue un rôle actif depuis dix ans dans la protection contre les risques informatiques, en partenariat avec différentes entités privées. Son site Web propose un formulaire d'annonce permettant de signaler des incidents:

MELANI – Formulaire d'annonce :

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Le SRC mène avec son programme Prophylax une action de prévention et de sensibilisation dans le domaine de la non-prolifération et de l'espionnage économique. Prophylax entend sensibiliser les entreprises ainsi que les institutions de formation:

Programme Prophylax :

http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.html

4.2 Systèmes de contrôle industriels

A l'ère de l'Internet des objets, les technologies de l'information et de la communication – et donc les systèmes de contrôle industriels (*SCI*) interconnectés – investissent toujours plus de domaines de notre quotidien. Le cas échéant, la question des cyberrisques s'y pose aussi. Le présent rapport semestriel étudie plus en détail certains systèmes cruciaux intervenant dans le contexte de la mobilité.

4.2.1 Gestion de parking consultable librement

La plupart d'entre nous sommes confrontés dans la vie de tous les jours, à notre insu parfois, à la gestion technique du bâtiment (domotique), qui fait partie intégrante des systèmes de contrôle industriels. La gestion de parking constitue un de ses champs d'application, dans le

cas des grands complexes de bâtiments. L'utilisation des SCI va de la simple horloge de parking reliée au réseau jusqu'au système de gestion des parkings d'une ville entière, En octobre 2015, MELANI a appris qu'une interface de gestion de parking en suisse était consultable librement sur Internet. N'importe qui pouvait y voir en tout temps quelles étaient les places occupées. D'où par exemple la possibilité pour des cambrioleurs de savoir à quel moment les locaux ont le plus de chances d'être vides, ou quand les collaborateurs ne sont pas à la maison.

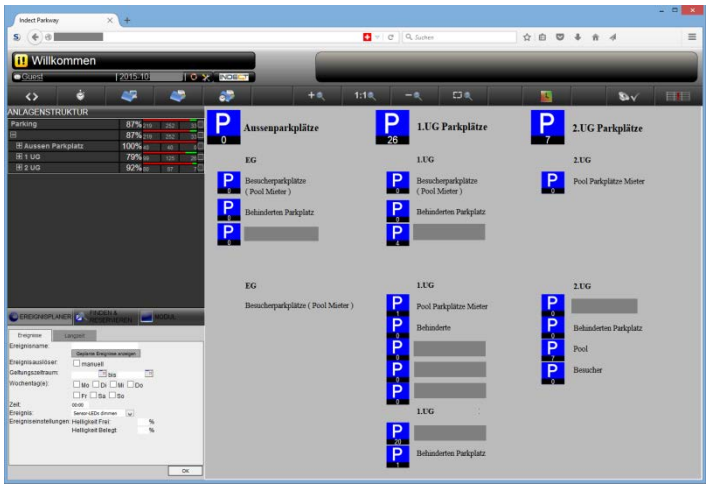

Fig. 1: Copie d'écran de l'interface de gestion du parking

MELANI a aussitôt expliqué à l'exploitant la situation et la menace potentielle.

4.2.2 Vulnérabilité de l'infrastructure ferroviaire

Les systèmes de contrôle industriels interviennent également dans les systèmes de transport, notamment dans les infrastructures ferroviaires toujours plus reliées à Internet. Ils s'emploient par exemple pour commander les signaux et régler les aiguillages. Au 32e Chaos Communication Congress, organisé du 27 au 30 décembre 2015 à Hambourg, le groupe russe *SCADA*-Strangelove[15] a présenté toutes sortes d'attaques possibles contre des infrastructures ferroviaires variées: outre les systèmes d'information des voyageurs publiquement accessibles, il n'était guère sorcier de découvrir les postes d'aiguillage automatisés, les caméras vidéo de surveillance et les stations solaires installées le long des tronçons. De tels SCI sont souvent vulnérables: l'accès à ces ressources est mal protégé, ils reposent sur des systèmes ou mécanismes de sécurité désuets, ou encore leurs mots par défaut sont connus. Afin de sensibiliser les équipementiers et les utilisateurs à cette problématique et de les convaincre de renoncer aux mots de passe standard, le groupe a publié une liste de 37 prestataires de composants de systèmes de sécurité usuels (par ex. serveurs, commutateurs), dont les mots de passe standard circulent sur Internet. La liste comprenait un fabricant suisse de routeurs et de solutions *VPN* destinés à l'industrie ferroviaire.

[15] https://blog.kaspersky.com/train-hack/10946/ (état: 29 février 2016).

Conclusion et recommandations

Nous utilisons les transports publics et commandons en ligne des marchandises, livrées si possible le lendemain. La logistique à notre disposition est toujours plus efficiente. Cela n'est toutefois possible que grâce à des systèmes de transport intelligents et à une gestion des stocks robotisée. Avec la mise en réseau croissante des objets qui nous entourent, les systèmes de contrôle industriels (SCI) avec leurs multiples facettes jouent un rôle croissant dans notre vie quotidienne.

Ce faisant, toujours plus de personnes sont exposées aux risques qui en découlent. MELANI propose sur son site Web une liste de mesures de protection des systèmes de contrôle industriels:

Mesures de protection des systèmes de contrôle industriels (SCI)

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

4.3 Cyberattaques (DDoS, défiguration de sites)

Les citoyens et entreprises suisses restent en butte à différents types d'attaques, ayant notamment pour cible leur site Web. Les attaques par déni de service distribué (DDoS) et les défigurations de sites sont d'autant plus problématiques pour les entreprises qu'elles ont besoin d'une présence en ligne crédible. Au deuxième semestre 2015, MELANI a observé une recrudescence d'attaques lancées contre des sites Web pour en diffuser ensuite des maliciels.

4.3.1 Réseaux publicitaires

Les agresseurs sont constamment à la recherche de possibilités d'infecter commodément un maximum d'appareils de victimes potentielles. Dans le passé, ils privilégiaient les courriels renfermant des liens ou des annexes. L'envoi de tels courriels ne demande guère de connaissances techniques. Or les chances de succès s'amenuisent toujours plus, car les internautes sensibilisés ne cliquent plus sur chaque annexe ou lien. D'ailleurs, les campagnes de publipostage par courriel ne passent pas inaperçues, et donc les maliciels sont très vite répertoriés par les banques de données des fabricants d'antivirus. D'où l'essor des *infections par drive-by download* pour propager les maliciels. Afin d'en assurer la diffusion à grande échelle, les escrocs piratent de préférence des sites Web très fréquentés. Avec une préférence pour les portails de journaux ou les réseaux publicitaires. Ces derniers ont pour particularité de gérer de manière centrale les contenus publicitaires, transmis ensuite aux journaux en ligne. Autrement dit, si une infection survient à ce niveau, elle risque d'être lourde de conséquences et d'entraîner un très grand nombre d'infections.

Deux cas de ce genre ont été signalés à MELANI durant la période sous revue:

4.3.1.1 Infection du site d'un quotidien

Une première infection a été signalée à MELANI par un chercheur en sécurité, le 11 septembre 2015. Un réseau publicitaire suisse exposait ses visiteurs au *kit d'exploits* Niteris. Or ce réseau approvisionne les éditions en ligne de divers quotidiens. D'où un nombre élevé de victimes potentielles. Lorsqu'un internaute visitait une page Web affichant une publicité compromise, le maliciel commençait par vérifier les paramètres linguistiques du terminal. S'il s'agissait de l'allemand ou du français, une série de vulnérabilités étaient testées dans l'Internet Explorer (par ex. CVE-2014-6332), dans Firefox (par ex. CVE-2013-1710), dans Java (par ex. CVE-2013-2465) ou Adobe Flash (par ex. CVE-2015-5119). Alors que les failles de sécurité des navigateurs étaient connues de longue date, remontant à 2013 et 2014, la mise à jour requise pour Adobe Flash n'était disponible que depuis le 7 juillet 2015. Les ordinateurs où ces programmes n'étaient pas à jour étaient contaminés. Le maliciel était le fameux cheval de Troie bancaire GOZI ISFB, dont divers groupes criminels se servent pour lancer des attaques contre des établissements financiers dans le monde entier. Or une semaine plus tard, le 18 septembre 2015, les escrocs ont commencé contre toute attente à supprimer les maliciels des ordinateurs infectés. Une telle démarche peut avoir différentes raisons. Le groupe aura peut-être réalisé que son opération avait été démasquée et tenté ainsi de brouiller les pistes.

Conclusion:

Indépendamment de tous les avantages et des économies qu'une centralisation des contenus Web peut lui offrir, toute entreprise devrait être bien consciente des risques qu'elle encourt. Non seulement les ordinateurs des internautes visitant son site Web risquent une infection par maliciel, mais en cas d'incident l'entreprise piratée s'expose à une grave perte de confiance.

Il faudrait donc absolument définir, en amont déjà, comment procéder au cas où du contenu de tiers serait compromis. L'entreprise a-t-elle accès à ces contenus, et peut-elle les modifier ou les supprimer en cas de nécessité? Il importe surtout d'établir par avance les contacts utiles à la sécurité informatique avec les entreprises tierces. Une telle approche permet de prévenir rapidement les bonnes personnes en cas d'incident et de prendre rapidement les mesures qui s'imposent.

4.3.1.2 Portail TV infecté

Le portail d'une chaîne télévisée a connu semblable mésaventure. Une infection de site Web constatée le 3 décembre 2015 distribuait le kit d'exploits Angler. Là encore, la contamination ne se faisait pas seulement à partir de ce site Web. Le contenu du site manipulé était également diffusé par le biais de partenaires médias, soit d'autres journaux en ligne dont un journal gratuit. D'où un bien plus grand cercle de victimes potentielles. Par chance, une seule sous-page était contaminée. MELANI a informé les exploitants du site Web, pour que le code malveillant soit désactivé.

Les infections de sites Web, dites par drive-by download, font entre-temps partie du répertoire standard des agresseurs, désireux de contaminer un maximum d'appareils. Le kit d'exploits Angler utilisé dans le cas d'espèce avait fait son apparition à fin 2013 et jouit depuis lors d'une popularité croissante. Le mode opératoire des groupes criminels est

presque toujours le même: le kit d'exploits lui-même analyse souvent les appareils-cibles à l'aide de JavaScripts, qui contrôlent les plugiciels installés et leurs versions pour repérer une lacune propice et l'attaquer à l'aide d'un exploit. Lorsque de nouvelles failles de sécurité sont publiées, les kits d'exploits se mettent à jour étonnamment vite. Tous ne comportent pas les mêmes exploits, et les variations peuvent être considérables. Par ailleurs, il est toujours plus fréquent que les kits d'exploits incluent des exploits zero-day.

4.3.2 Défiguration du site LeMatin.ch: Virus IRAQ

Le contenu piraté de tiers diffuseurs a fait les gros titres dans un autre cas encore: le 8 juillet 2015, le site Web du magazine télévisé de lematin.ch a affiché une image d'un groupe de hackers islamique intitulé Virus IRAQ.[16] L'intrusion ne s'était toutefois pas produite sur le propre site du quotidien Le Matin, mais sur celui du prestataire Guide Loisirs, qui fournit des contenus Web à différents clients. En outre, il ne s'agissait pas d'une attaque ciblée, mais d'une vaste opération de défiguration de sites (*defacement*), comme il s'en produit des milliers par jour. Virus IRAQ, le groupe ayant revendiqué ce barbouillage, sévit depuis longtemps. Selon le site Web zone-h.org, qui recense ce type d'attaques, il aurait attaqué de cette manière en 2015 plus de 300 sites Web. Les cibles sont choisies au hasard. Les sites Web défigurés se trouvent notamment en Ukraine, aux Pays-Bas, en Allemagne, en France, en République tchèque et surtout aux Etats-Unis.

Conclusion :

Les sites Web sont constamment passés au crible. Toute vulnérabilité identifiée est exploitée. Des messages à contenu politique ou religieux sont souvent publiés par ce biais. En outre, il existe une véritable escalade dans le domaine de la défiguration de sites, chaque groupe d'activistes cherchant à causer un maximum de dommages.

4.3.3 Usurpation d'adresses IP. Problématique du protocole BGP

Internet comprend des dizaines de milliers de réseaux (appelés *autonomous systems* AS), qui sont reliés entre eux et s'échangent des paquets de données. De tels échanges d'informations utilisent un protocole de passerelle frontière appelé *Border Gateway Protocol (*BGP*)*, qui indique aux routeurs le chemin à emprunter pour atteindre un réseau spécifique. Ce protocole, presque aussi ancien qu'Internet, n'a plus été remanié depuis 1991 (RFC 1269). Il présente hélas depuis lors des faiblesses. Par exemple, des attaques peuvent être menées avec des identités usurpées (attaques par *IP spoofing*). Ainsi, tout AS peut prétendre être propriétaire d'un réseau, même si le réseau indiqué ne lui appartient pas. Et il n'existe aucune possibilité technique de vérifier si une route est légitime ou non. Car les AS partent de l'idée que leurs interlocuteurs ne propagent que des chemins corrects.

Spamhaus, un des principaux fournisseurs mondiaux de listes de blocage, a informé MELANI à deux reprises l'année dernière que les espaces d'adressage d'AS suisses avaient

[16] http://www.tagesanzeiger.ch/digital/internet/Hacker-platzieren-SchockBilder-auf-Website-von-Le-Matin/story/27762519 (état: 29 février 2016).

été usurpés et que des spammer (polluposteurs) s'en servaient pour l'envoi de spam (pourriels). Dans le premier cas, annoncé à MELANI en juin 2015, les escrocs avaient détourné l'espace d'adressage d'un canton. Le second cas, survenu en septembre 2015, concernait des segments de l'espace d'adressage d'une entreprise pharmaceutique. Dans les deux cas, MELANI a informé l'organisation concernée.

Recommandations:

Si vous possédez votre propre espace d'adressage public, nous vous recommandons les mesures suivantes:

- Vérifiez auprès de votre registre Internet régional (par ex. RIPE) la justesse de vos affectations actuelles. Votre espace d'adressage doit en outre posséder une adresse valable destinée au signalement des abus ou fraudes (*abuse mailbox*).
- Si vous possédez un espace d'adressage que vous ne propagez pas, nous vous recommandons de le faire même si vous ne l'employez pas aujourd'hui. Il sera d'autant plus difficile aux spammers (polluposteurs) d'usurper des espaces d'adressage inutilisés.
- Procédez à la surveillance des annonces de vos espaces d'adressage (BGP-monitoring), afin de savoir si un AS étranger propage vos espaces d'adressage. Des entreprises commerciales proposent de tels services, si vous ne voulez ou ne pouvez pas vous en charger vous-mêmes.

Des compléments d'information sur la problématique du protocole BGP et sur l'usurpation d'adresses IP figurent sur le blog GovCERT.ch:

Blog GovCERT.ch:

http://www.govcert.admin.ch/blog/11/cantonal-ip-space-in-switzerland-hijacked-by-spammers

4.3.4 Chantage DDoS: après DD4BC, Armada Collective

Au deuxième semestre 2015, l'extorsion est restée une des méthodes favorites des cybercriminels pour obtenir de rapides gains financiers. Les familles de maliciels de cryptage sont toujours plus nombreuses (voir chap. 4.5.1 du présent rapport semestriel), et des attaques *DDoS* ont à nouveau cherché à rendre des sites Web inaccessibles pour rançonner ensuite les victimes. Alors que le groupe DD4BC sévissait surtout au milieu de l'année 2015, Armada Collective a pris le relais au deuxième semestre. Ces deux groupes avaient le même mode opératoire. Les attaques d'Armada Collective visaient notamment les fournisseurs de messagerie et les hébergeurs. La cyber-attaque lancée en novembre 2015 contre Protonmail, service suisse de messagerie sécurisée, a fait les gros titres de la presse internationale.

Les attaques DDoS sont un fléau connu depuis longtemps. Les attaques motivées par des considérations purement financières se sont multipliées en 2015. Les criminels ont essentiellement choisi des entreprises qui dépendent de l'accès à leur site Internet, et donc

qui peuvent être plus facilement soumises au chantage. Sous la menace d'une éventuelle perturbation de l'accès à leur site Internet et dans l'espoir d'obtenir une solution rapide, certaines entreprises sont prêtes à mettre la main au portemonnaie. Or en payant, elles donnent aux malfaiteurs les moyens financiers nécessaires pour renforcer leur infrastructure d'attaque et intensifier leurs actions. En outre, il n'existe aucune garantie que le paiement de la rançon permettra de stopper l'attaque. Les assaillants utilisent souvent ce que l'on appelle des services «Booter» ou «Stresser». Il s'agit là d'un service illégale permettant de conduire une attaque DDoS en échange de paiement (on pourrait parler d'un «DDoS as a service»). Plus un attaquant a d'argent à sa disposition, plus le service qu'il peut acquérir auprès d'un tel prestataire est considérable et donc plus l'ampleur de l'attaque – tant au niveau de l'intensité que de la durée – sera importante. Si par contre la rançon n'est pas payée, la tactique du criminel s'effondre. Céder à l'extorsion permet donc au mieux, et sans garantie, de faire disparaître momentanément les symptômes et ne renforce durablement ni l'infrastructure de la victime, ni la sécurité d'Internet contre les attaques DDoS.

Recommandations:

Lorsqu'une attaque DDoS prend une entreprise au dépourvu, il est généralement trop tard pour y réagir de manière rapide et efficace. Ces mesures sont d'autant plus importantes pour des entreprises dont la présence sur Internet est le principale canal de vente. Dans ces cas, la protection de la plateforme de vente devrait jouir d'une priorité absolue en tant que processus essentiel au bon fonctionnement de l'entreprise. D'où l'importance d'élaborer en amont une stratégie spécifique. Les services tant internes qu'externes compétents, ainsi que les autres personnes habilitées à agir en cas d'attaque doivent être connus. Dans l'idéal, une entreprise devrait prendre des mesures de prévention avant même d'avoir subi une attaque DDoS. Ces mesures s'inscriront dans la gestion générale des risques au niveau de la direction. Un certain niveau de préparation aux attaques DDoS s'impose encore sur le plan de l'exploitation. Toute organisation peut être la cible d'une attaque DDoS. Nous vous conseillons donc de parler avec votre fournisseur d'accès à Internet de vos besoins et des mesures préventives proposées. Le site MELANI propose une liste de contrôle, avec des instructions sur les mesures à prendre contre les attaques DDoS, à l'adresse suivante:

Mesures à prendre contre les attaques DDoS:

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/massnahmen-gegen-ddos-attacken.html

4.3.4.1 Attaque contre Protonmail

L'attaque DDoS lancée contre Protonmail revêt un caractère exceptionnel, tant par la publicité qui lui a été donnée que par son déroulement. Ce service de messagerie développé

par des chercheurs du CERN propose un *cryptage de bout en bout (end-to-end)*. L'entreprise a vu le jour en 2013, suite aux révélations d'Edward Snowden. Basée à Genève, elle a recours au financement participatif[17].

Dans la nuit du 3 novembre 2015 Protonmail a enregistré une attaque DDoS sur ses systèmes. Les soupçons se sont alors portés sur Armada Collective. Puis selon Protonmail, des agressions quotidiennes ont suivi. Ce n'est guère typique du mode opératoire d'Armada Collective, qui se contente d'habitude d'une démonstration de force, en espérant que la victime intimidée délie d'emblée les cordons de sa bourse. Les premiers jours, Protonmail a néanmoins cru à un agresseur unique. Ces cyberattaques avaient aussi des effets collatéraux sur d'autres clients du centre de calcul. D'entente avec ces entreprises, il a donc été décidé de payer la rançon. Puis comme les attaques persistaient et même Armada Collective s'était distancié de l'agression, Protonmail en a conclu qu'un second agresseur en était l'auteur[18].

Protonmail a d'emblée communiqué très ouvertement sur les incidents, soupçonnant un Etat d'être à l'origine de ces attaques[19]. La thèse n'a jamais pu être étayée. Par contre, un autre effet paraît vraisemblable. La politique de communication sur les attaques DDoS pourrait avoir mis la puce à l'oreille d'un second cybercriminel, qui aura saisi l'occasion pour sévir en parallèle à Armada Collective.

4.3.4.2 Arrestation chez DD4BC

Beaucoup de tentatives de chantage DDoS observées en 2015 émanent du groupe DD4BC (DDoS for BitCoin). Les 15 et 16 décembre, le High-Tech Crime Department de la République serbe de Bosnie (une des deux entités formant la Bosnie-Herzégovine) a lancé une opération intitulée Pléiades contre le groupe DD4BC. L'opération bénéficiait du soutien de fonctionnaires de police de divers Etats européens et d'Europol. L'Autriche était à l'origine de cette action, soutenue par le Centre européen de lutte contre la cybercriminalité (European Cybercrime Centre, EC3). La Suisse appuyait aussi l'opération, qui a conduit à l'arrestation du cerveau présumé de la bande et d'un comparse. Un ressortissant bosniaque de 32 ans est soupçonné d'avoir joué un rôle de premier plan au sein de DD4BC.

4.3.5 Menace d'Anonymous à Lausanne

Le groupement informel Anonymous a acquis une notoriété internationale sur de grandes questions comme la défense des activités de Julian Assange, fondateur de WikiLeaks, ou dans l'actuel conflit avec les sympathisants de l'Etat islamique sur Internet (voir aussi chap. 5.4.2 du présent rapport semestriel). Un exemple romand qui a fait les gros titres en juillet 2015 montre toutefois qu'Anonymous ne s'occupe pas que d'enjeux internationaux. Un groupe autoproclamé Anonymous Suisse a menacé la Municipalité de Lausanne de lancer une cyberattaque contre ses systèmes informatiques, si elle ne respectait pas les locataires

---

17 https://fr.wikipedia.org/wiki/ProtonMail (état: 29 février 2016).

18 https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/ (état: 29 février 2016).

19 https://twitter.com/ProtonMail/status/661683054866429798 4 (état: 29 février 2016).

de la tour de la Sallaz. La menace faisait suite aux vibrations d'un chantier, dont les résidents de la tour avaient souffert. Une plainte a été déposée contre cette menace. En outre, des précautions ont été prises pour dûment protéger le service informatique de la ville contre d'éventuelles attaques.

Conclusions:

Il est difficile de dire si le mouvement Anonymous a quelque chose à voir avec cette menace, ou si un individu s'est servi de son nom dans l'espoir d'obtenir une visibilité accrue, sachant qu'Anonymous n'est pas un groupe bien défini. Les liens informels en son sein se traduisent par une absence de coordination au niveau tant de la communication que des cyberattaques plus ou moins spectaculaires effectuées. Comme la structure d'Anonymous ne prévoit ni affiliation ni porte-parole officiel, et que personne ne porte la responsabilité d'ensemble de ce mouvement, chacun peut en principe publier des communiqués au nom d'Anonymous pour susciter l'intérêt des médias.

4.4 Social Engineering, phishing

Outre les attaques techniques en tous genres, les attaquants cherchent aussi à exploiter les faiblesses humaines.

4.4.1 Statistiques de phishing

Ces dernières années, le nombre de demandes liées au *phishing* a fortement augmenté. Soucieuse de traiter plus efficacement les annonces entrantes, la centrale MELANI a mis en place le site «antiphishing.ch» en 2015, où chacun peut signaler des sites de phishing. Au total, 2500 sites de phishing ont été dénoncés la première année, les annonces fluctuant beaucoup au fil du temps. Les raisons en sont diverses: d'une part, les pages signalées sont moins nombreuses en période de vacances (et les escrocs prennent eux aussi des vacances), d'autre part, les agresseurs passent régulièrement d'un pays à l'autre.

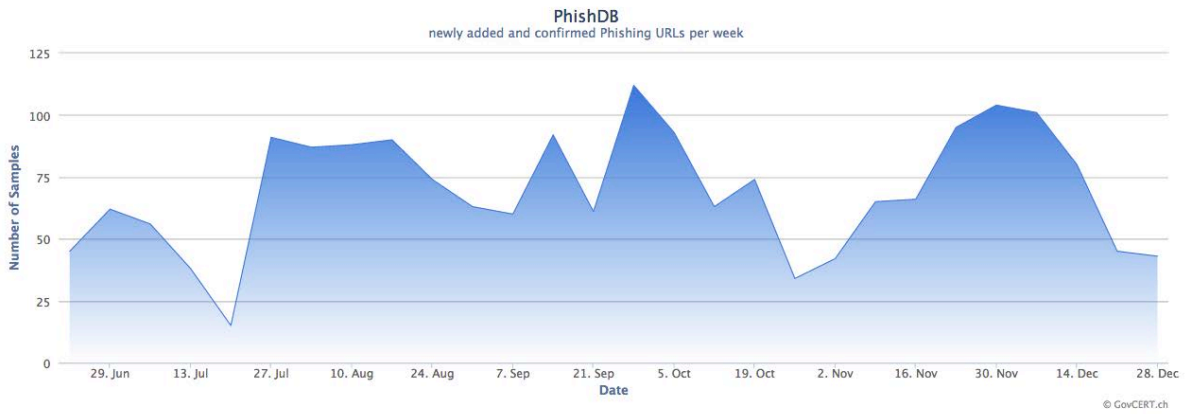

Fig. 2: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch

4.4.2 Usage abusif du logo de l'administration fédérale (1re partie)

Le logo de l'administration fédérale suisse est très prisé des escrocs. Il a été usurpé à deux reprises dans des tentatives de phishing, et une fois pour la diffusion de maliciels (voir chapitre 4.5.2 du présent rapport semestriel). Les attaques n'étaient toutefois pas dirigées contre l'administration fédérale. L'usage abusif du logo avait pour seul but d'inspirer confiance aux victimes.

Au deuxième semestre 2015, des escrocs ont tenté à plusieurs reprises de soutirer par courriel les données de cartes de crédit d'internautes, en se faisant passer pour l'Office fédéral de l'énergie (OFEN). Le même stratagème avait déjà été observé en 2014. Les destinataires étaient appâtés par une promesse de remboursement. Ils étaient priés de se rendre sur le site indiqué pour que le paiement puisse avoir lieu. Le site, ressemblant à l'original à s'y méprendre, réclamait non seulement les nom et adresse de la victime, mais aussi un numéro de carte de crédit, sa date d'expiration et son chiffre de contrôle.

Le nom de l'administration fédérale des contributions (AFC) a été usurpé dans un autre cas remontant à fin septembre 2015. Des escrocs ont cherché à se procurer par courriel les coordonnées bancaires ou postales de contribuables, des informations sur leurs cartes de crédit ainsi que des copies de leurs documents d'identité. Le message frauduleux était censé émaner de l'AFC.[20]

4.4.3 Phishing par le biais de la publicité

Depuis avril 2015, MELANI a observé un nouveau mode opératoire pour les attaques de phishing visant des établissements financiers suisses. Les escrocs n'envoient plus de courriels de phishing, mais publient des annonces publicitaires payantes auprès d'exploitants de moteurs de recherche comme Google, Yahoo ou Bing. A cet effet, ils acquièrent auprès des exploitants de moteurs de recherche les mots-clés (keyword) de l'établissement financier attaqué: si par exemple les criminels prennent pour cibles les clients de la «banque XY», ils publieront ces annonces de phishing sous les mots-clés «XY» ou «banque XY».

Les annonces publicitaires s'affichent habituellement en premier et de manière bien visible, avant les résultats de recherche proprement dits. Il y a donc de fortes chances qu'un internaute désirant accéder au site de la «banque XY» clique non pas sur le résultat effectif de sa recherche, mais sur l'annonce publicitaire frauduleuse.

[20] https://www.estv.admin.ch/estv/de/home/allgemein/aktuell/warnung--phishing.html (état: 29 février 2016).

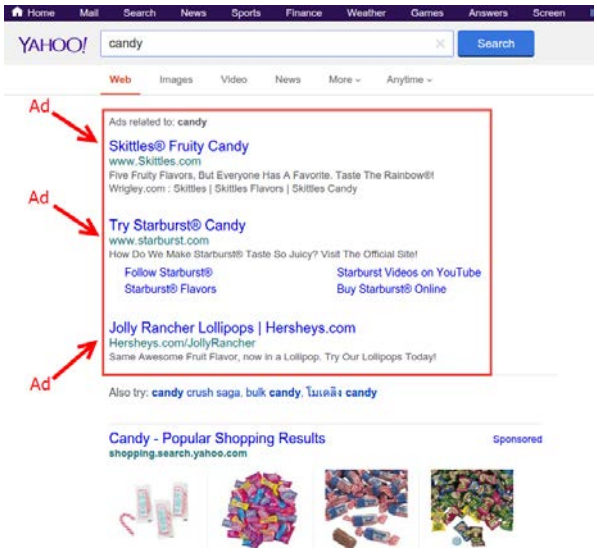

Fig. 3: Exemple d'annonce publicitaire sur Yahoo.

Forts de ce constat, les escrocs cherchent à attirer des internautes naïfs sur leurs pages de phishing. Les attaques par le biais d'annonces publicitaires publiées sur des moteurs de recherche connus ont d'autres avantages encore pour les agresseurs:

- Il est difficile aux entreprises de sécurité informatique et aux CERT de reconnaître comme telles les annonces de phishing sur les moteurs de recherche.
- Les agresseurs n'ont pas à s'inquiéter des filtres anti-pourriel ou des listes d'expéditeurs fiables, puisqu'aucun courriel n'est envoyé.
- Comme certains exploitants de moteurs de recherche ne contrôlent pas, ou du moins pas suffisamment leurs nouveaux clients, les agresseurs peuvent en tout temps créer un nouveau compte d'utilisateur sur leurs plateformes publicitaires pour y diffuser de fausses annonces.

MELANI a pris contact avec les trois grands exploitants de moteurs de recherche de Suisse, afin d'étudier le problème. Deux d'entre eux étaient concernés par les attaques de phishing précitées.

Recommandations:

Des compléments d'information relatifs au phishing basé sur les annonces publicitaires figurent sur le blog GovCERT.ch:

INFO

Blog GovCERT.ch:

http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

4.4.4 Phishing basé sur des fichiers PDF

Au deuxième semestre 2015, MELANI a observé le recours croissant à un autre mode opératoire, soit le phishing avec l'aide de fichiers PDF. Les habituels courriels de phishing sont envoyés. Mais au lieu d'un lien HTML aboutissant à la page infectée, ils contiennent une annexe à l'extension .pdf. Le fichier PDF renferme des instructions visant à inciter la victime à cliquer sur le lien qui la conduira à la page de phishing.

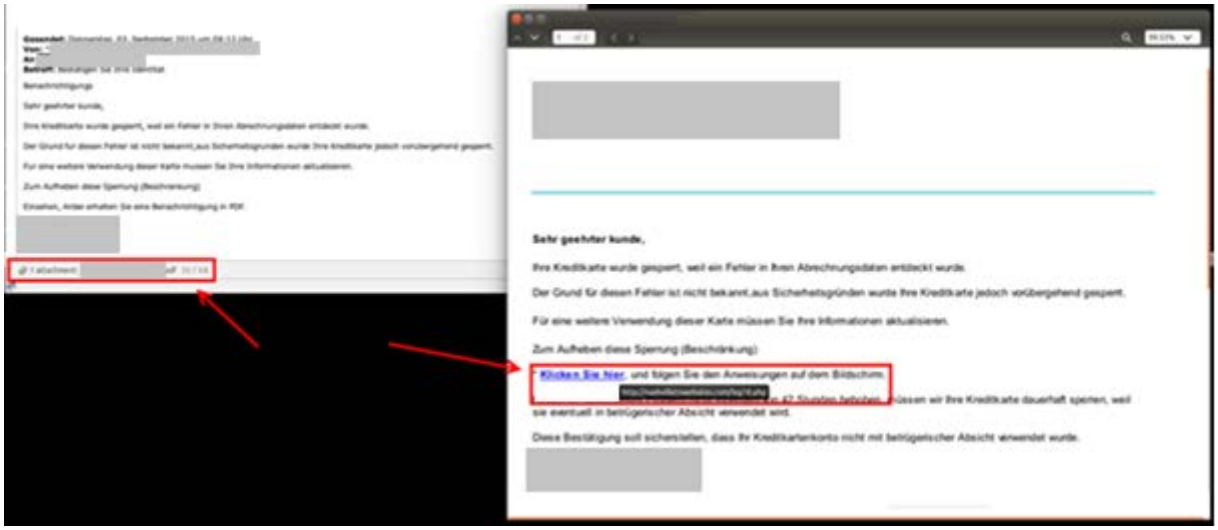

Fig. 4: Exemple de courriels avec lien de phishing figurant dans une annexe au format .pdf.

Conclusions:

Alors qu'il n'y a guère de différence, pour le destinataire d'un courriel de phishing, si la page créée par les escrocs figure directement dans le courriel ou si elle est dissimulée dans un fichier annexé, cette nouvelle pratique offre un grand avantage aux agresseurs: l'usage de fichiers PDF déjoue la vigilance des filtres de messagerie, qui ne recherchent généralement du contenu dangereux que dans les courriels eux-mêmes. Les cybercriminels semblent l'avoir compris et privilégient désormais cette astuce.

4.5 Logiciels criminels (crimeware)

L'expression *crimeware* désigne tout logiciel malveillant spécialement conçu par des fraudeurs pour automatiser la cybercriminalité économique. Comme l'indique la statistique ci-dessous, les chevaux de Troie bancaires restent très répandus. En Suisse, une grande partie des annonces de systèmes infectés faites à MELANI sont dues à des chevaux de Troie comme Torpig, Dyre, Tinba, Gozi ou ZeuS. Alors que Tinba avait surtout sévi au semestre précédent, le cheval de Troie bancaire Gozi remporte la palme sur toute l'année. Cette progression s'explique notamment par la méthode de diffusion via les réseaux publicitaires infectés décrite au chap. 4.3.1. Mais comme au premier semestre 2015, la plupart des infections restent dues à Downadup (aussi appelé Conficker). Ce ver apparu il y a plus de huit ans se répand par une faille de sécurité des systèmes d'exploitation Windows, découverte en 2008 et déjà comblée à l'époque.

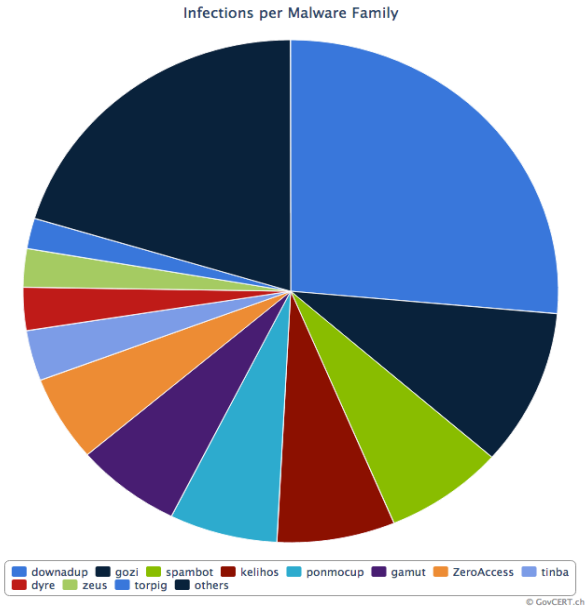

Fig. 5: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. La date de référence est le 31 décembre 2015. Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

Comme au premier semestre 2015, Zurich et le Valais continuent d'afficher au deuxième semestre un taux d'infection supérieur aux autres cantons (compte tenu du nombre d'habitants). Alors qu'à Zurich ce résultat tient à la forte densité d'ordinateurs, les raisons du taux d'infection élevé en Valais ne sont pas connues à l'heure actuelle.

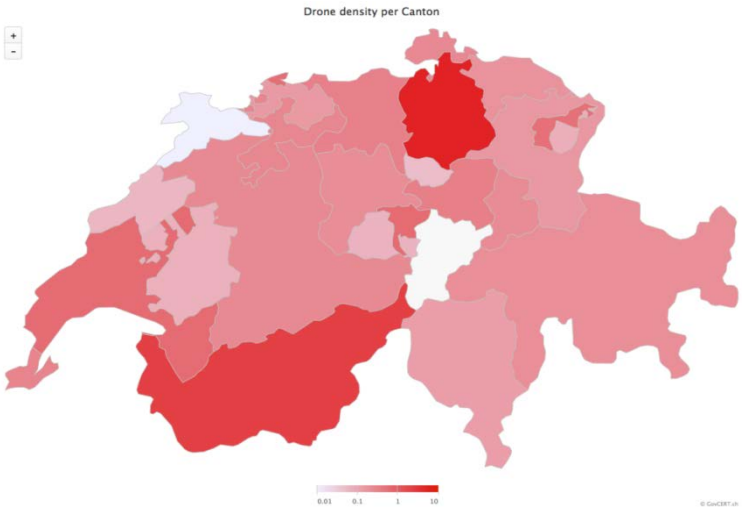

Fig. 6: Nombre d'infections par canton, au prorata de la population. La date de référence est le 31 décembre 2015. Les données actuelles sont publiées à l'adresse: http://www.govcert.admin.ch/statistics/dronemap/

4.5.1 Chevaux de Troie chiffrant les données – toujours aussi répandus

Au deuxième semestre 2015 aussi, divers cas de chevaux de Troie cryptant les données ont été annoncés. Il s'agissait le plus souvent du ransomware ou *rançongiciel* Teslacrypt, encore

que des cas impliquant d'autres familles de chevaux de Troie comme Cryptowall aient été signalés à MELANI. Les victimes sont aussi bien des particuliers que des entreprises de toute taille, actives dans toutes les branches. Si aucune sauvegarde n'a été faite auparavant ou en cas de sauvegarde désuète, les données risquent d'être irrémédiablement perdues.

Recommandations :

Les données figurant sur l'ordinateur devraient être copiées régulièrement sur des supports externes (backup). Ces derniers seront connectés à l'ordinateur uniquement lors de la sauvegarde des données, et conservés en lieu sûr.

INFO

Mesures préventives contre les ransomwares (rançongiciels):

https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html

4.5.2 Usage abusif du logo de l'administration fédérale (2e partie)

Selon le service de coordination de la lutte contre la criminalité sur Internet (SCOCI) de l'Office fédéral de la police (fedpol), au début de juillet 2015, des courriels prétendument expédiés par fedpol invitaient leurs destinataires à télécharger sur un site Web des documents d'une audience de jugement fictive. Une autre vague d'escroqueries a été observée en janvier 2016. Le texte visait à intimider et mettre sous pression le destinataire: si la personne ne livrait pas les données demandées dans les quinze jours, une audience de jugement aurait lieu en son absence. Le lien aboutissait à une page Internet imitant le site de fedpol. La victime devait inscrire un code de sécurité (*captcha*) et télécharger des fichiers. Or quiconque se conformait aux instructions du site ou du courriel installait à son insu le ransomware Cryptolocker.

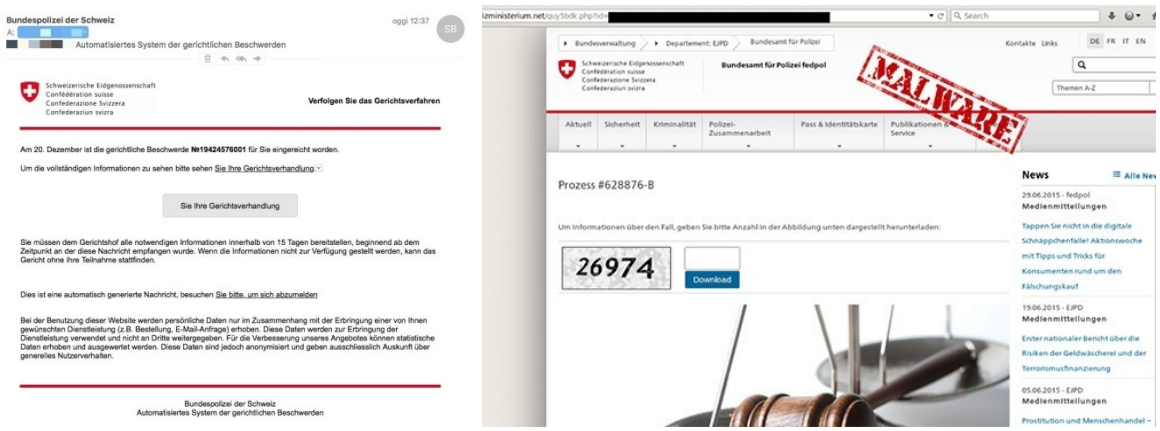

Fig. 7: Contrefaçon du site de l'Office fédéral de la police utilisée pour diffuser le cheval de Troie Cryptolocker. Source :SCOCI/ fedpol

Au début de février 2016, une autre variante frauduleuse usurpant le logo de l'Office fédéral de la police bloquait l'écran et le navigateur de l'internaute imprudent. Il lui était reproché d'avoir commis des activités illégales sur Internet. Il avait la possibilité de déverrouiller le navigateur et d'éviter des poursuites pénales, moyennant le versement d'une amende, à

régler par carte prépayée PaySafeCard. De tels cas sont régulièrement apparus ces dernières années. A la différence du cheval de Troie cryptant les données, cette variante d'escroquerie n'est pas très sophistiquée. Selon le système d'exploitation et le navigateur, la victime peut refermer la fenêtre bloquée de son navigateur et empêcher la réouverture automatique de la dernière page visitée (pour éviter au même incident de se reproduire). Il convient à cet effet de consulter les instructions du logiciel concerné. Dans le cas de Windows, la fermeture s'effectue au moyen du gestionnaire de tâches (Ctrl-Alt-Del).

Les utilisateurs d'ordinateurs ne sont pas les seuls à être touchés par ce type d'attaques. En effet, les utilisateurs de navigateurs conçus pour smartphones et tablettes sont de plus en plus visés eux aussi par des codes exécutables.

Fig. 8: Fausse page de blocage au logo de l'Office fédéral de la police. Source :SCOCI/ fedpol

4.5.3 Chevaux de Troie bancaires: Retefe et Tinba

MELANI a décidé à la fin de novembre 2015, d'entente avec ses partenaires et les établissements financiers concernés, de désactiver l'*infrastructure de commande et de contrôle (C&C)* utilisée par le cheval de Troie bancaire Retefe. La centrale MELANI est intervenue à cet effet auprès des hébergeurs et des registraires accrédités l'étranger, pour les prier de bloquer les serveurs et les noms de domaine utilisés par Retefe. L'opération de retrait (*takedown*) a porté sur plus de 30 serveurs et noms de domaine en Europe. Au cours des semaines suivantes, MELANI a constaté l'absence de toute nouvelle infection ou vague de pourriels liée à Retefe. La désactivation du *réseau de zombies* s'est donc avérée un succès jusqu'à l'apparition, à fin décembre 2015, de nouvelles vagues de pourriels identiques à celles observées les mois précédents avec Retefe. L'analyse des annexes a toutefois livré des résultats étonnants. Le maliciel utilisé n'était plus Retefe, mais un autre cheval de Troie bien plus connu, Tinba (aussi appelé «Tiny Banker»). Le collectif utilisant Retefe avait donc visiblement changé d'arme et opté en décembre 2015 pour Tinba, et donc pour une nouvelle infrastructure C&C.

Le chevaux de Troie Retefe et Tinba comportent des différences majeures: alors que Retefe était manifestement un produit propre des agresseurs, réservé aux fraudes à l'e-banking en Suisse, en Autriche, en Suède et ponctuellement au Japon, Tinba est un kit servant à créer des logiciels criminels (*crimeware kit*), mis en vente dans des forums clandestins. Une autre différence tient au mode de fonctionnement de ces deux chevaux de Troie: alors que Retefe modifie les paramètres DNS ou les réglages de proxy de l'ordinateur infecté, Tinba s'incruste

dans le système et communique régulièrement avec une infrastructure C&C centrale. D'où la possibilité pour ses propriétaires d'accéder en tout temps à l'ordinateur de la victime à des fins de fraude à l'e-banking.

4.5.4 Réseaux de zombies: Dridex / Bugat

En octobre 2015, la justice américaine a frappé fort, avec le FBI, contre le réseau de zombies Bugat. Mieux connu sous le nom de Dridex, Bugat est un cheval de Troie bancaire s'en prenant à la clientèle de dizaines d'établissements financiers, dans le monde entier. La justice américaine a inculpé un Moldave de 30 ans pour administration du réseau. Or malgré les tentatives du FBI de démanteler le réseau et d'arrêter les personnes impliquées, Bugat est encore en activité, cherchant tous les jours à infecter les appareils d'internautes crédules aux Etats-Unis et en Europe, lors de campagnes de spam (pollupostage).

Recommandations:

MELANI recommande aux internautes de ne jamais ouvrir les annexes suspectes de messages, même quand elles semblent provenir d'expéditeurs dignes de confiance. En outre, il faut s'assurer d'avoir installé un antivirus et le maintenir constamment à jour.

INFO

Règles de comportement courrier électronique:

https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.html

4.5.5 Razzia contre les acheteurs de Droidjack

Les outils d'administration à distance (*remote access tool ou remote admnistration tool*, RAT) pour Android remportent un succès croissant sur le marché souterrain des services cybercriminels. En effet, les RAT permettent de surveiller un smartphone[21], par exemple de contrôler les échanges de données, d'épier les conversations et les bruits environnants, de se connecter à la caméra, voire de repérer l'emplacement exact de l'appareil. A la fin d'octobre, une razzia a été lancée en Allemagne, à l'initiative des autorités de poursuite pénale, contre les vendeurs du RAT Droidjack. Des perquisitions ont été menées en parallèle au Royaume-Uni, aux Etats-Unis, en France, en Allemagne, en Belgique et en Suisse. Les acquéreurs de ce logiciel sont accusés d'espionnage illégal des données et de fraude informatique. L'outil était vendu en ligne au prix de 210 dollars. Ces indices visent à remonter la filière pour démasquer l'auteur de l'application, qui n'était pas au centre de la razzia. Cependant les indices pointent vers l'Inde. Autres thèmes

4.5.6 Gestion de noms de domaine: un processus d'importance vitale

Les noms de domaine ne désignent pas que l'adresse à laquelle une page Web est publiée. Dans les entreprises, ils constituent généralement la partie de l'adresse des collaborateurs

[21] http://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime (état: 29 février 2016).

située après l'arobase, et peuvent par exemple faire partie de l'infrastructure permettant aux employés d'accéder à distance aux réseaux internes. Les noms de domaine constituent des ressources d'adressage dans le trafic de télécommunication, ils offrent une pluralité d'applications et sont en dernier lieu une marque de l'entreprise. Au vu des différentes fonctions que remplissent les noms de domaine, dans les entreprises notamment, leur gestion peut être un processus d'importance vitale: si par exemple le site Web et les courriels sont cruciaux pour l'activité professionnelle déployée, ou si la configuration de l'infrastructure informatique ne peut être transférée vers d'autres noms de domaine qu'au prix d'efforts considérables.

Les noms de domaine ne peuvent toutefois pas être «achetés» – il faut les enregistrer. Ce faisant, on obtient un droit d'utilisation limité dans le temps de la ressource d'adressage correspondant, en tant que titulaire. Ce droit doit être régulièrement renouvelé. En cas d'oubli, le site Web cessera brusquement d'être accessible et les courriels ne seront plus acheminés – pour ne mentionner que les conséquences techniques visibles.

Le processus d'attribution des noms de domaine suisses a été modifié en 2015.[22] Depuis lors, le registre n'offre plus directement l'enregistrement d'un nom de domaine de premier niveau *(top level domain, TLD)* «.ch» à des clients finaux (titulaires ou registrants de nom de domaine). En outre, il a été décidé qu'après un délai transitoire, le registre abandonnerait toutes ses relations contractuelles avec les clients finaux. Il doit entre-temps se contenter de la gestion technique du domaine .ch, l'attribution des noms de domaine et l'administration des clients finaux étant désormais du ressort exclusif des registraires, par souci d'une scission complète avec le marché des domaines. Par conséquent, les registrants qui se procuraient jusque-là leurs noms de domaine directement auprès du registre SWITCH ont dû se chercher un registraire qui administre pour eux l'enregistrement des domaines. A cet effet, ils ont dû bien réfléchir à leurs besoins, puis choisir une offre adéquate.

Plusieurs registrants se sont plaints auprès de MELANI, à la fin de 2015, parce que leur nouveau registraire ne les avait pas informés à temps et sous une forme adéquate de l'expiration imminente du contrat portant sur l'enregistrement de leurs noms de domaine. Ces derniers ont ensuite été désactivés – avec les conséquences susmentionnées pour la marche des affaires. Comme par chance les noms de domaine périmés .ch ne sont pas aussitôt remis sur le marché pour un nouvel enregistrement, les (anciens) registrants ont pu les récupérer avec l'aide de leur registraire, moyennant un certain effort administratif.

---

[22] Séparation des tâches dans la gestion des adresses Internet .ch: http://www.bakom.admin.ch/themen/internet/00468/04167/04981/index.html?lang=fr (état: 29 février 2016).

Recommandations:

Toute entreprise doit savoir combien de noms de domaine elle a enregistrés et lesquels, dans quels buts elle les utilise et quand il lui faudra renouveler les enregistrements correspondants. Discutez avec votre registraire de vos besoins et de ses offres. Définissez des processus et des mécanismes de protection de vos noms de domaine contre toute modification involontaire ou malveillante, qu'elle soit de nature administrative ou technique.

Sécurité informatique: aide-mémoire pour les PME :

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

5 Situation internationale

5.1 Espionnage

5.1.1 Piratage de Hacking Team

Hacking Team, fabricant italien de logiciels de surveillance, s'est fait dérober une grande quantité de données. Le 5 juillet 2015, plus de 400 gigabytes de données volées ont été publiées. La société Hacking Team produit des logiciels de surveillance pour les autorités judiciaires, les services de renseignement et les entreprises privées. La police cantonale zurichoise compte parmi ses clients.[23] Outre Windows, MacOS et Linux, leurs produits permettent d'infiltrer tous les systèmes d'exploitation de smartphones. Les logiciels de surveillance développés par Hacking Team donnent accès aux smartphones comme aux ordinateurs et offrent par exemple la possibilité de lire les SMS ou d'espionner les conversations téléphoniques ou sur Skype.

La confidentialité est primordiale dans les activités de surveillance. En plus de ruiner la réputation de l'entreprise piratée, l'attaque a eu de fâcheuses conséquences pour ses clients. Les données publiées contenaient par ex. des courriels, des listes de clients et d'autres documents confidentiels. Selon toute probabilité, les journalistes et les prestataires de sécurité ne sont pas seuls à avoir épluché ces informations, des groupes avides de profit auront aussi cherché à profiter des vulnérabilités et des portes dérobées révélées au grand jour. Dans le meilleur des cas, les programmes mis en place et payés par les clients sont rapidement devenus obsolètes, tandis que dans le pire des cas, des tiers non autorisés s'en sont servis à leur tour. L'entreprise a donc mis en garde contre le risque d'utilisation abusive de ses logiciels par des cybercriminels ou des terroristes.[24] Divers fournisseurs de logiciels se sont donc empressés de combler les lacunes utilisées à leur insu. La police cantonale zurichoise, qui avait acquis de la société Hacking Team le logiciel de surveillance Galileo pour près d'un demi-million de francs, a notamment déclaré qu'elle renonçait à utiliser ce produit. L'incident montre très clairement à quel point la gestion des failles de sécurité et des portes dérobées s'avère délicate et périlleuse (voir chap. 3 et 5.1.2 Juniper).

La liste des pays de provenance de la clientèle est longue[25] et comprend, à côté de la Suisse, des Etats-Unis ou de l'Allemagne, d'autres Etats comme le Soudan, où l'ONU a pourtant décrété un embargo sur les armes. L'incident devrait raviver les discussions visant à savoir dans quelle mesure les programmes informatiques doivent être assimilés à des armes, dont les exportations sont soumises à des restrictions.

Au niveau politique également, la publication des données internes de la société Hacking Team a provoqué des turbulences: Andreas Pentaras, chef du service de renseignement

---

23 http://www.heise.de/newsticker/meldung/Hacking-Team-Kantonspolizei-kaufte-Ueberwachungssoftware-trotz-Bedenken-des-Bundesgerichts-2911887.html (état: 29 février 2016).

24 http://www.heise.de/newsticker/meldung/Hacking-Team-Terroristen-koennten-geleakte-Schnueffeltechnik-nutzen-2746071.html (état: 29 février 2016).

25 http://www.watson.ch/Digital/Best%20of%20watson/477908232-Die-uns%C3%A4glich-peinliche-Geschichte-der-gehackten-Hacker-(und-Kapo-ZH-Lieferanten)-in-25-Tweets-erz%C3%A4hlt (état: 29 février 2016).

chypriote, a démissionné suite au tollé provoqué par l'achat du logiciel de Hacking Team. En effet, la surveillance des communications est prohibée à Chypre. Le Parlement chypriote avait certes révisé la Constitution il y a cinq ans, autorisant la surveillance à certaines conditions. Mais les bases légales n'ont pas encore été mises en place.[26] Tout en affirmant avoir respecté toutes les prescriptions, Andreas Pentaras a démissionné pour éviter que le service de renseignement chypriote ne soit remis en cause.

En Suisse Mario Fehr, directeur cantonal de la police zurichoise, a subi de vives critiques. Il avait approuvé la commande du logiciel de la société Hacking Team. L'achat exclusivement destiné aux poursuites pénales avait certes été réalisé selon la procédure normale, par décision du directeur de la sécurité.[27] Par contre, l'usage des mesures techniques de surveillance doit être ordonné par le tribunal des mesures de contrainte, dont dépendent les autorisations de surveillance. Les Jeunes socialistes du canton de Zurich ont déposé plainte contre Mario Fehr. A leurs yeux, l'achat était contraire au droit constitutionnel à la protection de la liberté personnelle et de la sphère privée. Mais le parquet zurichois n'a pas ouvert de procédure.

5.1.2 Espionnage avec Juniper, Synful Knock et certificats exportables

Le fournisseur d'équipements de réseau Juniper a découvert dans son système d'exploitation ScreenOS, lors d'un réexamen interne de ses logiciels, des «lignes de programme non autorisées». Juniper, qui a son siège aux Etats-Unis, est après Cisco le plus grand fournisseur de solutions réseau au monde, produisant des routeurs haut de gamme qui s'emploient au niveau des réseaux fédérateurs à haut débit d'Internet, appelés *backbones*. Avant Noël 2015, deux failles de sécurité ont été publiées, avec les mises à jour correspondantes. Ces versions ont beau ne pas être très répandues, elles servent à la communication confidentielle et sûre des entreprises.

L'une des vulnérabilités, l'existence d'un mot de passe principal dans le code du programme, serait apparue dans le système d'exploitation en 2013. Alors qu'avant la divulgation de la faille les agresseurs devaient être rares à posséder ce passe-partout, la publication a permis de localiser aisément le mot de passe problématique. Il a suffi de quelques heures pour qu'il soit publié dans Internet, et des attaques ciblées ne se sont guère fait attendre.

La deuxième lacune est plus complexe. Il s'agit concrètement d'une porte dérobée des communications cryptées, qui permet à un agresseur d'épier les liaisons VPN. D'où la possibilité de décrypter a posteriori même les données réseau dûment enregistrées. La faille se base sur le générateur de nombres aléatoires EC_DRBG, dont on sait depuis les révélations d'Edward Snowden qu'il ne livre pas des variables aussi aléatoires qu'il devrait. Or en lieu et place d'un changement complet, Juniper s'est contenté de remplacer les

---

[26] https://intelnews.org/tag/cyprus-intelligence-service/ (état: 29 février 2016).

[27] http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html (état: 29 février 2016).

verrous critiqués et non le générateur EC_DRBG. Par la suite, un agresseur inconnu a remodifié les verrous à nouveau à son profit.

Conclusion:

La seconde lacune de sécurité surtout laisse penser à un acteur étatique. De telles vulnérabilités montrent à quel point les principaux composants informatiques suscitent la convoitise. Cet exemple souligne encore un autre aspect, à savoir le risque lié à la mise en place délibérée de portes dérobées et de vulnérabilités. Car des tiers peuvent découvrir n'importe quand ces portes dérobées, et les exploiter à leur profit.

Cisco, n° 1 mondial des équipements de réseau, aurait également subi une attaque de son matériel réseau, selon la société FireEye.[28] Lors de l'incident SYNful Knock, au moins quatorze routeurs basés en Ukraine, aux Philippines, au Mexique et en Inde ont été compromis et pourvus de portes dérobées. Le nombre d'appareils infectés est très vraisemblablement nettement plus élevé.[29] A la différence de l'incident survenu à Juniper, aucune faille de sécurité n'a été exploitée pour accéder aux systèmes. L'accès s'est fait normalement, par un mot de passe d'administrateur. Puis des microprogrammes (*firmware*) ont été partiellement récrits avec des maliciels. Les attaquants ont obtenu des mots de passe par différents biais. Dans certains cas, ils se sont contentés d'utiliser des mots de passe standard, ce qui montre une fois de plus l'absence fréquente de vraie réflexion sécuritaire.

Selon une information parue le 23 novembre 2015, Dell installait son propre *certificat d'autorité de certification racine (Root CA)* dans la liste de certificats Windows. Ce certificat racine de confiance permet à n'importe qui d'émettre des certificats valables pour les appareils Dell. Or même s'il est marqué comme non exportable, le certificat pouvait tout de même être exporté sans peine. D'où la possibilité d'intercepter facilement, lors d'attaques du type *Man-in-the-Middle*, les liaisons cryptées utilisant l'interface de programmation d'application cryptographique (*crypto-API*) de Dell. Outre que presque tous les programmes Windows sont vulnérables, il est aisé d'installer par ce biais un maliciel sur un ordinateur Dell. Une signature non valable empêche normalement l'installation des logiciels non approuvés, ou du moins l'utilisateur est prié de confirmer s'il souhaite réellement installer un tel logiciel. Ce mécanisme de sécurité disparaît si l'agresseur est en possession d'un certificat d'autorité de certification racine, qui lui permet de munir d'une signature valable n'importe quel logiciel (malveillant). Dell a réagi par une mise à jour écartant ce certificat problématique.

[28] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html (état: 29 février 2016).

[29] http://www.theregister.co.uk/2015/09/22/synful_knock_spreads_embaddened_boxen_in_31_countries/ (état: 29 février 2016).

Conclusion:

Les exemples ci-dessus démontrent deux éléments fondamentaux: Premièrement, les Etat continueront à essayer d'intercepter les communications à des fins de renseignements. Deuxièmement, il existe deux approches principales pour s'y prendre. D'un côté, les Etats peuvent s'assurer de leur emprise sur des nœuds et canaux de communications importants au niveau mondial. De l'autre, ils interceptent les informations en ciblant leurs opérations sur un des deux pôles de la communication (tels que l'ordinateur d'un suspect). En dehors des problèmes juridiques et politiques liés à la première approche (RS 2013 I et II), le recours au chiffrement des communications diminue l'utilité des données interceptées. Le seul moyen de sauver la première approche serait d'interdire ou de diminuer l'efficacité les systèmes de chiffrement ou de leurs composantes. La deuxième approche, ciblée sur le point d'entrée ou de sortie du chiffrement, nécessite de nombreuses ressources, est complexe et comporte des risques opérationnels. Cela augmente automatiquement le coût limitant ainsi le nombre d'interception.

L'affaiblissement du chiffrement est déjà discuté au niveau international et une augmentation des tensions est à prévoir. Les Etats de droit qui dans le cadre de la sécurité intérieure et extérieure ne veulent pas renoncer à la possibilité d'intercepter des communications, devront choisir l'une des deux approches dans un avenir plus ou moins lointain.

5.2 Fuites d'informations

5.2.1 Talk Talk

TalkTalk est un fournisseur de téléphonie, d'accès à Internet et de télévision payante britannique. Le 21 octobre 2015, cette entreprise a été victime d'une attaque ayant abouti au vol de données personnelles de 157 000 clients – dont plus de 15 000 se seraient également fait subtiliser leurs données bancaires. En décembre 2014 et en février 2015 déjà, des vols d'informations avaient permis à des escrocs de cibler des clients de TalkTalk, dans le cadre de tentatives d'escroquerie usant d'ingénierie sociale.

L'entreprise s'est retrouvée sous le feu des critiques pour sa gestion de l'incident actuel et pour ses procédures internes, mais également pour ne pas avoir su tirer les leçons des expériences passées. Il lui a notamment été reproché l'absence de tout chiffrement lors du stockage des données personnelles.

Selon plusieurs experts, l'intrusion a débuté par *une injection SQL*. Un aspect intéressant est que TalkTalk a également fait l'objet d'une *attaque DDoS*. On peut légitimement supposer que cette dernière a été lancée à des fins de diversion, afin de permettre aux attaquants de compromettre les systèmes tandis que TalkTalk cherchait à assurer la disponibilité de ses services[30]. Par la suite, les données saisies ont connu le destin habituel en pareil cas.

[30] Même si le fait n'a pas été confirmé, l'existence d'une demande d'extorsion a été évoquée.

Revendues sur des marchés souterrains, elles ont servi à mettre sur pied des fraudes sur mesure visant les clients de TalkTalk.

Conclusions:

Cet incident rappelle l'importance, pour chaque entreprise détenant des informations personnelles, de procéder à une analyse du risque. Il s'agit de s'interroger sur les moyens qu'un attaquant pourrait déployer afin d'y accéder, et sur le risque qu'un tel événement ferait courir aux clients concernés. Suite à cette réflexion, des mesures de protection adéquates – dont le chiffrement – seront mises en place. Il convient par ailleurs de définir une procédure de réponse à une telle éventualité, qui intègre notamment les modalités de communication tant avec les victimes de l'attaque, soit les clients, qu'avec les autorités compétentes.

5.2.2 Autres cas de perte de données

Pendant deux semaines, des attaquants auraient réussi à piller les données de clients du revendeur britannique Carphone Warehouse. L'incident a été découvert le 5 août 2015. Au total, près de 2,4 millions de données personnelles auraient été copiés illégalement sur plusieurs sites Internet gérés par Carphone Warehouse (par ex. OneStopPhoneShop.com, e2save.com, mobiles.co.uk), dont les détails de 90'000 cartes de crédit. Les clients touchés ont été averti de l'incident, et une ligne directe a été mise en service pour renseigner la clientèle inquiète.

Lors d'une cyberattaque survenue entre septembre 2013 et septembre 2015, le spécialiste irlandais de l'information Experian, qui analyse la solvabilité des clients de T-Mobile aux Etats-Unis, s'est fait dérober les données personnelles de 15 millions de clients hébergées dans ce contexte. Les données sensibles volées incluaient les numéros de sécurité sociale et de permis de conduire. Ces informations avaient beau être enregistrées en mode crypté, les attaquants pourraient les décrypter. L'incident ne concernerait toutefois pas les données des comptes bancaires ou de cartes de crédit.

Le 28 septembre 2015, la plateforme de financement participatif Patreon a elle aussi été victime d'une perte massive de données. Des informations cryptées (mots de passe, données fiscales, numéros de sécurité sociale) auraient été copiées. Par contre, les adresses électroniques ont été récupérées en texte clair. En outre, les données dérobées incluaient des courriers du système de messagerie interne. Tout en soulignant que les mots de passe étaient chiffrés, l'exploitant a recommandé aux utilisateurs de les changer. L'attaque a abouti grâce à une sauvegarde (*backup*) de la base de données des systèmes de production archivée sur un serveur test. Or ce serveur était apparemment accessible depuis Internet, via une application Web, et les attaquants ont su exploiter cette faille. Les 2,3 millions d'adresses électroniques dérobées ont été publiées sur Internet. Il est intéressant de signaler qu'un courriel de chantage est apparu dans ce contexte. Les escrocs ont menacé leurs destinataires de publier d'autres données sensibles à leur sujet, s'ils ne leur versaient pas un *Bitcoin* dans les 48 heures. On ignore dans quelle mesure les escrocs possédaient de telles données, ou s'ils se sont contentés d'écrire au hasard aux adresses électroniques dont ils avaient eu connaissance.

5.3 Systèmes de contrôle industriels

Depuis longtemps déjà, on parle beaucoup du risque inhérent aux systèmes de contrôle industriels (*SCI*) mal protégés. Les automates programmables industriels (API, en anglais *programmable logic controller, PLC*) susceptibles de faire partie d'un SCI, et qui bien souvent sont librement accessibles par Internet, permettent à un agresseur de s'infiltrer à des fins par exemple d'espionnage de systèmes industriels. Les logiciels nécessaires sont téléchargeables à volonté. Bien souvent, de telles mises en garde sont dénigrées, comme si les risques n'apparaissaient qu'en milieu de laboratoire. Or l'organisme de certification technique TÜV-Süd a montré, à propos d'une centrale hydraulique fictive raccordée à Internet en tant que *honeynet*, que même des systèmes à première vue anodins sont sujets à des cyberattaques en tous genres [31]. Les résultats ont été publiés à la fin de juillet 2015.

A peine le leurre était-il opérationnel que la centrale hydraulique fictive recevait son premier visiteur. Pendant les huit mois qu'a duré l'expérience, les experts de TÜV-Süd ont enregistré plus de 60 000 accès en provenance de plus de 150 pays. La plupart de ces tentatives émanaient d'*adresses IP* enregistrées en Chine, aux Etats-Unis ou en Corée du Sud, mais cette information ne dit rien de la localisation effective de l'agresseur. Expérience à l'appui, les accès se font généralement en pareil cas à partir d'adresses IP masquées ou falsifiées.

Les tentatives d'accès reposent généralement sur des protocoles standard. Mais l'installation d'essai décrite ici a également reçu des demandes basées sur des protocoles industriels comme Modbus/TCP ou S7Comm. Ce test montre aux exploitants de ce genre d'installations que les vulnérabilités dans la configuration sont activement recherchées, identifiées et dûment exploitées.

L'exemple décrit ci-après au chap. 5.3.1 montre que les systèmes fictifs ne sont pas seuls à exciter la convoitise. Il décrit la première panne électrique massive imputable à une cyberattaque. Or il ne faut pas oublier qu'à l'avenir, d'autres domaines, comme les appareils médicaux (chap. 5.3.3) ou les voitures (chap. 5.3.4), intéresseront toujours plus les attaquants.

5.3.1 Panne de courant en Ukraine due à un maliciel

L'avant-veille de Noël 2015, 80 000 personnes ont été privées de courant dans l'oblast d'Ivano-Frankivsk en Ukraine. Plusieurs entreprises régionales d'approvisionnement électrique ont signalé que leurs systèmes avaient été victimes d'une cyberattaque. L'incident a abouti à la déconnexion de sept sous-stations à 110 kilovolts et 23 alimentées à 35 kilovolts du réseau électrique ukrainiens [32].

---

[31] http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall (état: 29 février 2016).

[32] http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (état: 29 février 2016).

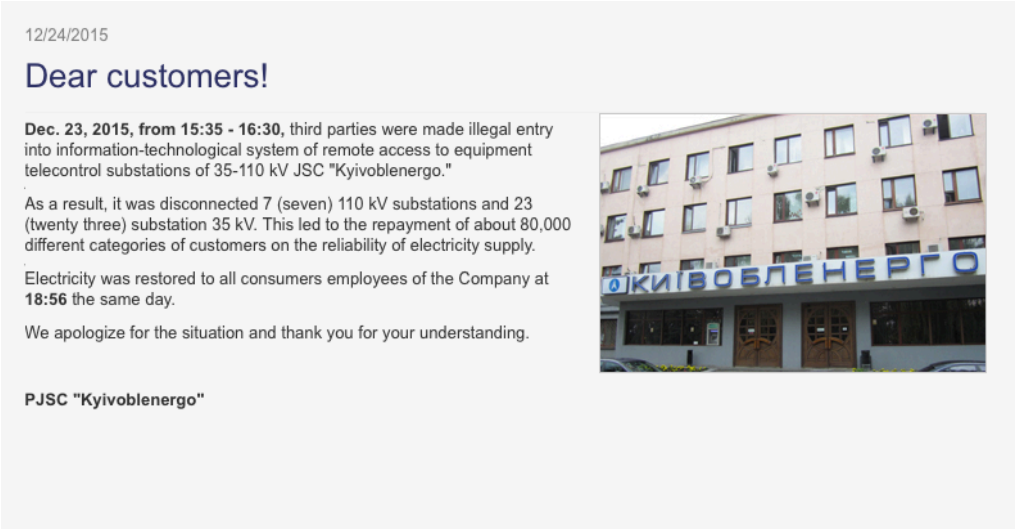

Fig. 9: Information à la clientèle d'un distributeur local ukrainien d'électricité.

L'attaque contre le fournisseur électrique a été déployée à plusieurs niveaux. Grâce à l'appui international reçu, le CERT ukrainien (CERT-UA) a identifié sur les ordinateurs des entreprises électriques touchées plusieurs variantes du maliciel BlackEnergy (BE2 et BE3). Le maliciel lui-même n'a toutefois pas pu être reconnu comme cause principale de la panne électrique[33].

Selon l'état actuel des connaissances, les faits se seraient déroulés de la façon suivante: une attaque de *spear phishing* (pêche au harpon) avec des fichiers attachés Office spécialement préparées, a infecté des ordinateurs du réseau des sociétés du secteur énergétique prises pour cibles. Le maliciel BlackEnergy a permis aux agresseurs d'explorer le réseau et d'accéder à d'autres appareils, dont ceux d'opérateurs où ils ont trouvé les consoles ICS servant au pilotage des sous-stations. Ils ont probablement provoqué la panne électrique en actionnant les disjoncteurs à partir de telles consoles, comme un opérateur légitime peut le faire localement à des fins de maintenance. Afin d'empêcher le rétablissement de l'approvisionnement électrique et d'effacer les traces du méfait, les agresseurs ont encore utilisé le maliciel KillDisk, qui a rendu inutilisables les disques durs des ordinateurs infectés. Enfin, ils ont déclenché des *attaques DDoS* contre le site Web de l'entreprise et son centre d'appels, pour l'empêcher de signaler les pannes et entraver la communication avec sa clientèle.[34]

Peu après les incidents, des représentants du gouvernement ukrainien ont accusé la Russie d'être à l'origine de l'agression. La même accusation a suivi en janvier 2016, où le virus BlackEnergy a été découvert dans le réseau de l'aéroport de Kiev Boryspil, où il n'a toutefois causé aucun dégât. Les soupçons n'ont toutefois pas pu être étayés. L'entreprise de sécurité iSight Partners attribue l'agression au collectif Sandworm, qui a lancé dans le passé d'autres attaques étonnamment similaires et conformes aux intérêts de l'Etat russe. Mais

33 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B (état: 29 février 2016).

34 http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (état: 29 février 2016).

BlackEnergy est un maliciel très répandu et vendu sur le marché noir, ce qui rend l'identification de l'agresseur d'autant plus délicate.

Conclusions et recommandations:

L'incident décrit ci-dessus est la première grave panne électrique consécutive à une cyberattaque. Les exploitants d'infrastructures similaires feraient bien de tirer les leçons de cet exemple pour mieux protéger leurs propres réseaux ou installations contre de telles méthodes d'attaque.

MELANI tient à disposition une liste de contrôle des mesures de protection des systèmes de contrôle industriels. Lesdites mesures devraient faire partie intégrante d'un processus global de sécurité, qui en garantisse la bonne mise en place et qui prévoie des contrôles réguliers et des améliorations constantes. En outre, il est important que l'exploitant d'une installation connaisse les menaces actuelles et qu'il procède à des contrôles ponctuels, débouchant sur de nouvelles mesures de sécurité ou des optimisations en la matière. A cet effet, une étroite collaboration s'avère cruciale entre les processus concernés – gestion des risques, ingénierie et exploitation.

DOKU

Mesures de protection des systèmes de contrôle industriels (SCI)

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

5.3.2 Manipulations des données traitées de façon automatisée dans l'industrie pétrolière et gazière

Avant même l'apparition du virus Stuxnet, on craignait déjà que les systèmes de pilotage des processus d'importance vitale ne subissent des cyberattaques. Comme indiqué au sous-chapitre précédent concernant BlackEnergy, il n'est même pas nécessaire de dérégler directement le système de pilotage, un agresseur peut également influencer les processus en manipulant les données des systèmes adjacents. En novembre 2015, Alexander Polyakov et Mathieu Geli, de l'entreprise de sécurité ERPScan, ont expliqué à la conférence Black Hat Europe comment, en manipulant les *systèmes ERP*, on pourrait dérégler les soupapes de pipelines dans l'industrie pétrolière et gazière.[35] Selon les experts ERP, la complexité de l'environnement système et son automatisation à de nombreux niveaux (voir fig. 10) le rendent vulnérable à trois types d'attaques:

L'un des modes opératoires consiste à falsifier les valeurs mesurées, comme la température et la pression, dans une application de gestion des ressources. D'où l'obligation pour l'exploitant d'envoyer à grands frais des équipes de maintenance, au pire des cas sur une plateforme pétrolière située en plein océan. Si en outre l'attaquant modifie de façon ciblée le

35 https://www.blackhat.com/docs/eu-15/materials/eu-15-Polyakov-Cybersecurity-For-Oil-And-Gas-Industries-How-Hackers-Can-Manipulate-Oil-Stocks-wp.pdf (état: 29 février 2016).

niveau et la capacité des citernes, des explosions sont même à craindre. Enfin, par souci d'efficacité, des systèmes tiers sont autorisés à donner certains ordres au niveau de système de pilotage. Autrement dit, il n'est même pas nécessaire que le système de contrôle lui-même soit vulnérable pour subir une attaque de sabotage.

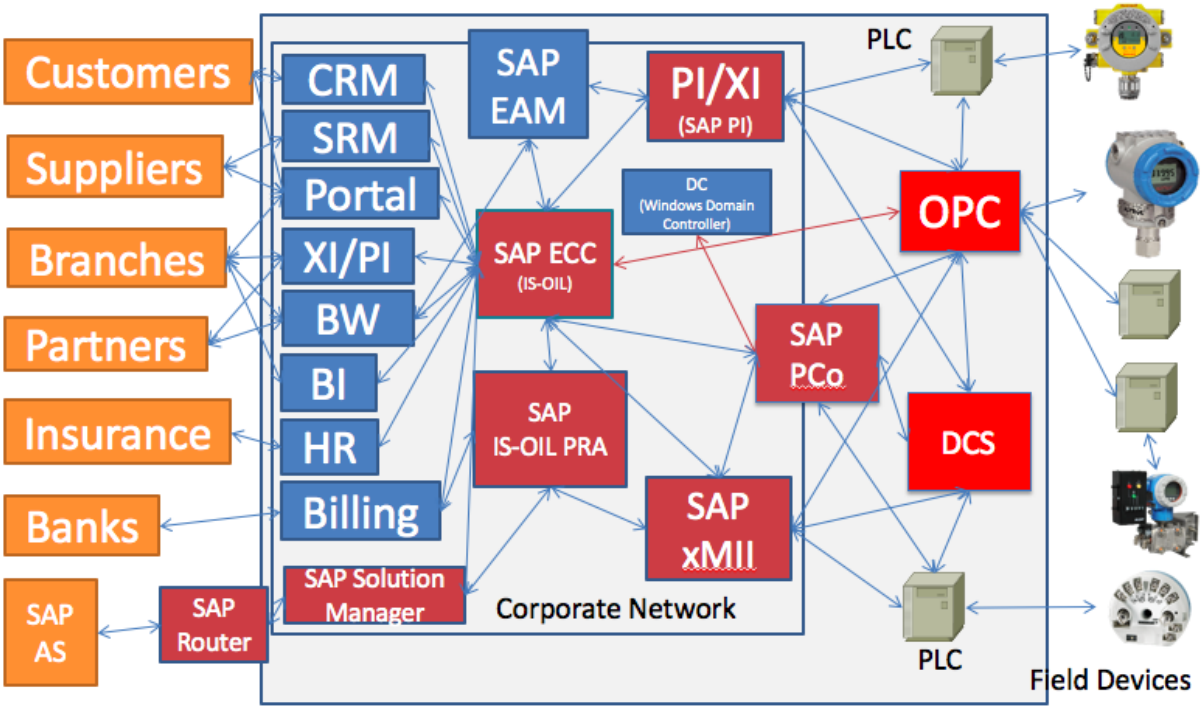

Fig. 10: Exemple d'environnement système dans l'industrie pétrolière et gazière. Source: Alexander Polyakov et Mathieu Geli

Conclusions:

Cet exemple montre les problèmes que crée au niveau des processus l'automatisation basée sur les données. Au-delà des gains d'efficience des processus, l'utilisation à grande échelle de compteurs électriques intelligents rend aussi les vecteurs d'attaque toujours plus redoutables pour saboter les installations.

5.3.3 Des milliers d'appareils médicaux accessibles par Internet

Il faut agir vite dans les hôpitaux. Car des vies humaines dépendent de décisions basées sur des données de laboratoire et de diagnostic. Le personnel traitant doit les avoir aussitôt sous la main. La rapidité et la facilité d'utilisation semblent primer sur les considérations de sécurité, au niveau de la configuration des appareils médicaux et de l'interface de gestion des données patients.

A la conférence de sécurité Derbycon 2015[36], les chercheurs Scott Even et Mark Collao ont présenté les résultats d'une étude consacrée à une entreprise du secteur de la santé où 68'000 appareils médicaux étaient directement accessibles – et donc attaquables – via Internet. De telles agressions peuvent très bien se produire, comme le montrent les résultats de dix leurres (*honeypot*) se faisant passer pour un défibrillateur ou un système IRM. Ces appareils fictifs ont subi 299 attaques de maliciels, dont 24 fructueuses.

Les risques dans le secteur de la santé vont toutefois au-delà des accès non autorisés aux équipements médicaux. Ces derniers temps, les accès à des données personnelles sensibles ont régulièrement fait les gros titres[37]. Certains patients exposent d'ailleurs eux-mêmes leurs données personnelles, en utilisant des applications peu fiables. Par ailleurs, sur 79 logiciels d'application (app) autorisés par le NHS, soit le système national de santé britannique, après avoir été testées par l'Imperial College[38], 23 étaient dépourvus de mécanismes de protection[39]. Dans quatre cas, les données concernant la santé étaient même transmises en clair.

5.3.4 La voiture intelligente – responsabilité de l'industrie automobile

La scène pourrait provenir d'un film d'horreur: lors d'une balade estivale en voiture, le chauffage s'enclenche, un programme radio détesté se fait entendre, les essuie-glaces s'activent tout seuls et sur l'écran de navigation un inconnu signale avoir pris le contrôle du véhicule. Peu après, toute tentative d'accélérer ou, pire encore, de freiner reste vaine.

Même si de telles attaques n'ont pas encore abouti dans la vie réelle, elles ne sont pas inventées. Une faille de sécurité a permis aux chercheurs Miller et Valasek de prendre le contrôle du système d'info-divertissement Uconnect à distance [40]. Il leur a suffi de connaître l'*adresse IP* du système. Ils ont ensuite injecté leur propre code dans le *firmware* (microprogramme) Uconnect afin d'accéder aux processeurs de commande situés à proximité. Ils sont ensuite parvenus, via le réseau de communication interne (bus CAN, *controller area network data bus*), à donner des commandes au moteur et aux freins, et donc à priver à distance le conducteur du contrôle de son véhicule.

Les chercheurs ont présenté à la conférence Black Hat 2015 leurs découvertes et le programme correctif (*patch*)[41] qu'ils avaient conçu avec le groupe Fiat-Chrysler et l'opérateur télécom Sprint. Leur scénario clair a frappé les esprits, dans l'industrie automobile comme dans le grand public. Mais l'intérêt s'est vite émoussé, et les consommateurs apprécient toujours autant de pouvoir piloter commodément certaines fonctions de leur véhicule à partir de l'app correspondante de leur smartphone.

---

36 http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao (état: 29 février 2016).

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (état: 29 février 2016). http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (état: 29 février 2016).

38 https://www.imperial.ac.uk (état: 29 février 2016).

39 http://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds (état: 29 février 2016).

40 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (état: 29 février 2016)

41 https://ics-cert.us-cert.gov/advisories/ICSA-15-260-01 (état: 29 février 2016).

Il reste à espérer que des considérations de sécurité amènent à séparer l'électronique de loisirs de celle de commande, sachant que de nouveaux vecteurs d'attaque potentiels apparaissent à tout moment. Il est par exemple déjà possible de déjouer les dispositifs antidémarrrage des télécommandes radio[42], ou de transmettre des ordres par le biais des systèmes d'info-divertissement, en manipulant les signaux radio[43].

Conclusions:

Plus on confie de responsabilités aux véhicules dits intelligents, et plus on s'expose à voir surgir de nouveaux problèmes. A l'ère des véhicules autonomes et intelligents et des systèmes de communication Car2X, les frontières entre la sécurité physique et la sécurité de l'information tendent à s'estomper. D'où la nécessité de procéder à des tests au moins aussi approfondis des systèmes informatiques que pour les essais de choc en laboratoire.

5.3.5 Piratage d'un barrage, probable mesure de rétorsion

En 2013, des attaquants vraisemblablement iraniens se sont introduits dans les systèmes de contrôle d'un barrage proche de New York. C'est ce qu'a rapporté en décembre 2015 le Wallstreet Journal[44], en citant deux personnes chargées de l'instruction du cas. La digue de retenue, de dimensions modestes il est vrai, aurait été victime de mesures de rétorsion après la découverte des activités de sabotage dues à Stuxnet. Il est important de tirer les leçons de l'analyse de ce genre d'incidents, et d'améliorer encore le dispositif de sécurité des infrastructures d'importance vitale.

5.4 Attaques de sites Web: DDoS, défigurations

5.4.1 BBC victime d'un «test» du collectif New World Hacking

Le 31 décembre, beaucoup d'Anglais qui désiraient revoir leur émission préférée de la BBC avant le Réveillon, ou alors faire leurs préparatifs avec son application iPlayer Radio, ont dû déchanter. Le site Web de la BBC n'affichait qu'un message d'erreur (voir fig. 11).

42 http://www.heise.de/make/meldung/Wegfahrsperre-VW-Hack-ist-offen-2778194.html (état: 29 février 2016).

43 http://www.bbc.com/news/technology-33622298 (état: 29 février 2016).

44 http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559 (état: 29 février 2016).

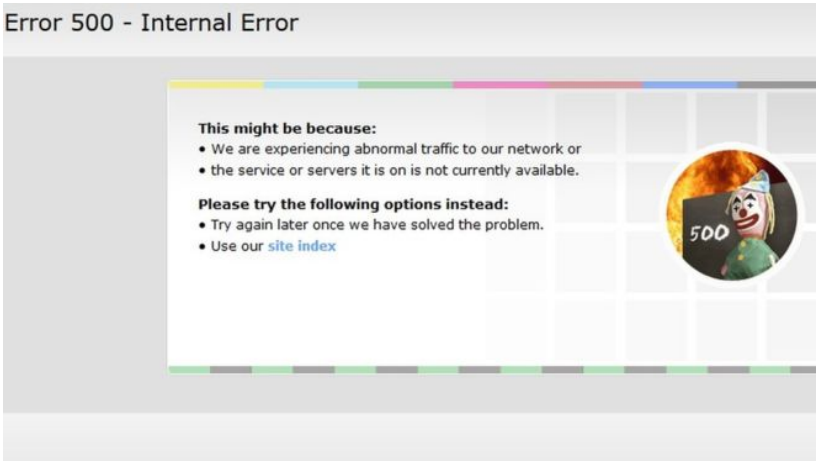

Fig. 11: Message d'erreur du site de la BBC, le 31 décembre 2015.[45]

La panne de plusieurs heures n'était pas due à un dérangement technique, mais à un test effectué par le collectif New World Hacking pour vérifier les capacités de ses serveurs. Un membre du groupe, caché sous le pseudonyme Ownz, a revendiqué l'attaque DDoS auprès de Rory Cellan-Jones, correspondant de la BBC spécialisé en technologie. Les activités du collectif auraient pour cible première la présence en ligne de l'Etat islamique. Mais pour tester son nouvel outil nommé Bangstresser, il avait choisi d'inonder le site de la BBC. Le hacker a précisé que le collectif New World Hacking n'avait nullement cherché à provoquer une panne aussi longue, et qu'il était le premier étonné de la puissance de feu de son infrastructure.

5.4.2 Anonymous contre l'Etat islamique – guerre de propagande sur Internet

Suite aux attentats de janvier 2015 contre l'hebdomadaire satirique Charlie Hebdo, le collectif Anonymous avait lancé sa campagne «#OpISIS», qui vise principalement à saboter les canaux de communication des terroristes et à entraver le recrutement de nouveaux membres. Le lendemain des nouveaux attentats de Paris, ce groupement informel a publié par vidéo[46] une déclaration de guerre à l'Etat islamique.

Faute de structure claire et précise, les mesures d'Anonymous qui ont suivi les attentats n'ont guère été coordonnées. De vives discussions ont eu lieu quant à savoir s'il fallait lancer, en plus de l'opération existante «#OpISIS», une opération séparée baptisée «#OpParis». De même, les désaccords quant à l'utilité d'une déclaration de guerre et les proclamations divergentes de sous-groupes ont amené le collectif à publier le 18 novembre 2015 un communiqué spécifique[47]. Ce document rappelait les objectifs des activités en cours d'Anonymous, en recommandant d'utiliser ses canaux de communication privilégiés. Le sous-groupe Ghost Security (GhostSec) prévoyait d'identifier et de bloquer dans les médias sociaux les comptes en relation avec l'organisation terroriste. Tous les membres ne voyaient

[45] http://www.bbc.com/news/technology-35213415 (état: 29 février 2016).
[46] https://www.youtube.com/watch?v=RwGGcZoRs-k (état: 29 février 2016).
[47] https://www.docdroid.net/hUQ7Ez2/anonymous-operations-isis-11-2015.pdf.html (état: 29 février 2016).

cependant pas d'un bon œil la coopération ponctuelle de GhostSec avec des autorités étatiques.

La presse a parlé de l'appel[48] à une journée de moqueries («Trolling Day»), organisée le 11 décembre 2015 pour ridiculiser les djihadistes sur les réseaux sociaux, et surtout des activités de «*doxing*» du groupe GhostSec. Le doxing consiste à révéler publiquement l'identité réelle ainsi que le lieu de séjour des propriétaires de sites Web ou de comptes sur les médias sociaux. Hormis la diffusion d'instructions[49] sur la manière de mieux se protéger en ligne, aucune réaction n'a été observée de la part de l'Etat islamique. Dans ces instructions, l'organisation terroriste recommande parmi d'autres produits les applications suisses Swisscom IO et Threema, ainsi que les solutions de communication de Silent Circle, entreprise basée à Genève. Il se peut qu'avec cette publicité sulfureuse, ces sociétés ou leur clientèle se soient aussi trouvés dans la ligne de mire des hacktivistes.

5.4.3 Codes QR manipulés

Les codes-barres, et désormais aussi les *codes QR* bidimensionnels, interviennent dans toutes sortes de scénarios d'application. Tout le monde connaît les codes-barres des emballages qui renferment, en plus du prix, diverses autres informations. Le code QR s'est notamment imposé dans l'aviation, où il sert à identifier les voyageurs auprès des compagnies aériennes, lors de l'embarquement.

Jusqu'ici, les craintes portaient surtout sur le risque d'utilisation abusive des informations figurant sur ces codes-barres. Or le chercheur en cybersécurité Yang Yu a démontré que les codes imprimés peuvent également constituer un vecteur d'attaque contre les systèmes informatiques qui les lisent[50]. Il a publié sous le titre «Badbarcode» plusieurs vidéos, et exposé ses découvertes à la conférence PacSec 2015, organisée à Tokyo. Yang Yu exploite toute une série de défaillances des programmes servant à scanner les codes. A partir de codes-barres manipulés par ses soins et imprimés, il a amené les systèmes de scanning non seulement à lire des informations, mais aussi à exécuter des commandes malveillantes.

Même si à ce jour aucune application malveillante de ces possibilités n'est connue, de telles failles sont potentiellement dangereuses selon Yang Yu.

5.5 Logiciels criminels (crimeware)

5.5.1 Nouveaux TLD et maliciels

Les domaines de premier niveau (*top-level domain,* TLD) n'offrent pas tous le même niveau de sécurité. Il n'est donc guère surprenant que certains soient plus prisés que d'autres par les groupes criminels. En outre, l'introduction des TLD génériques a donné aux attaquants

---

48 https://ghostbin.com/paste/ucsf3 (état: 29 février 2016).

49 http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (état: 29 février 2016).

50 http://motherboard.vice.com/read/badbarcode-project-shows-customized-boarding-passes-can-hack-computers (état: 29 février 2016).

de nouvelles possibilités d'accéder à des domaines attrayants et guère contrôlés, où ils déploient leur *infrastructure de commande et de contrôle (C&C)*. Mais les criminels se servent souvent aussi des domaines les plus connus (par ex. .com ou .biz) pour leurs méfaits.

Selon le site ntldstats.com, les TLD génériques suivants sont sujets aux maliciels:

* .science
* .click
* .link
* .party
* .xyz

On trouve régulièrement aussi des domaines de pays dont les groupes criminels se servent volontiers. Les raisons en sont multiples. Le registraire freenom.com permettait par exemple d'enregistrer gratuitement différents TLD de pays africains, ce qui a provoqué dans ces Etats une forte hausse des enregistrements de domaines à des fins criminelles.

Les domaines nationaux suivants sont notamment infestés de maliciels:

.gq (Guinée équatoriale)
.tk (Tokelau)
.ga (Gabon)
.cf (République centrafricaine)
.ml (Mali)

Le registre et les registraires doivent disposer de règles claires en matière d'*abus*, qui précisent ce qu'il arrive en cas d'utilisation criminelle d'un domaine. Il importe bien entendu de faire dûment respecter ces règles. En outre, il faut prévoir des processus bien établis et des administrateurs (*abuse teams*) qui s'occupent de tels incidents et les traitent rapidement. Vous trouverez au chap. 6.2 un rapport détaillé sur la lutte contre l'utilisation abusive des noms de domaine suisses.

5.6 Autres thèmes

5.6.1 Sueurs froides du système Android de Google

Une vulnérabilité découverte par l'entreprise de sécurité Zimperium et publiée le 27 juillet 2015 permettait à des attaquants d'accéder par MMS aux données de smartphones Android, sans la moindre interaction de l'utilisateur. Selon des estimations, la faille concernait jusqu'à 95 % des smartphones Android. Pour l'exploiter, il suffisait à l'agresseur d'envoyer à sa victime un MMS spécialement préparé, que la victime ne devait même pas ouvrir. Son smartphone était compromis dès que le système avait traité le message. L'unique moyen de défense jusqu'à la publication et à l'installation des mises à jour correspondantes consistait à désactiver la fonction de réception des MMS. Deutsche Telekom avait même suspendu l'acheminement des MMS, afin de protéger sa clientèle en cas d'attaque.

6 Tendances et perspectives

6.1 Paiement mobile

La Suède pourrait devenir le premier pays du monde sans argent liquide. Il y a dix ans encore, il aurait été impensable que les cartes de crédit et de débit remplacent un jour complètement l'argent liquide. Entre-temps, en Scandinavie, les moyens de paiement numériques sont quasiment les seuls acceptés, même dans les marchés de Noël. Selon des prévisions actuelles, le smartphone pourrait toutefois évincer les cartes de paiement susmentionnées, et le paiement mobile s'imposer comme méthode de paiement de l'avenir. Aux Etats-Unis, quatre acheteurs sur dix ont indiqué avoir déjà effectué au moins une fois un paiement mobile et, selon le site d'information Statista, la tendance continuera d'augmenter de 20% par an. La Suisse, où le paiement sans espèces a déjà une longue tradition, peine par contre à introduire des appareils à *paiement mobile*. Une telle offre existe ici depuis 2011, quand la société Mobino s'est lancée sur le marché.

Le paiement mobile est redevenu un sujet brûlant il y a quelques mois, quand les grands acteurs du marché se sont intéressés à ce créneau. Depuis la fin 2015, plus de 3000 caisses Coop réparties dans toute la Suisse sont munies du logo hexagonal vert de Twint. Ce service de Postfinance permet d'effectuer ses paiements par smartphone, dans les points de vente équipés du terminal *Bluetooth* correspondant. Paymit, produit concurrent lancé par UBS, SIX et la Banque cantonale zurichoise, a été proclamé en 2015 meilleure application de Suisse, et son téléchargement à plus de 170 000 reprises en fait l'application de paiement par smartphone la plus répandue de Suisse. D'autres prestataires de services lancent régulièrement de nouveaux produits sur le marché: la clientèle de Migros, Manor et Starbucks peut désormais régler ses factures par smartphone. Depuis peu aussi, la plateforme numérique Swiss One Wallet, créée par les sociétés Aduno, Swisscard et Netcetera, permet d'effectuer ses achats dans des boutiques en ligne ou par paiement mobile. A cela s'ajoutent les produits d'entreprises comme Apple, Facebook ou Google. Or en dépit d'une offre variée, ces services semblent avoir de la peine jusqu'ici à s'implanter en Suisse. Outre qu'il faut du temps pour changer les habitudes, l'évolution hésitante peut s'expliquer par l'offre pléthorique et peu transparente, par des craintes en matière de protection des données, ou par le fait que de nombreux prestataires ont opté pour des technologies peu répandues, que les opérateurs mobiles ne prennent pas toujours en charge. Ainsi, le fiasco de l'application de paiement Tapit de Swisscom tient notamment à ce que la méthode de communication utilisée (*nearfield communication, NFC)* a longtemps été réservée aux utilisateurs d'Android. Apple ne l'a introduite qu'avec l'iPhone 6.

Chaque application diffère par les prestations proposées, par les technologies utilisées et le public cible. Les analyses ci-après s'en tiennent par conséquent aux services Paymit et Twint, qui pourraient bientôt dominer le marché suisse.

Paymit a fait son apparition dans les premiers commerces en février 2016, et pourra s'utiliser pour les achats en ligne à partir du deuxième trimestre 2016. Cette application convient aussi pour des paiements mobiles entre particuliers. Pour utiliser Paymit, il n'est pas nécessaire d'être client d'UBS, mais il faut avoir un numéro de téléphone et un compte bancaire en Suisse, ainsi qu'une carte de crédit ou à prépaiement. Les transactions se font directement sur le compte bancaire, et la banque procède à des contrôles comme pour les

paiements classiques. Un code de sécurité protège l'application en cas de vol. Aucune autorisation supplémentaire n'est toutefois demandée lors de l'exécution des paiements. Pour limiter encore les risques, une limite des dépenses de 500 francs par jour est prévue, qu'il est possible d'augmenter le cas échéant.

Twint permet non seulement de payer dans les commerces via Bluetooth, mais aussi d'effectuer des paiements entre particuliers et dans certaines boutiques en ligne, grâce à un système de pair à pair (peer-to-peer, P2P). Nul besoin d'être client de PostFinance pour employer Twint. La liaison directe avec un compte bancaire n'est toutefois possible qu'avec six banques partenaires. Contrairement à Paymit, Twint fonctionne sans carte de crédit: la somme désirée est directement chargée sur le «portemonnaie numérique» de cette application à partir de la carte Postfinance, par recouvrement direct (LSV), par bulletin de versement ou encore par un code de crédit Twint. Par mesure de sécurité, il est possible de charger au maximum 3000 francs, et l'âge minimal des utilisateurs est fixé à douze ans.

La technologie Bluetooth est en soi sûre. Mais même si elle prévoit une authentification par mot de passe et fait appel au chiffrement, elle comporte des risques. Cabir, le premier virus pour smartphones, s'était répandu par ce canal et le programme d'espionnage Flame, découvert en mai 2012 par la société de sécurité informatique Kaspersky, utilisait notamment Bluetooth pour accéder au carnet d'adresses.

En bref, le paiement mobile est un service simple et pratique. Le risque que le portemonnaie numérique tombe entre de mauvaises mains n'est pas plus élevé que pour un portemonnaie traditionnel et, contrairement à celui-ci, il est encore protégé par un code PIN. L'inconvénient est que d'autres attaques plus perfides sont à craindre. Les cybercriminels très actifs dans le réseau développent constamment de nouvelles méthodes pour accéder aux appareils connectés à Internet et offrant des perspectives lucratives. Les limites de retrait rebutent peut-être encore les escrocs. Mais dès que les sommes susceptibles d'être soutirées augmenteront, il n'est pas exclu que des attaques du type *Man-in-the–Middle* ou de *social engineering* (ingénierie sociale) soient lancées pour détourner de l'argent au profit de criminels.

Recommandations:

- Désactiver la connexion Bluetooth lorsque celle-ci n'est pas utilisée.
- Maintenir une limite de débit basse.
- Activer les mesures de sécurité du portable (par ex. un code PIN).

Comment se protéger? Logiciel et paramètres:

https://www.melani.admin.ch/melani/fr/home/schuetzen/grundschutz.html

6.2 Répression de l'usage abusif des numéros de téléphone et des noms de domaine suisses

De nouvelles ressources d'adressage sont apparues à l'ère d'Internet dans le trafic des télécommunications, soit les noms de domaine et les adresses IP. Alors que la gestion des adresses IP n'est pas du ressort des autorités étatiques, chaque pays a reçu un nom de domaine de premier niveau (TLD) qui correspond à son code ISO à deux lettres, et qui lui permet d'attribuer à son tour des noms de domaine. En Suisse, le domaine «.ch» est administré par – ou sur mandat de – l'Office fédéral de la communication (OFCOM). La Suisse a opté pour un régime très libéral d'octroi des noms de domaine. En principe, chacun est libre, dans le monde entier, d'enregistrer et d'utiliser des noms de domaine se terminant par «.ch». Des mesures d'accompagnement sont néanmoins prévues, pour combattre les abus de manière rationnelle et efficace. Par exemple, une autorité suisse intervenant dans le cadre de l'exécution de ses tâches pourra exiger d'un titulaire qu'il indique une adresse de correspondance valable en Suisse[51] pour l'envoi de la correspondance officielle. Cette mesure vise à éviter les longues procédures d'assistance administrative ou d' entraide judiciaire, ainsi qu'à prévenir tout litige sur les compétences et le droit applicable. Concrètement, les domaines suisses relèvent du droit suisse, dont le mécanisme susmentionné permet d'assurer l'application. Ce processus prend toutefois du temps (il faut accorder au titulaire ou registrant de nom de domaine un délai pour répondre à la demande formulée). C'est ce qui a conduit à prévoir une compétence de blocage immédiat des noms de domaine suisses utilisés à des fins de *phishing* ou de diffusion de *maliciels*, afin de protéger les internautes de telles menaces.[52] Il est prouvé que l'usage systématique de cette compétence – au niveau du registre notamment – a contribué à améliorer encore la réputation du domaine suisse et à en renforcer la sécurité.[53]

Les ressources d'adressage traditionnelles ont également bénéficié de nouvelles impulsions, car la *téléphonie par Internet* ne s'est pas longtemps limitée exclusivement au réseau. Entre-temps, les appels à partir de presque tous les raccordements téléphoniques ordinaires transitent par les *réseaux IP*, une fois franchi le «dernier kilomètre» séparant le client du réseau de son prestataire. D'où de nombreuses possibilités d'interface entre Internet et le réseau téléphonique: par exemple, la téléphonie par Internet permet d'appeler des numéros situés dans des pays lointains au tarif local en vigueur là-bas, dès lors que l'opérateur dispose d'un raccordement sur place. Ou alors, un prestataire international offrira un service clients au tarif local, dans tous les pays où il a enregistré un numéro de téléphone.

Pour effectuer des appels sortants, il n'est plus nécessaire sur le plan technique d'avoir son propre numéro de téléphone. Le numéro affiché pouvant être librement choisi, l'appelant peut masquer sa véritable identité ou en prendre une fausse (*spoofing*). Le Secrétariat d'Etat à l'économie (SECO) a d'ailleurs enregistré ces dernières années une forte progression des

---

51 Art. 23, al. 3, ODI: https://www.admin.ch/opc/fr/classified-compilation/20141744/index.html#a23 (état: 29 février 2016).

52 Art. 15 ODI: https://www.admin.ch/opc/fr/classified-compilation/20141744/index.html#a15 (état: 29 février 2016).

53 https://www.switch.ch/fr/news/cybercrime/ (état: 29 février 2016).

plaintes relatives aux appels publicitaires non sollicités.[54] L'arsenal de mesures dont disposent les autorités s'avère ici inefficace. Car pour lutter contre les auteurs de tels appels, une procédure internationale complexe s'impose souvent, notamment avec les fournisseurs de marchandises ou services vendus par téléphone. D'où la difficulté pratique de poursuivre les escrocs, à l'instar de ceux se faisant passer pour le support de Microsoft[55]. La nécessité de recourir à l'entraide judiciaire internationale représente ici un obstacle majeur.

Souvent, les auteurs de tels appels se contentent d'une seule sonnerie avant de raccrocher. Les personnes appelées seront ainsi tentées de rappeler. A cet effet, les escrocs ont besoin d'un numéro de téléphone valable. S'il s'agit d'un numéro suisse, ils auront de bien meilleures chances d'être rappelés qu'avec numéro étranger. Les escrocs indiquent souvent sur les sites Web exploités pour leurs activités criminelles des numéros suisses en service, afin d'inspirer confiance à leurs victimes potentielles.

Le SECO combat les appels publicitaires non sollicités en déposant des plaintes pénales (souvent contre inconnu), ou des plaintes civiles dans le cas des opérateurs par présélection.[56] Il a par ailleurs obtenu dans plusieurs cas que des fournisseurs de services de télécommunication bloquent des numéros de téléphone utilisés abusivement, sous peine de poursuites en justice.

La gestion des numéros de téléphone incombe au plus haut niveau à l'OFCOM. Ils sont remis par blocs de 10 000 aux entreprises du secteur des télécommunications (y c. aux sociétés étrangères, qui ont besoin d'une simple adresse de correspondance en Suisse); ces dernières les transmettent à leur tour, en plus petits blocs ou individuellement, à leurs clients (finaux) basés en Suisse ou l'étranger. En réponse à l'augmentation des réclamations pour utilisation abusive de numéros de téléphone suisses, les possibilités de l'OFCOM de révocation des ressources d'adressage attribuées ont été accrues l'année dernière[57].

Le Conseil fédéral a en outre mis en consultation, le 11 décembre 2015, une modification de la loi sur les télécommunications et de la loi fédérale contre la concurrence déloyale (LCD). La modification projetée vise notamment à améliorer les instruments techniques et juridiques prévus contre les appels publicitaires non sollicités. Il est prévu d'obliger les fournisseurs de services de télécommunication à filtrer ce genre d'appels, à l'instar de ce qui se fait déjà dans la lutte contre le spam.

---

54 https://www.seco.admin.ch/seco/fr/home/Werbe_Geschaeftsmethoden/Unerbetene_Werbeanrufe.html; voir brochure «Se préserver des appels publicitaires non sollicités»: https://www.seco.admin.ch/seco/fr/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/ruhe-vor-unerbetenen-werbeanrufen_seco.html (état: 29 février 2016).

55 Voir lettre d'information de MELANI https://www.melani.admin.ch/melani/fr/home/themen/fake_support.html (état: 29 février 2016).

56 http://www.seco.admin.ch (état: 29 février 2016).

57 Voir art. 11 de l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT): https://www.admin.ch/opc/fr/classified-compilation/19970410/index.html#a11 (état: 29 février 2016).

Conclusions:

Plus l'attribution des ressources d'adressage est libérale, plus il faut simplifier les compétences de révocation ainsi que les mesures à prendre en cas d'abus, pour préserver la confiance accordée auxdites ressources. Les organismes attribuant les nouveaux noms de domaine génériques de premier niveau (new gTLD) ont bien compris ce principe: dans le cas des noms de domaine bon marché et faciles à obtenir, et donc attrayants pour les cybercriminels, les registres peuvent se montrer impitoyables en matière de révocation. S'ils ne le faisaient pas, la réputation de leurs TLD en pâtirait. Car les internautes risqueraient d'éviter systématiquement les adresses possédant une telle extension, voire de les filtrer au niveau technique. Avec pour résultat que les acteurs sérieux renonceraient à enregistrer la moindre adresse auprès d'eux.

Même si le problème ne se pose pas avec la même acuité dans la téléphonie, il faut garder à l'esprit que les numéros de téléphone suisses inspirent traditionnellement une grande confiance, du moins en Suisse. Pour préserver cette confiance, il faut autant que possible prévenir les abus et, en cas d'incident, les combattre de manière efficace.

6.3 Quand les criminels s'invitent dans la chambre d'enfants

Les enfants ont toujours eu accès à un vaste choix de jouets, leur permettant d'imiter le monde des adultes. Les plus jeunes pouvaient bercer et nourrir des poupées, s'amuser avec des voitures à piles, construire des maisons miniatures ou préparer des douceurs en plastique dans leur propre cuisine. Aujourd'hui, la numérisation a une influence sur les préférences des enfants: si leurs parents passent beaucoup de temps à l'ordinateur ou sur leur smartphone, ils cherchent à les imiter et la branche des jouets s'adapte, en commercialisant des tablettes ou des poupées high-tech pour les plus petits. L'Internet des objets s'est invité dans les chambres d'enfants, avec ses risques et avantages.

VTech Holdings Ltd., entreprise basée à Hong Kong qui produit des applications technologiques pour enfants et des jouets numériques, a été victime en novembre 2015 d'une des plus vastes cyberattaques de tous les temps. Un tiers a accédé à des données de sa boutique en ligne Learning Lodge, qui permet de télécharger des jeux et applications, des vidéos et des livres électroniques. Les banques de données du réseau social Kid Connect, grâce auquel les parents et les enfants peuvent rester en contact en s'envoyant des messages entre une tablette et un smartphone, et la banque de données PlanetVTeach ont également été pillées.

Après s'être procuré par *injection SQL* des privilèges d'administrateur et donc l'accès à 5 millions de comptes d'adultes et à 6,3 millions de comptes de mineurs, le hacker a contacté le site spécialisé Motherboard, afin de l'informer de ses agissements, en précisant qu'il avait voulu dénoncer par sa cyberattaque les mesures de sécurité insuffisantes de l'entreprise. VTech a reconnu ne pas avoir sécurisé de manière optimale son réseau, en confirmant que le vol concernait tant les parents (nom, adresse postale, adresse électronique et adresse IP, mot de passe avec question secrète et réponse pour le récupérer) que les enfants (nom, sexe et date d'anniversaire). En revanche, les numéros de sécurité sociale, de permis de conduire ou de carte de crédit n'avaient pas été dérobés.

L'entreprise n'a toutefois pas répondu au reproche selon lequel des photos et des conversations vidéo d'enfants seraient tombées entre les mauvaises mains.

La société japonaise Sanrio, propriétaire de la célèbre marque Hello Kitty, a également été victime d'un incident. A la fin de novembre, elle s'est fait subtiliser les données personnelles de 3,3 millions d'utilisateurs. Là encore, les mesures de sécurité prévues laissaient manifestement à désirer.

VTech et Kittyleaks ne sont pas des cas isolés. Mattel et la start-up Toy-Talk ont également comblé des vulnérabilités qui, selon les experts informatiques, auraient permis d'utiliser la poupée interactive Hello Barbie comme moyen d'espionnage. Car la poupée, reliée à Internet par le réseau local sans fil, peut avoir des discussions interactives, grâce à un micro soumettant les données entrantes au serveur d'une entreprise tierce. Cette faille de sécurité aurait par exemple permis de prendre le contrôle de la poupée par le micro.

Les exemples qui précèdent montrent que dans la société actuelle, on n'a toujours pas réalisé partout quelles sont les données sensibles. Les données d'enfants sont spécialement sensibles et requièrent une protection particulière. Les jouets reliés au réseau constituent un phénomène récent et devraient enregistrer une forte croissance ces prochaines années. Il reste à espérer que les fabricants n'investiront pas seulement dans de nouvelles fonctions, mais aussi dans la sécurité.

Recommandations:

- Changer souvent de mot de passe.
- Se souvenir que chaque objet relié à Internet est susceptible de présenter un risque.
- Aborder le thème de la sécurité avec les enfants.
- Ne pas utiliser les coordonnées des enfants pour commander et payer des produits leur étant destinés.

INFO

Comment se protéger? Règles de comportement :

https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.html

7 Politique, recherche et politiques publiques

7.1 Interventions parlementaires

Objet	N°	Titre	Déposé par	Date de dépôt	Conseil	Dépt	Etat des délibérations et lien
Ip	15.4073	L'armée est-elle réellement capable de protéger l'espace cybernétique helvétique?	Fathi Derder	25.09.2015	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154073
Po	15.5064	Débat sur le service public. Répondre aux défis de la société de l'information en prévenant la discrimination des	Balthasar Glättli	25.09.2015	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154064

		médias novateurs					
Po	15.3980	Evaluer les chances et les risques de l'Industrie 4.0	Groupe des Verts	24.09.2015	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153980
Mo	15.3979	Une plate-forme pour accompagner l'Industrie 4.0	Adèle Thorens Goumaz	24.09.2015	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153979
Po	15.3957	Mesures contre le commerce illégal en ligne d'espèces menacées	Guillaume Barrazone	24.09.2015	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153957
Ip	15.3917	Crowdfunding. Zone charnière entre l'innovation financière et la protection des investisseurs	Konrad Graber	23.09.2015	CE	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153917
Mo	15.3903	Légaliser sans attendre les casinos en ligne	Peter Schilliger	23.09.2015	CN		https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153903
Iv.pa	15.482	Egalité de traitement entre les diffuseurs privés et les diffuseurs privés qui opèrent en ligne	Thomas Matter	22.09.2015	CN	CTT-CN	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20150482
Ip	15.3959	Poursuite temporaire de la fourniture de services de messagerie électronique après la résiliation du contrat	Anita Fetz	24.09.2015	CE	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153959
Ip	15.3882	Risques sanitaires liés à l'utilisation des TIC dans la société de l'information	Thomas Böhni	22.09.2015	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153882
Qst.	15.5466	Engagement de la Poste dans le développement d'une plate-forme de vote électronique	Cédric Wermuth	15.09.2015	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20155466
QU	15.1059	Aide financière d'urgence de la Confédération suite à la cyberattaque contre TV5 Monde	Didier Berberat	10.09.2015	CE	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20151059
Ip	15.3822	Il faut rapidement corriger les défauts de jeunesse du nouvel abonnement de transports publics «Swiss Pass»	Jean Christophe Schwaab	09.09.2015	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153822
Mo	15.3799	Arrêté sur le réseau et vignette électronique	CTT-CE	18.08.2015	CE	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153799
Ip	15.4062	Mettre en œuvre rapidement les projets destinés à réduire la bureaucratie	Hans Grunder, groupe BD	25.09.2015	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154062
Ip	15.3994	Mesures visant à garantir la réussite des projets informatiques de la Confédération. Pléthore de «prestations humaines»	Thomas Maier, Martin Bäumle	24.09.2015	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153994

Po	15.4045	Droit d'exploiter des données personnelles. Droit d'obtenir une copie	Fathi Derder	25.09.2015	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154045

7.2 Loi allemande sur la sécurité informatique

Une nouvelle loi abondamment discutée, destinée à renforcer le niveau de sécurité des systèmes informatiques (loi sur la sécurité informatique), est entrée en vigueur le 25 juillet 2015 en Allemagne. Elle vise à accroître sensiblement le niveau de sécurité informatique, au profit de l'économie et des utilisateurs privés.[58] Les destinataires de la loi sont principalement les exploitations d'infrastructures critiques et les exploitants de sites Web non destinés à un usage strictement privé. La loi astreint les exploitants d'infrastructures critiques à protéger leurs systèmes informatiques selon l'état actuel de la technique, ainsi qu'à notifier les incidents significatifs de cybersécurité. Une agence centrale chargée de la sécurité informatique des infrastructures critiques a été créée à l'Office fédéral de la sécurité des technologies de l'information (BSI), soit l'organe de contrôle. Les infractions aux nouvelles obligations (par ex. absence de notification, annonce incorrecte, incomplète ou tardive) seront dorénavant passibles d'une amende pouvant aller jusqu'à 100 000 euros.

Alors que la finalité générale indiquée est l'amélioration substantielle de la sécurité des systèmes informatiques en Allemagne et la protection des infrastructures critiques, les objectifs concrets de diverses dispositions de loi, qui relèvent essentiellement du droit pénal accessoire, ne se voient pas d'emblée. Il est trop tôt pour dire si l'exécution se concentrera sur la surveillance du respect, par les assujettis, des prescriptions destinées à protéger différentes catégories de données (personnelles) sensibles, sur le respect de l'obligation de notifier les incidents de cybersécurité – voire sur ces deux aspects. Les services compétents devront d'abord mettre en place une pratique cohérente avec les critères d'appréciation requis, notamment en ce qui concerne la proportionnalité et la notion juridique indéterminée d'«état de la technique».

La loi sur la sécurité informatique n'aura pas de conséquence directe pour la Suisse, puisqu'il s'agit de droit allemand. Mais des efforts similaires sont en cours, par exemple pour imposer de signaler les incidents, dans le projet de directive européenne en faveur d'un niveau élevé commun de sécurité des réseaux et de l'information (SRI). La future directive SRI pourrait amener la Suisse à reprendre de telles propositions, à la faveur de l'adaptation autonome au droit européen. En outre, les entreprises helvétiques ayant outre-Rhin des filiales soumises à la loi sur la sécurité informatique devront rapidement se pencher sur la question. Car à supposer qu'une enquête soit ouverte contre une filiale soupçonnée d'avoir violé la loi allemande, des répercussions pour la maison mère suisse ne peuvent être exclues.

[58] http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html (état: 29 février 2016).

7.3 Conférence SNPC

La deuxième conférence sur les cyberrisques en Suisse s'est tenue le 2 novembre 2015 au Stade de Suisse à Berne. Plus de 250 représentants de l'économie, de la politique, de l'administration et de la société civile y ont eu droit à des informations sur la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et à un aperçu des mesures déjà prises dans ce domaine. Des intervenants tant suisses qu'étrangers y ont abordé les divers aspects des cyberrisques. Le GovCERT.ch a notamment évoqué le déroulement concret d'une analyse en cas d'incident. MELANI a présenté le prototype des tableaux de la situation établis dans le cadre de la SNPC. La conférence s'est en outre intéressée à la répression de la cybercriminalité. Le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) a tiré un bilan des travaux visant à établir l'image de la cybercriminalité en Suisse, et le Ministère public zurichois a évoqué des exemples concrets tirés de la pratique quotidienne des autorités pénales compétentes. La démonstration en direct d'un hacker expliquant comment identifier systématiquement les installations de commande des systèmes industriels et leurs vulnérabilités a suscité un vif intérêt.

La protection de la Suisse contre les cyberrisques reste donc un enjeu de taille. Mais la conférence a aussi montré le chemin parcouru ces dernières années. La clé du succès réside dans la coordination des nombreux acteurs impliqués. Aussi la SNPC veillera-t-elle, en 2016 aussi, à intensifier encore cette fructueuse collaboration.

8 Produits publiés par MELANI

Outre ses rapports semestriels, MELANI met à disposition du grand public des produits aussi nombreux que variés. Les sous-chapitres suivants passent en revue les blogs, lettres d'informations, listes de contrôle, instructions et fiches d'information parus durant la période sous revue.

8.1 GovCERT.ch Blog

8.1.1 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ http://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.1.2 Ads on popular Search Engine are leading to Phishing Sites

23.11.2015 - GovCERT.ch and Reporting and Analysis Centre for Information Assurance (MELANI) are aware of an ongoing phishing campaign that is targeting a large credit card issuer in Switzerland. What makes this phishing campaign somehow unique is the way how the phishers are advertising their phishing sites: while traditionally phishing sites are being promoted through phishing emails that are usually being sent to a large audience, the phishers are using advertisements (Ads) on a popular search engine to promote their phishing sites.

➔ http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

8.1.3 Update on Armada Collective extort Swiss Hosting Providers

08.11.2015 - During the recent days and weeks, various Hosting Providers in Switzerland have been blackmailed by a hacking group that calls themselves Armada Collective. As the Distributed Denial of Service (DDoS) attacks carried out by the Armada Collective have grown in terms of intensity and frequency, we have decided to publish an update to our previous blog post about Armada Collective, providing a short overview on the current situation in Switzerland and some additional information.

➔ http://www.govcert.admin.ch/blog/15/update-on-armada-collective-extort-swiss-hosting-providers

8.1.4 Armada Collective blackmails Swiss Hosting Providers

22.09.2015 - Earlier this year, we warned about DD4BC, a hacker group that tried to extort money from high value targets in Switzerland and abroad. While DD4BC is still around, MELANI / GovCERT.ch as well as the Cybercrime Coordination Unit Switzerland (CYCO) did receive several independent reports from hosting Providers in Switzerland recently that they are being blackmailed by a hacker group that calls themselves Armada Collective.

➔ http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

8.1.5 Swiss Advertising network compromised and distributing a Trojan

22.09.2015 - On September 11, 2015, MELANI / GovCERT.ch got informed by security researcher Kafeine about a popular advertising network in Switzerland that obviously got compromised by cybercriminals, leading to an exploit kit called Niteris.

➔ http://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan

8.1.6 Analysing a new eBanking Trojan called Fobber

11.09.2015 - Some weeks ago we read an interesting blog by Malwarebytes about Fobber, a new e-banking focussed malware in the arena that seems to be a Tinba spinoff. We decided to have a closer look at it to find out whether Swiss critical infrastructures are targeted by it.

We'd like to share our findings with you, because it contains some interesting advanced techniques that at the same time are implemented in a comparably simple way; we think this makes Fobber an ideal case study.

➔ http://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber

8.2 Lettre d'information

8.2.1 TeslaCrypt: les rançongiciels qui chiffrent les données et exigent le paiement d'une rançon ne faiblissent pas

03.12.2015 - La centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a reçu ces derniers jours plusieurs annonces témoignant d'une recrudescence d'infections avec le rançongiciel « TeslaCrypt », qui chiffre les données et exige le paiement d'une rançon.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/teslacrypt.html

8.2.2 Céder au chantage finance et renforce l'infrastructure des attaques DDoS

19.11.2015 - L'extorsion est actuellement une des méthodes favorites des cybercriminels visant un rapide gain financier. Différents types d'attaques sont employés pour soutirer de l'argent à une cible. Parmi ceux-ci, on trouve les attaques par déni de service (distributed denial of service, DDoS), qui visent à empêcher l'accès à des sites Internet ou à des services informatiques. Cette année, MELANI a déjà rapporté plusieurs cas d'attaques accompagnées de demandes de rançon et lancées par les groupes Armada Collective et DD4BC, qui ont fait grand bruit dans les médias suisses. MELANI déconseille fortement d'entrer en matière sur les exigences des maîtres chanteurs.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/ddos_extortion.html

8.2.3 MELANI consacre son 21e rapport semestriel à la sécurité des sites Web

29.10.2015 - Le 21e rapport semestriel de MELANI porte notamment sur les attaques d'espionnage, qui n'ont pas épargné la Suisse, sur les attaques d'hameçonnage (phishing), toujours aussi fréquentes, et sur le thème prioritaire que constitue la sécurité des sites Internet. L'introduction d'un thème prioritaire est l'une des nouveautés du rapport semestriel.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/MELANI-21-rapport-semestriel.html

8.2.4 Formulaire d'annonce des cas d'hameçonnage

29.07.2015 - Au cours de ces dernières années, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a traité un nombre croissant de demandes concernant des affaires d'hameçonnage (phishing). Les tentatives d'hameçonnage au moyen

de courriers électroniques ou de sites Internet qui ont été signalées visaient la plupart du temps des clients d'établissements financiers suisses ainsi que des utilisateurs de plateformes en ligne de renommée mondiale (telles que des réseaux sociaux, des services de messagerie électronique ou des fournisseurs de services de paiement en ligne). Afin d'assurer un traitement plus efficace des annonces de phishing, MELANI a lancé un site Internet sur lequel les cas présumés d'hameçonnage peuvent être signalés.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/meldeportal_gegen_phishing.html

8.3 Listes de contrôle et instructions

MELANI n'a pas publié listes de contrôle ou d'instructions supplémentaires durant le deuxième semestre de 2015

9 Glossaire

Terme	Définition
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (par exemple : 172.16.54.87).
Application Programming Interface (API)	Une interface de programmation applicative (API) est un ensemble de fonctions permettant d'accéder aux services d'une application, par l'intermédiaire d'un langage de programmation.
DDoS (Attaque)	Une attaque par déni de service distribué (Distributed Denial-of-Service attack) est une attaque durant laquelle la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Programmable Logic Controller (PLC)	Un automate programmable industriel (PLC) est un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Depuis plusieurs années, de tels dispositifs remplacent dans la plupart des domaines le pilotage par des réseaux logiques câblés.
Backbone	Réseau à grande vitesse servant à interconnecter des réseaux plus petits. Synonymes: réseau fédérateur, dorsale Internet.
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Bibliothèque	Collection de fonctions, de sous-programmes ou de programmes destinés à des applications particulières ou utilisés dans le cadre d'un système de développement.
Bitcoin	«Bitcoin» désigne à la fois un système de paiement à travers le réseau Internet et l'unité de compte utilisée par ce système de paiement.
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 (par ex. la souris).
Booter/Stresser	Service illégal permettant même à des débutants de lancer des attaques DDoS.

Border Gateway Protocol (BGP)	Protocole d'échange de routes utilisé notamment sur le réseau Internet, pour la connectivité entre des systèmes autonomes.
Bot / Malicious Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (malicious bots) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
Bug Bounty Programs	Programme proposé par de nombreux sites web et développeurs de logiciel, permettant à des personnes de recevoir reconnaissance et compensation après avoir signalé des bugs (exploits, vulnérabilités). Les développeurs pourront les découvrir et les corriger avant que le grand public en soit informé, évitant des abus.
Bus	Système de transfert de données entre plusieurs unités fonctionnelles de traitement de données par l'intermédiaire d'une voie de transmission commune, dans lequel les composants ne prennent aucune part à la transmission des données entre les autres participants.
Captcha	CAPTCHA est l'acronyme de Completely Automated Public Turing test to tell Computers and Humans Apart. Les CAPTCHA servent à déterminer si l'interlocuteur est un être humain ou une machine.
Abuse teams	Equipe d'experts veillant au respect des règles de bon usage d'Internet et réceptionnant toutes les plaintes.
CERT	Un CERT (Computer Emergency Response Team) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises et aux administrations, mais dont les informations sont généralement accessibles à tous.
Certificat	Un certificat numérique est l'équivalent, dans le cyberespace, d'une pièce d'identité et sert à attribuer une clé publique spécifique à une personne ou organisation. Il porte la signature numérique de l'autorité de certification.
Cheval de Troie	Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.

Cloud Computing	L'informatique en nuage (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les technologies de l'information et de la communication ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises auprès d'un ou plusieurs prestataires. Les applications et les données ne se trouvent plus sur l'ordinateur local ou au centre de calcul de l'entreprise, mais en nuage (cloud). L'accès à ces systèmes à distance s'effectue par un réseau.
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).
Crimeware Kit	Boîte à outils composée de codes malveillants personnalisables et permettant même aux débutants de lancer à grande échelle des attaques «clés en main».
Cryptage de bout en bout	Méthode où le chiffrement des données est effectué à l'origine, dans le système émetteur, le déchiffrement correspondant ne se faisant qu'à l'arrivée, dans le système récepteur (end-to-end encryption).
Defacement	Défiguration de sites Web
Doxing	Recherche via Internet puis publication d'informations sur une personne, généralement pour lui nuire.
Firmware	Microprogrammes. Instructions enregistrées dans une puce pour commander un appareil (par ex. numériseur, carte graphique). Elles sont en général modifiables par des mises à jour.
Flash	Adobe Flash (s'abrégeant Flash, auparavant Macromedia Flash) est un environnement de développement intégré propriétaire servant à créer des contenus multimédia. Flash s'emploie aujourd'hui sur de nombreux sites Web, dans des bannières publicitaires ou comme fonction d'un site, par exemple comme menu système. Des sites sont entièrement développés à l'aide de Flash.
Honeypot	Le terme honeypot (pot de miel) désigne, en jargon informatique, un programme ou un serveur simulant

	un ordinateur, un réseau complet ou le comportement d'utilisateurs fictifs. Les pots de miel servent à observer le comportement et à enregistrer les méthodes d'attaque de hackers.
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. L'attaquantcherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le serveur.
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.
JavaScript	Langage de script basé objet pour le développement d'applications. Les JavaScripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les JavaScripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
KillDisk	Utilitaire de formatage permettant de détruire complètement toutes les données présentes sur un disque dur, éliminant toute possibilité de récupération.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Macro	Programme constitué d'une suite de commandes dispensant l'utilisateur de les saisir, et qui seront rejouées dans le même ordre par la suite.

Malware	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (par ex. les virus, les vers ou les chevaux de Troie).
Man-in-the Middle	Man-in-the-Middle attack (attaque de l'homme du milieu) où l'attaquant s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
NFC (Near Field Communication)	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.
Paiement mobile	Toute transaction effectuée depuis un téléphone mobile et débitée sur une carte bancaire, sur la facture de l'opérateur ou encore sur un portemonnaie électronique.
Patch	Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi par exemple à une lacune de sécurité.
Phishing	Par l'hameçonnage, des criminels tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir par exemple d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (par ex. eBay) ou des données d'accès pour l'e-banking. Les criminels 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.
Porte dérobée	Une porte dérobée (backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un hacker d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Spam (pourriel)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de spammer (polluposteur) et ses envois de spamming (pollupostage).
QR-Codes	Le code QR (Quick Response) est un type de code-barres bidimensionnel pouvant être lu et interprété rapidement par un smartphone notamment.

Ransomware	Rançongiciel. Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le criminel chiffre ou bloque la machine et demande de l'argent pour permettre de ré-accéder aux données ou à la machine.
Remote Administration Tool ou Remote Access Tool (RAT)	Un Remote Administration Tool, outil de télémaintenance, est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Routeurs	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un routeur 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).
Streaming (Service de transmission en continu)	Principe utilisé pour l'envoi en continu et la lecture de flux audio ou vidéo par le réseau.
SmartMeter	Un Smart Meter (compteur intelligent) est un compteur électrique de nouvelle génération, qui identifie la consommation énergétique de l'utilisateur de manière détaillée et peut transmettre ces données à l'entreprise chargée de la distribution.
Smartphone	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.).
SMS	Short Message Service (service de messages courts). Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
Spear phishing	Hameçonage ciblé. La victime aura par exemple l'illusion de communiquer par courriel avec une personne connue d'elle.
Switch	Commutateur réseau, équipement reliant plusieurs segments d'un réseau.
Système de cryptage	Technique ayant pour but de chiffrer un message, c'est-à-dire de le rendre inintelligible pour ceux à qui il

	n’est pas destiné. La cryptographie permet d’assurer la sécurité des transactions et la confidentialité des messages.
Système ERP	ERP (enterprise resource planning) désigne un progiciel permettant de gérer tous les processus d’une entreprise, en intégrant l’ensemble de ses fonctions, dont la gestion des ressources humaines, la gestion comptable et financière, l’aide à la décision, mais aussi la vente, la distribution, l’approvisionnement et le commerce électronique.
Systèmes autonomes	Ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne est cohérente.
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. Dans le domaine industriel, l'expression «systèmes de contrôle industriels» (Industrial Control Systems, ICS) est entrée dans le langage courant.
Top Level Domain	Tout nom de domaine dans Internet est formé d’une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d’un ordinateur ou d’un site est de.example.com, le TLD sera «com».
TOR (The Onion Router)	Réseau informatique permettant d’anonymiser les données de connexion.
USB Memory Stick	Clé mémoire USB. Petit dispositif de stockage des données connecté à l'interface USB d'un ordinateur.
Spoofing	Technique consistant à manipuler un système informatique afin de cacher son identité par celle d’une autre personne, afin d’agir anonymement.
VoIP	Voice over IP, téléphonie par le protocole Internet (IP). Protocoles souvent utilisés: H.323 et SIP.
VPN	Virtual Private Network (réseau privé virtuel). Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (par ex. Internet).
Watering Hole Attack	Attaque dite du trou d’eau, attaque ciblée par un maliciel n’infectant que des sites supposés être visités par un groupe spécifique d’utilisateurs.

Zero-Day (vulnérabilité)	Une faille de sécurité qui n’est pas connue publiquement.