Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de stratégie informatique de la Confédération USIC
Service de renseignement de la Confédération SRC

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

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2010/II (juillet à décembre)

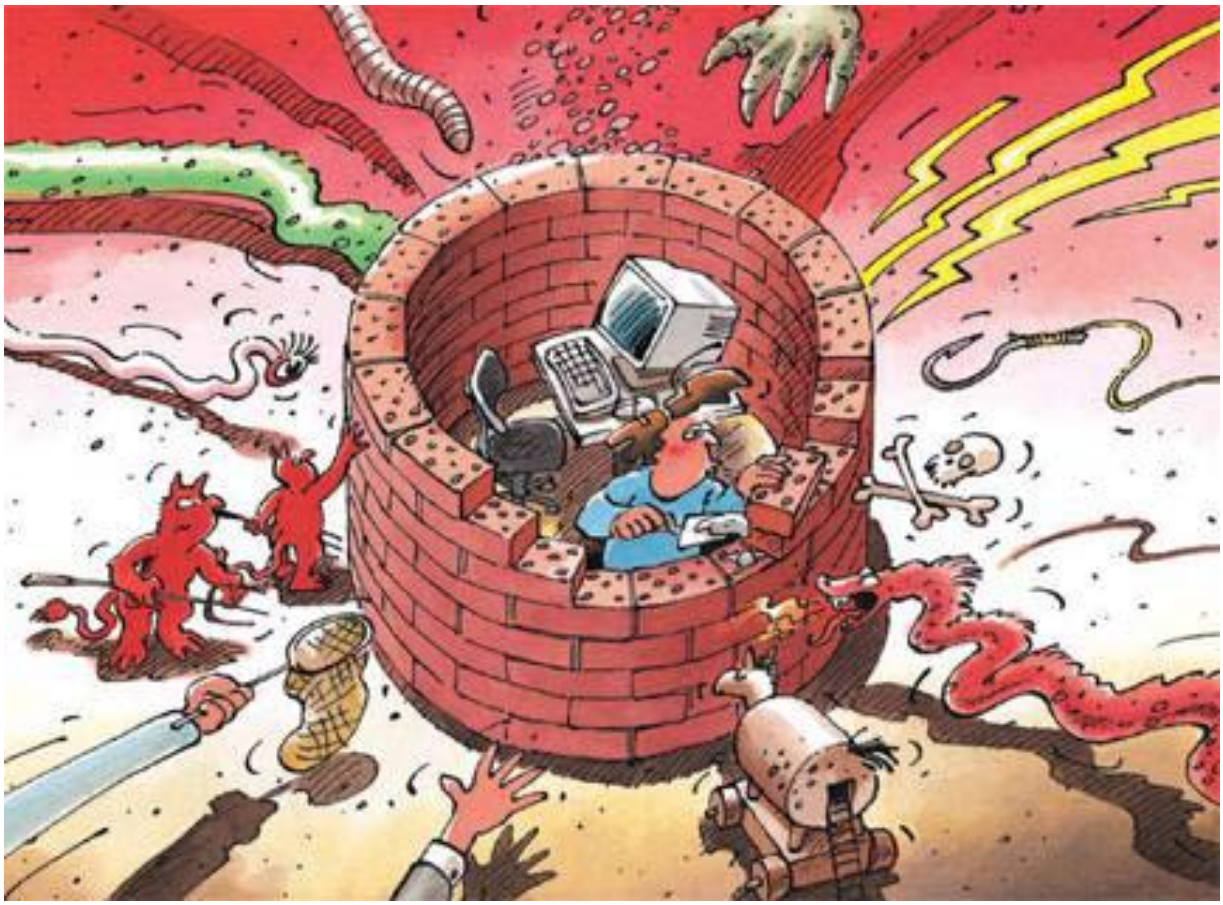

Table des matières

1 Temps forts de l'édition 2010/II

- **Stuxnet – Attaque contre les systèmes de contrôle**
  Suite à l'apparition du ver informatique Stuxnet, les médias ont examiné en 2010 sous ses différentes facettes la problématique des cyberattaques dirigées contre des systèmes de contrôle (SCADA), thème dont les milieux spécialisés discutent depuis longtemps déjà. Stuxnet est toutefois le premier cas à bénéficier d'une audience planétaire. Pour peu que les cyberpirates soient aussi motivés et leurs ressources suffisantes, tout système risque un jour d'être infiltré et saboté. Et tout indique que des attaques similaires se reproduiront.
  ► Situation sur le plan international: chapitre 4.1
  ► Situation sur le plan international: chapitre 4.6
  ► Tendances / Perspectives: chapitre 5.1
- **Attaques par déni de service distribué (Distributed Denial of Service, DDoS)**
  Des attaques DDoS, inondant la victime de messages envoyés simultanément par de nombreux systèmes, sont menées dans le cyberespace à différentes fins. Au début, il s'agissait le plus souvent de simples actes de vandalisme. Entre-temps, les motivations ont évolué. On observe p. ex. le lancement d'attaques DDoS à titre de vengeance, pour nuire à la concurrence, pour extorquer de l'argent ou pour des mobiles d'ordre politique.
  ► Situation en Suisse: chapitre 3.1
  ► Situation en Suisse: chapitre 3.2
  ► Tendances / Perspectives: chapitre 5.2
  ► Annexe: chapitre 7.1
- **Sécurité des smartphones**
  On a longtemps cru que les smartphones n'étaient pas une cible attrayante pour l'industrie des maliciels. Outre le nombre élevé de systèmes d'exploitation, les sceptiques faisaient valoir la difficulté des maliciels à se propager et l'absence de modèles d'affaires spécifiques parmi les cybercriminels. Or la diffusion croissante de smartphones et de téléphones mobiles dotés de fonctions analogues à un ordinateur, de même que la sauvegarde de données sensibles sur ces appareils, en font une cible toujours plus attrayante pour les escrocs.
  ► Tendances / Perspectives: chapitre 5.3
- **Infections de sites Web toujours aussi nombreuses**
  Les infections de sites Web sont en ce moment le principal vecteur de diffusion des maliciels. Les serveurs centraux hébergeant le contenu de différents sites y contribuent largement. Une seule page compromise peut en contaminer quantité d'autres, surtout s'il s'agit de publicité en ligne ou de services statistiques.
  ► Situation en Suisse: chapitre 3.9
  ► Situation en Suisse: chapitre 3.13
- **Recrudescence du phishing contre les services Internet**
  Les services les plus exposés sont ceux dont la protection se limite à un nom d'utilisateur et un mot de passe et qui permettent à un intrus de s'enrichir, de manière directe ou indirecte. Outre le négoce des émissions, ce sont principalement les cartes de crédit, les systèmes de paiement en ligne, les plates-formes de vente aux enchères, les fournisseurs de messagerie électronique et les réseaux sociaux.
  ► Situation en Suisse: chapitre 3.5
  ► Situation sur le plan international: chapitre 4.3
  ► Situation sur le plan international: chapitre 4.4

2 Introduction

Le douzième rapport semestriel (juillet à décembre 2010) de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) commente les grandes tendances et les risques liés aux technologies de l'information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l'étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (*écrits en italique*) sont expliqués dans un **glossaire (chapitre 6)** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

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

Les **chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six derniers mois de l'année 2010. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

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

Le **chapitre 7** est une annexe contenant des développements ou instructions sur certains thèmes du rapport semestriel.

3 Situation en Suisse de l'infrastructure TIC

3.1 Atteinte à la disponibilité des sites du PS, du PDC, du PLR et de l'UDC

En l'espace d'une semaine, les sites Web des quatre principaux partis politiques suisses ont subi à tour de rôle une *attaque par déni de service distribué* (DDoS), qui a ralenti leur fonctionnement voire les a paralysés pendant plusieurs heures à chaque fois. Les attaques contre le PS ont débuté lundi 8 novembre 2010, et le PDC a été pris pour cible le jeudi suivant. C'était au tour du PLR le vendredi soir, puis de l'UDC le dimanche. Selon le PS, jusqu'à 200 ordinateurs situés principalement en Allemagne, aux Pays-Bas et aux Etats-Unis appelaient son site en même temps. D'où huit millions de tentatives d'accès en quatre heures. Le PDC a parlé de plus de 120 machines adressant simultanément des requêtes à son site. Les attaques étaient probablement l'œuvre d'un *réseau de zombies*.

On ignore tout des mobiles de ces attaques, notamment d'un lien éventuel avec les votations du 28 novembre 2010. Parmi les objets du scrutin figurait l'initiative sur le renvoi. Outre ces attaques dénoncées dans les médias, il y a sans doute eu un nombre élevé d'agressions (contre de plus petites entreprises ou leurs sites Web) qui n'ont pas été rendues publiques.

Même sans grandes connaissances techniques, il est relativement simple d'organiser une attaque DDoS sur le marché clandestin. Le prix varie selon la capacité du site à attaquer. Quelques centaines de dollars suffisent généralement à louer ce genre de service. Comme les ordinateurs impliqués sont des systèmes compromis d'utilisateurs ne se doutant de rien, il est très difficile d'identifier par des moyens techniques l'origine de l'attaque. Selon le type d'attaque lancé, l'adresse IP de l'expéditeur est d'ailleurs falsifiée.

3.2 Attaque des partisans de Wikileaks

Le 5 décembre 2010, le prestataire de services financiers PostFinance a bloqué le compte sur lequel parvenaient les dons en faveur du site Wikileaks. Son fondateur Julian Assange avait fourni des données erronées sur un prétendu domicile genevois. Par la suite, le site de PostFinance a été victime d'une attaque *DDoS* attribuée à des partisans de Wikileaks. L'incident a perturbé son fonctionnement pendant près de 22 heures: les 1,2 millions clients d'e-banking de PostFinance n'ont pu accéder à leurs comptes, ou alors seulement au ralenti. Les attaques étaient visiblement coordonnées par une groupe informel du nom d'Anon Operation se livrant, depuis décembre 2010, à des «cyberreprésailles» contre les supposés adversaires de Wikileaks. Ce groupe a publiquement invité à télécharger en ligne un programme capable d'envoyer en grandes quantités des requêtes illégitimes à n'importe quelle adresse électronique. Car plus les utilisateurs du logiciel étaient nombreux, plus il devenait probable que le site visé soit surchargé et donc inaccessible. Outre PostFinance, la filiale d'Ebay PayPal ainsi que les sites de Mastercard et Visa, ceux d'Interpol et des autorités suédoises ont subi des attaques similaires.

Suite à cette cyberattaque, les autorités de poursuite pénale de différents pays ont procédé à des arrestations. Le FBI a perquisitionné sur sol américain 40 maisons ou appartements.[1] En

[1] http://www.tagesanzeiger.ch/digital/internet/FBIAktion-gegen-Anonymous/story/23000748 (état: 10 janvier 2011).

Grande-Bretagne, la police a arrêté cinq présumés cyberpirates.[2] Un Néerlandais de 16 ans a connu le même sort.[3] Les autorités allemandes et françaises ont également ouvert leurs propres enquêtes dans ce contexte.[4]

Ce genre d'attaque est normalement l'œuvre de réseaux de zombies. Dans le cas d'espèce, les sympathisants de Wikileaks avaient la possibilité de télécharger un programme appelé LOIC (Low Orbit Ion Canon), puis d'indiquer manuellement l'URL à attaquer ou d'accepter que leur ordinateur soit contrôlé à distance. L'appel avait été lancé via des réseaux sociaux comme Facebook ou Twitter. Vu qu'il existe aussi une version de LOIC s'exécutant automatiquement dans le navigateur, même les néophytes pouvaient participer à l'attaque. Les auteurs des attaques n'avaient pas de grandes connaissances en informatique, il a été assez facile pour la police d'identifier ces personnes.

Les attaques DDoS ne sont pas nouvelles et sont fréquemment utilisées comme moyen de chantage ou pour nuire à la concurrence. On observe toutefois un nombre croissant d'attaques à mobiles politiques, comme dans le cas précité. Outre les manifestations dans la rue, les protestations sont toujours plus nombreuses dans le monde virtuel.

3.3 Premier exercice Cyber Europe

Le 4 novembre 2010, l'Union européenne a mené un premier exercice paneuropéen visant à tester la capacité de réaction des Etats membres de l'UE et de l'AELE à une cyberattaque. L'opération était organisée par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Outre le secteur de la protection des infrastructures d'information critiques, les autorités de poursuite pénale dans le domaine de la cybercriminalité, les GovCERTs et les régulateurs ont été testés. Quelque 22 pays de l'UE et de l'AELE, dont la Suisse, ont participé à l'exercice. Par ailleurs, huit pays européens étaient présents comme observateurs au Centre de contrôle de l'exercice, situé à Athènes. Plus de 150 experts issus de 70 organisations et agences du service public de toute l'Europe ont collaboré à cette occasion. En Suisse, il s'agissait de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (GovCERT.ch), de la Police judiciaire fédérale ainsi que de l'Office fédéral de la communication (OFCOM). Les pays participants ont été confrontés à plus de 320 incidents. Le scénario de l'exercice prévoyait une paralysie progressive des principales connexions transfrontalières d'Europe. Les Etats membres devaient collaborer afin de prévenir des pannes supplémentaires et de rétablir les liaisons bloquées. L'évaluation portait aussi bien sur la coopération internationale que sur la collaboration nationale entre les divers services responsables de lutter contre les cyberattaques. Il s'agissait principalement d'analyser les canaux de communication, les points de contact et les processus en place sur le plan tant national qu'international. De même, l'exercice visait à tirer un bilan de la gestion des incidents sur le plan européen, dans l'optique d'améliorer les processus d'entraide mutuelle en cas d'incident ou de cyberattaque à grande échelle.

L'exercice Cyber Europe 2010 était la première étape-clé visant à renforcer la cyberdéfense de l'Europe et s'inscrit dans l'engagement accru de l'UE pour améliorer la *protection des infrastructures d'information critiques (PIIC)*. Au printemps 2009, la conférence ministérielle

[2] http://cms.met.police.uk/news/arrests_and_charges/five_arrested_under_computer_misuse_act (état: 10 janvier 2011).

[3] http://www.n-tv.de/politik/Hacker-rufen-zum-Cyber-Krieg-article2110826.html (état: 10 janvier 2011).

[4] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,742298,00.html (état: 10 janvier 2011).

sur la PIIC de Tallinn avait reconnu l'urgence d'optimiser au sein de l'UE les possibilités de défense, la sécurité ainsi que la stabilité de ces infrastructures.

Cet exercice était en son genre une première pour l'Europe. Le simple fait que 22 pays y aient participé constitue un succès. Il est certes encore trop tôt pour en donner une analyse détaillée. Mais on peut déjà dire que la communication a bien fonctionné, entre *CERT* nationaux notamment. Au niveau européen voire mondial, des annuaires de contacts existent d'ores et déjà et des organisations comme le groupe ECG (European Government CERT) sont contactées tous les jours. Les exploitants privés d'infrastructures d'information critiques n'étaient pas impliqués dans ce premier exercice. Leur participation est toutefois prévue dans les futurs exercices.

3.4 «Petites histoires d'Internet» pour une société de l'information plus sûre

Des services de la Confédération et des cantons ont publié conjointement une brochure intitulée «Petites histoires d'Internet – que personne ne voudrait vivre». Des bandes dessinées y racontent des situations dangereuses sur le Web et indiquent comment les reconnaître et les éviter. Les sujets vont de la transmission de données personnelles aux activités criminelles sur Internet, en passant par la protection insuffisante des enfants et des jeunes, les abus dont sont victimes les consommateurs ou encore les ordinateurs et les *réseaux WLAN* non sécurisés. Chaque histoire est accompagnée de liens vers les organisations pouvant fournir de plus amples informations. Le but de cette publication est de renforcer la sécurité et la confiance de la population en matière d'utilisation des technologies de l'information et de la communication (TIC).
Ces histoires, qui s'adressent à la population tout entière, sont publiées en français, allemand, italien, romanche et anglais. Elles peuvent être téléchargées sur Internet ou commandées sous forme de brochures sur papier.[5] Au besoin, elles peuvent également être fournies dans des formats permettant leur publication (mention de la source obligatoire).
La brochure est une mesure d'application du concept Sécurité et confiance, dont le Conseil fédéral a pris connaissance le 11 juin 2010.[6] Ce document présente des mesures conçues afin d'aider la population et les PME à utiliser les TIC de manière légale et sûre. Il a également pour but de renforcer la confiance dans les TIC. Les mesures sont mises en œuvre sous la direction du Bureau de coordination Société de l'information de l'OFCOM, en collaboration avec divers organismes spécialisés.

Internet, les ordinateurs et les téléphones mobiles font désormais partie du quotidien de la population suisse. Or, si Internet présente des avantages, il comporte également des risques. Car contrairement aux coins sombres que l'on repère facilement en marchant dans la rue, sur Internet les lieux dangereux ne sont pas reconnaissables au premier coup d'œil. La brochure, qui aide à identifier les situations à risques sur le Web, a rencontré un vif succès auprès du public. Elle s'utilise dans l'enseignement scolaire comme pour la formation d'adultes, pour la sensibilisation interne aux entreprises, dans les commissariats de police ou pour informer les consommateurs. Rapidement épuisée, la brochure a dû être réimprimée.

[5] http://www.petiteshistoiresdinternet.ch (état: 10 janvier 2011).

[6] http://www.bakom.admin.ch/themen/infosociety/01691/01710/index.html?lang=fr (état: 10 janvier 2011).

3.5 Phishing visant les comptes de messagerie

Les courriels de *phishing* s'en prenant aux fournisseurs de messagerie électronique, dont Swisscom, sont en augmentation depuis décembre 2010. A la différence des attaques antérieures, où la victime était priée d'écrire son nom d'utilisateur et son mot de passe directement dans le courriel et de le renvoyer à une adresse de messagerie falsifiée, les attaques actuelles comportent un lien qui, en cas de clic, renvoie à un site de phishing. Ce site falsifié ressemble à s'y méprendre à l'original et invite à indiquer le nom d'utilisateur et le mot de passe, ainsi que d'autres données personnelles. Cette technique plus sophistiquée a déjà servi contre les prestataires de service financiers. On peut en tirer deux conclusions: d'abord, les victimes potentielles ne réagissent plus (ou alors trop rarement) aux courriels maladroits, ensuite les données d'accès à la messagerie électronique restent très convoitées car elles se vendent aisément.

L'intérêt croissant des cybercriminels pour les données d'accès aux services Internet, et surtout pour les données des cartes de crédit, confirme les propres estimations de MELANI. Les tentatives de phishing visant des fournisseurs de messagerie comme Bluewin, Hotmail, etc. sont en augmentation. Les données d'ouverture de session des administrateurs de sites sont également dérobées pour placer sur les sites des *infections par drive-by download*. Des exemples d'escroqueries commises avec de telles données d'ouverture de session sont décrits dans les rapports semestriels 2009/1[7], au chapitre 3.3 et 2008/2[8], au chapitre 3.6. Par contre, les cas de phishing classique contre les prestataires de services financiers suisses se raréfient. La raison tient à l'introduction d'éléments de sécurité variés dans le e-banking.

On constate que les attaques contre le e-banking avec *authentification à deux facteurs* (phishing classique ou maliciels s'en prenant aux applications de e-banking) et le phishing aux dépens des services Internet uniquement protégés par un nom d'utilisateur et un mot de passe reposent sur différents modèles d'affaires et qu'ils impliquent des groupes criminels différents. Les groupes actifs dans le «simple» phishing s'intéressent aux données d'ouverture de session et pas nécessairement aux escroqueries commises plus tard avec elles. Cela réduit l'énergie criminelle déployée puisque les pirates se contentent de vendre les données, sans participer à l'escroquerie proprement dite. Dans le cas des cyberattaques contre le e-banking, la distinction entre l'acquisition des données d'ouverture de session et l'escroquerie proprement dite disparaît. En effet, l'authentification à deux facteurs ne laisse qu'une petite fenêtre temporelle pour commettre le forfait. Non seulement le processus est plus complexe, mais il faut encore trouver un moyen d'obtenir l'argent escroqué. Il doit être blanchi, ce qui nécessite une importante infrastructure d'agents financiers. D'où la nécessité d'une bonne organisation et surtout d'une bien plus grande énergie criminelle.

De nombreux services Internet sont accessibles par simple introduction du nom d'utilisateur et du mot de passe. En cas d'oubli ou perte de son mot de passe, le client peut en générer un nouveau en cliquant sur le lien «Mot de passe oublié». Il reçoit alors par courriel son nouveau mot de passe. Si un pirate parvient à accéder au compte de messagerie, il pourra aisément utiliser ce service afin d'accéder aux diverses prestations de service utilisées par la victime et d'en abuser à son profit.

[7] MELANI rapport semestriel 2009/1, chapitre 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=fr (état: 10 janvier 2011).

[8] MELANI rapport semestriel 2008/2, chapitre 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=fr (état: 10 janvier 2011).

3.6 Panne d'Internet mobile

Le 9 novembre 2010, un dérangement a affecté le réseau mobile de données de Swisscom. Presque tous les clients de Swisscom ont été privés d'accès mobile à Internet pendant plusieurs heures. Selon cet opérateur, la panne est survenue vers 7h30 sur le réseau *GPRS*, lors de travaux de maintenance. Afin de la résoudre, il a fallu redémarrer le service durant la matinée, opération problématique qui a provoqué cette interruption du trafic mobile des données à grande échelle.[9] Par contre, ni les appels passés sur le réseau mobile, ni l'envoi et la réception de SMS ainsi que les connexions sur le réseau fixe n'ont été touchés. Swisscom a versé dix francs à tous les clients d'Internet mobile, à titre d'indemnisation. Outre la téléphonie mobile, la panne a notamment affecté les terminaux de paiement par carte de crédit et les ordinateurs portables des chefs de train.

L'accès mobile à Internet fait toujours plus partie de notre quotidien, afin p. ex. de consulter rapidement l'horaire du bus, d'acheter un billet ou de télécharger les derniers bulletins d'information. Un dérangement du réseau mobile de données peut obliger à se passer de ces prestations de service, ce qui est sans doute supportable.

Or d'autres prestations de service «plus importantes», comme des terminaux mobiles de cartes de crédit, fonctionnent toujours plus souvent via une connexion mobile à Internet. La situation est plus grave encore pour les installations de commande de l'industrie ou pour les infrastructures d'approvisionnement basées sur l'Internet mobile. Si une perte de connexion devait empêcher leur contrôle à distance, les conséquences seraient dramatiques pour une partie de la population.

3.7 Panne de radio dans l'agglomération bernoise

Le 16 décembre 2010 à 7h15, un automobiliste a perdu le contrôle de son véhicule sur la chaussée verglacée et a percuté un pylône des Forces motrices bernoises (FMB). Cela a suffi à provoquer une panne électrique dans la région. Outre que beaucoup ménages se sont retrouvés sans courant ce matin-là, l'approvisionnement de l'émetteur du Bantiger a été interrompu. Toute l'agglomération bernoise a été temporairement privée de radio et de télévision. Pour éviter une telle mésaventure, la tour émettrice dispose de deux sources d'approvisionnement indépendantes. Par malchance le commutateur permettant, en pareil cas, de passer au circuit électrique de rechange ne fonctionnait pas.

La radio sert à donner l'alarme à grande échelle en cas de catastrophe ou de dérangement. Le concept de protection en cas d'urgence au voisinage des installations nucléaires prévoit qu'en cas d'accident de réacteur, les communes reçoivent par radio les instructions du canton et de la Centrale nationale d'alarme[10] de l'Office fédéral de la protection de la population. Auprès de la population on sait qu'il faut enclencher son poste radio lorsque les sirènes d'alarme retentissent. D'où l'importance de veiller à l'absence de défaillance et à la stabilité du réseau radio. Les stations FM de SRG SSR sont réparties par classes de disponibilité. Les émetteurs importants, telle la station du Bantiger, figurent dans une classe de disponibilité élevée. Le critère déterminant ici est la durée d'interruption maximale

[9] http://www.swisscom.com/GHQ/content/Media/Medienmitteilungen/2010/20101109_MM_Stoerung_Mob_Internet_aufgehoben.htm (état: 10 januar 2011).

[10] http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/dokumente/unterlagen_nat__abc-schutz.parsys.22314.downloadList.26821.DownloadFile.tmp/notfallschutzkonzeptkernanlagenf.pdf , page 8 (état: 10 janvier 2011).

autorisée par incident. Cette dernière vaut pour toute la chaîne d'approvisionnement incluant, outre l'émetteur, la réception des programmes, les commandes de l'émetteur, etc. Par ailleurs, les programmes radio ordinaires ne font l'objet d'aucune prescription en matière d'alimentation de secours. L'Information de la population par la Confédération en temps de crise (IBBK) fait exception, étant soumise à des exigences de protection plus élevées. Elle s'appuie à cet effet sur son propre réseau émetteur d'urgence par radio OUC.

Un tel incident montre d'une façon exemplaire l'importance de réexaminer régulièrement les concepts de protection en cas d'urgence.

3.8 Campagne de *black hat SEO*: domaines en «.ch» visés

L'optimisation d'une page Web pour les moteurs de recherche (search engine optimization, SEO) décrit les mesures visant à favoriser son positionnement parmi les résultats du classement établi par les moteurs de recherche. Elle fait partie du marketing exercé sur les moteurs de recherche. Diverses techniques appelées «*cloaking*», «*keyword stuffing*» ou encore «*hidden text*» (ou *hypertext*) servent à hisser des sites inconnus à la tête des classements établis par les moteurs de recherche, afin d'obtenir une meilleure visibilité et donc un plus grand nombre de visiteurs. La variante éthique, conforme aux directives des moteurs de recherche, porte le nom de «white hat». On parle d'optimisation «black hat» en cas d'usage de méthodes illégales pour tromper les robots d'indexation.

Afin de propager de manière optimale leurs maliciels, les pirates privilégient les sites très fréquentés (voir chapitre 5.5). Un seul site peut ainsi infecter des dizaines de milliers d'ordinateurs. Or les sites les plus consultés sont généralement aussi les mieux protégés (on trouve toutefois dans le Web de nombreuses exceptions qui confirment cette règle). Les techniques de SEO permettent de compromettre des sites Web peu connus (et mal protégés) et de les catapulter en tête des classifications des moteurs de recherche.

En août 2010, une vaste campagne de «black hat SEO» a été menée pour diffuser un *scareware*. Elle s'en est prise à divers domaines suisses[11]. Dès qu'une faille de sécurité était identifiée sur un serveur Web suisse, une redirection (self.location.href) y était placée sous chaque nom de domaine. Les victimes aboutissaient à un site comportant un domaine de premier niveau en «co.cc», qui affichait le message «You're infected» et leur proposait un programme permettant soi-disant de nettoyer leur ordinateur (voir fig.).Si l'on téléchargeait et installait ce programme, c'est là que les problèmes commençaient. La technique consistant à ajouter sur un grand nombre de pages – dans le cas d'espèce des sites piratés – des liens menant au même site porte le nom de *ferme de liens* (linkfarm). Cette technique relève également du «black hat SEO».

[11] Dancho Danchev, expert en sécurité informatique, a analysé la campagne en détail sur son blog: http://ddanchev.blogspot.com/2010/08/dissecting-scareware-serving-black-hat.html (état: 10 janvier 2011).

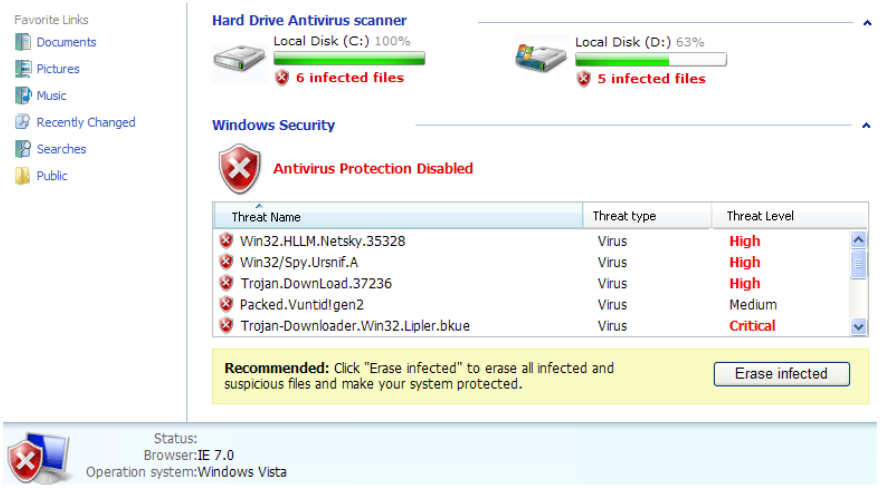

Fig. 1: Les visiteurs de sites en «.ch» compromis sont détournés vers une page prétendant que leur ordinateur est infecté.

Même les sites Web qui, à première vue, ne présentent guère d'attrait pour les escrocs devraient absolument être protégés avec toute la minutie nécessaire. Quiconque utilise un système de gestion de contenu (*content management system,* CMS) comme WordPress, Joomla, Drupal, etc. devrait mettre régulièrement à jour ces applications, pour ne pas laisser le champ libre aux escrocs. De leur côté, les hébergeurs veilleront à accroître la sécurité de leur serveur.

3.9 Lutte contre les sites Web malveillants

Contexte

Les cybercriminels s'en prennent toujours plus souvent aux sites Web légitimes pour y placer des codes malveillants. Ils parviennent ainsi à mettre en ligne des pages de phishing (voir chap. 3.5) ou à infecter discrètement des sites Web (voir chap. 3.13). Dans le second cas, il suffit d'appeler une page manipulée pour s'infecter de *virus* ou de *chevaux de Troie*.

Tout ordinateur ayant accès à Internet est susceptible d'être infecté par des maliciels. Les utilisateurs de Linux et de MacOS auraient donc tort de croire que les virus et les chevaux de Troie sont un problème spécifique à Windows. Même les smartphones font l'objet d'attaques toujours plus fréquentes (voir chap. 5.3).

Mesures prises par MELANI et SWITCH

Depuis la fin de novembre 2010 SWITCH, le registraire gérant les noms de domaine suisses, a redoublé d'activité contre les sites suisses qui diffusent des maliciels et qui infectent les ordinateurs de leurs visiteurs.[12] SWITCH contrôle tout indice montrant qu'un site Web diffuse des logiciels malveillants et contacte le détenteur et le gestionnaire (fournisseur de services Internet) en les priant de régler le problème. Si rien n'a été fait en l'espace d'un jour ouvrable, SWITCH bloque l'adresse Internet durant cinq jours ouvrables au maximum, supprime l'assignation y relative à un serveur de noms et informe MELANI. Si le maliciel n'a

[12] http://www.switch.ch/fr/about/news/2010/malware-nov2010.html (état: 10 janvier 2011).

toujours pas disparu, MELANI peut demander la prolongation de ces mesures pendant 30 jours.[13]

Comme expliqué au chapitre 3.5 du dernier rapport semestriel MELANI[14], ces mesures visent en premier lieu à protéger les internautes et à prévenir les exploitants dont le site a été compromis. Le blocage de noms de domaine constitue un moyen de dernier recours si le titulaire n'a pas nettoyé son site et faute de pouvoir écarter autrement le danger qui en résulte. Expérience à l'appui, la plupart des exploitants sont reconnaissants d'être informés et remettent en état leur site en temps utile. Dans ce contexte, MELANI n'a jamais eu à demander de blocage et ne le fera qu'en dernier ressort, en cas de menace aiguë pour un nombre élevé d'utilisateurs.

Mesures adoptées par d'autres organisations

Comme le problème des sites compromis tend à s'aggraver et les registraires ne sont pas tous aussi zélés que SWITCH, toujours plus d'acteurs s'engagent sur ce terrain, adoptant des mesures et proposant des produits destinés à protéger les internautes. En particulier, les créateurs de navigateurs ont introduit des mécanismes de mise en garde à l'égard des sites potentiellement nuisibles. Quiconque appelle une telle adresse connaît ainsi le risque lié au chargement du site en question. Google signale déjà depuis peu dans les résultats des recherches les sites susceptibles d'être dangereux. En outre, divers fabricants d'antivirus proposent des produits qui, d'une part, signalent les résultats des recherches comme étant sans danger ou problématiques et, d'autre part, mettent en garde contre toute tentative d'appel de sites malveillants.

Toutes ces initiatives et fonctions méritent d'être saluées. En particulier, les mesures de protection incluses dans le navigateur et activées par défaut aident certainement à éviter aux internautes peu expérimentés de s'infecter. Le taux de reconnaissance des sites dangereux est toutefois très variable et les utilisateurs s'en remettant entièrement à un produit donné ont tort de se croire en sécurité. Car comme n'importe quelle mesure de défense contre les contenus Internet nuisibles, aucune solution sur le marché n'offre une protection à 100 %, d'autant plus que les méthodes des pirates évoluent constamment pour déjouer l'identification des codes malveillants infiltrés. Outre les mécanismes de protection proposés par différents prestataires et intégrés dans les navigateurs, sur les sites Internet ou dans les *barres d'outils*, il reste donc indispensable d'installer un antivirus ordinaire (scanneur antivirus) et d'actualiser régulièrement son système d'exploitation et toutes ses applications, afin de réduire au minimum le risque d'infection.

Initiative anti-phishing adoptée par la France

Comme les sites de phishing apparaissent sans crier gare, la vitesse de réaction des filtres antiphishing s'avère cruciale. Typiquement, ce sont les heures suivant l'envoi de courriels contenant un lien à un tel site qui constituent le moment critique. La plupart des navigateurs sont équipés d'une fonction permettant d'annoncer les sites de phishing. Il existe en outre des *barres d'outils* (mises au point par les fabricants d'antivirus ou par des prestataires spécialisés) qui mettent en garde contre de tels sites. Là encore, les utilisateurs ont la possibilité de soumettre un site de phishing découvert par eux. Chaque dénonciation fait l'objet d'une validation et, typiquement, des avertissements sont donnés aussitôt après aux

[13] http://www.admin.ch/ch/f/rs/784_104/a14bist.html (état: 10 janvier 2011).

[14] MELANI rapport semestriel 2010/1, chapitre 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=fr (état: 10 janvier 2011).

internautes. Au début de 2011, Microsoft a lancé avec PayPal et le laboratoire français CERT-LEXSI une initiative visant à lutter contre les attaques francophones de phishing. La population est invitée à soumettre sur un site spécial les URL des sites de phishing.[15]

Comme le temps de réaction varie fortement d'un exploitant et d'un hébergeur à l'autre, aucune possibilité de protection des internautes n'est à négliger. Plus la mise en garde est publiée rapidement, moins il y aura de victimes potentielles. Or compte tenu du nombre élevé de prestataires, dont aucun ne saurait être informé du moindre site problématique, leurs produits ne peuvent mettre en garde contre tous les sites dangereux. Il est faux de croire qu'en utilisant un produit antiphishing, on n'aura jamais affaire à un tel site. Mieux vaut donc ignorer tout courriel invitant à révéler son mot de passe. Autrement dit, il faut toujours considérer d'un œil critique les invitations reçues par courriel à indiquer ou «vérifier» sur un site Web ses données personnelles (mots de passe, informations sur la carte de crédit).

Le fait d'avoir son propre site Web indexé par les filtres antivirus ou antiphishing peut être très désagréable et faire perdre des clients potentiels. Une fois le site remis en état, encore faut-il qu'il disparaisse des listes de filtrage ou d'avertissement. C'est compliqué car outre que l'on ignore dans combien de listes – et lesquelles – l'adresse figure, la prise de contact avec les prestataires n'est bien souvent fructueuse que par le biais de leur produit. Il s'ensuit que lorsqu'un site a été compromis, un long travail doit être effectué pour la réparation de l'incident. Les prestataires ont beau contrôler régulièrement que leurs filtres soient à jour, le cas échéant il faut attendre relativement longtemps pour qu'une inscription soit effacée.

Pour éviter que son propre site ne soit compromis, il est indispensable d'actualiser en permanence ses applications Web. En outre, il est recommandé de surveiller sa propre présence sur le Web pour effacer le cas échéant toute modification abusive – avant de figurer dans les listes de filtrage ou d'avertissement.

3.10 27C3: We come in peace – et piratons ton site Web

Du 27 au 30 décembre 2010, Berlin a accueilli le 27e Chaos Communication Congress, sous la devise «we come in peace».[16] Les participants à cette manifestation organisée par le Chaos Computer Club (CCC) ont notamment analysé toutes sortes de sites Web, à la recherche de lacunes de sécurité. Leur quête a été fructueuse p. ex. avec le site du Grasshopper Club Zurich. Les pirates ont ainsi brièvement remplacé le logo de cette société par celui du FC Zurich. En outre, ils ont publié sur le site des extraits de la base de données de la boutique en ligne et des données concernant les utilisateurs enregistrés.

Dans la nuit du 28 au 29 décembre, le site du GC se présentait de la façon suivante:

[15] http://www.phishing-initiative.com (état: 10 janvier 2011).

[16] http://events.ccc.de/congress/2010/wiki/Welcome (état: 10 janvier 2011).

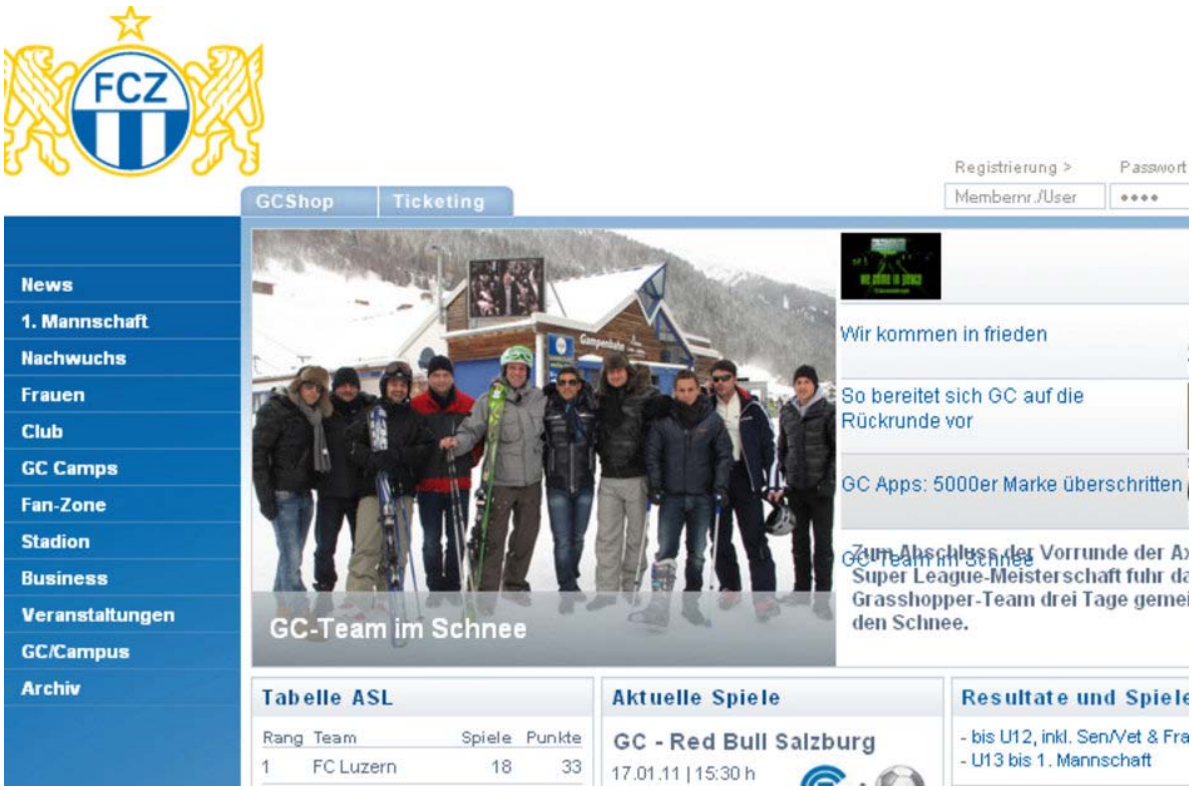

Fig. 2: Site défiguré du GC.

Suite à leur action, les pirates ont envoyé un courriel à tous les abonnés à la newsletter du GC (dont l'adresse figurait dans l'une des banques de données pillées), pour leur signaler la protection insuffisante de leur site.


We Come In Peace

Es ist Zeit dem Verein "uf de andere siite vo de Gleis" lebewohl zu sagen und das Spielfeld den echten Profis freizugeben.

Es ist tagisch, immer wenn ein Verein oder eine Seite aus dem Internet verschwindet, stirbt mit ihm ein Stueck Geschichte....
Um diesem auszuweichen, haben wir eine Sicherung der Datenbank der Shops und der Userdaten erstellt. - gern geschehn :)

Was vielleicht auch noch ganz informativ ist:

Dieses typo3 CMS ist so unfassbar scheisse. ich koennte pausenlos kotzen.
FCZ wird natuerlich wieder Meister und gcz wird abstreiten dass die Datenbank mit allen Benutzerdaten uA der Shops verloren gegangen sind.
Kann ja passieren, nicht jeder ist so fit mit Moderner technik. und so Datenbanken gehn nunmal einfach verloren, ist ja auch schon anderen grossen Firmen passiert. solange keine Kreditkarteninformationen in der Datenbank gesp... moment...

Fig. 3: Courriel adressé par les pirates aux abonnés à la newsletter du GC.

Comme les mots de passe figuraient sans cryptage dans la banque de données piratée, MELANI recommande aux utilisateurs du site de changer immédiatement de mot de passe.

MELANI recommande en outre de choisir des mots de passe différents pour chaque service Web, afin d'éviter que suite à une telle panne, des pirates ne puissent usurper l'identité de leurs victimes. En particulier, quand l'identifiant est l'adresse électronique, il ne faudrait JAMAIS utiliser le même mot de passe que pour son compte de messagerie. En effet, si les pirates sont mal intentionnés, ils s'empresseront de chercher à ouvrir la boîte de messagerie à l'aide du mot de passe dérobé; puis ils essaieront d'accéder à différents réseaux sociaux.

D'autres failles de sécurité ont été repérées sur des sites de partis politiques, de groupes d'extrême-droite, d'aéroports, de médias, d'offices gouvernementaux, etc.[17] Les pirates se sont notamment permis une plaisanterie aux dépens de la première chaîne de télévision allemande, en y publiant la fausse nouvelle ci-dessous:

Fig. 4: Site compromis, avec une fausse nouvelle, de la première chaîne de télévision allemande.

3.11 Etude évaluative de l'initiative suisse anti-Botnet

Il est possible de louer les services d'un réseau de zombies pour quelques dollars par jour, le prix final variant en fonction de la puissance de frappe et de la durée d'intervention souhaitée. Il n'est donc guère étonnant qu'aujourd'hui, les réseaux de zombies soient à l'origine de la plupart des activités criminelles commises dans Internet.

Une lutte fructueuse contre les réseaux de zombies nécessite une étroite collaboration entre les fournisseurs d'accès à Internet, l'Etat et, le cas échéant, le Ministère public. MELANI a donc chargé à la fin de 2010 l'école d'ingénieurs de Zurich de mener une étude évaluative. Il s'agit de montrer sous quelle forme une telle collaboration serait possible et dans quelle mesure les initiatives déployées à l'étranger (p. ex. botfrei.de[18]) pourraient être adaptées en Suisse. L'étude s'achèvera à la fin de juin 2011.

3.12 Chef de projet pour la défense cybernétique

Le 10 décembre 2010, le Conseil fédéral a examiné de près la menace que font peser sur la Suisse les attaques cybernétiques et les contre-mesures envisageables. Il a décidé de renforcer les mesures de protection contre de telles attaques dirigées contre la Suisse. A cet

[17] http://events.ccc.de/congress/2010/wiki/Hacked (état: 10 janvier 2011).

[18] Le Centre de conseil anti-Botnet est un service de l'association de l'économie internet allemande eco qui bénéfice du soutien de l'Office fédéral de la sécurité des technologies de l'information (BSI). https://www.botfrei.de/ (état: 10 janvier 2011).

effet, le Conseil fédéral a nommé pour une durée déterminée Kurt Nydegger, ancien chef de la Base d'aide au commandement de l'armée, au poste de chef de projet pour la défense cybernétique. Il dirigera un groupe d'experts chargé d'élaborer, d'ici la fin de 2011, une stratégie globale de la Confédération contre les menaces cybernétiques.[19]

3.13 Serveur OpenX

Diverses infections de sites Web enregistrées l'année dernière provenaient de failles de sécurité au niveau des serveurs de publicité (*ad server*). Ainsi, le serveur de publicité *open source* OpenX a présenté pendant toute l'année dernière des lacunes de sécurité, qui ont permis à un pirate de se procurer des droits d'administrateur[20]. Comme les mises à jour servant à combler de telles lacunes de sécurité ne sont pas automatiquement activées, les administrateurs Web doivent faire preuve de vigilance. C'est ainsi qu'en juin 2010, des experts en sécurité ont mis en garde à différentes reprises contre les anciennes versions d'OpenX, où les mises à jour tardaient parfois à être effectuées.[21]

En Suisse aussi, les *failles de sécurité* d'OpenX constatées en 2010 ont provoqué de nombreuses infections, dont celle du site Web d'un grand journal suisse. En l'occurrence, un maliciel avait pris place dans la publicité accompagnant l'édition en ligne. Il est bien clair que l'infection de ce genre de sites porte beaucoup plus à conséquence que pour un site Internet privé (voir aussi chapitre 5.5).

	200
hxxp://openx /www/delivery/ajs.php?zoneid=3&source=hxxp://www. .ch&cb= &loc=hxxp://www .ch&referer=hxxp://www .ch	200
about:blank	200
hxxp://www.dhfyjrud321.com/tds/in.cgi?default	**200**
hxxp://www.nbvhhdtn321.com/tds/in.cgi?8	**302**
hxxp://korkonvasiliy.com/hehehe/index.php?s=c4de1af395e576f5156ba255734c26c9	**302**
hxxp://korkonvasiliy.com/hehehe/404.php	**200**

Fig. 5: Protocole de connexion d'une infection provoquée par l'édition en ligne d'un journal suisse.

Comme le montre le protocole de connexion, le visiteur du site du journal a été redirigé sur le serveur «dhfyjrud321».com, où les pirates ont tenté d'exploiter diverses vulnérabilités de son *navigateur* et de ses *applications.* En outre, un *cookie* a été installé pour que l'infection ne soit visible qu'à la première visite. Cette technique complique tant le travail d'analyse des experts en sécurité que l'identification et la réparation des erreurs par l'administrateur de site.

Les infections de sites Web sont en ce moment le vecteur de diffusion de *maliciels* le plus répandu. Les serveurs centraux, mettant du contenu à disposition de différents sites Web, jouent ici un rôle central. Dans le cas de la publicité en ligne notamment, mais aussi des services statistiques, la moindre page compromise peut être lourde de conséquences.

[19] http://www.news.admin.ch/message/index.html?lang=fr&msg-id=36731 (état: 10 janvier 2011).

[20] http://www.heise.de/security/meldung/Ein-Jahr-alte-Luecke-gefaehrdet-OpenX-Ad-Server-1077941.html (état: 10 janvier 2011).

[21] http://news.softpedia.com/news/OpenX-Based-Malvertising-Attack-Discovered-145903.shtml (état: 10 janvier 2011).

La manière dont les annonceurs et autres fournisseurs de contenus en ligne utilisent le logiciel choisi par eux revêt donc une très grande importance. Là encore, tous les programmes doivent être constamment actualisés. Le cas échéant, un site ne peut prétendre offrir une plus grande sûreté que celle de son maillon faible. Et bien souvent, il s'agit d'offres de tiers, de contenus injectés sur le site et échappant de ce fait à tout contrôle de l'exploitant.

4 Situation internationale de l'infrastructure TIC

4.1 Stuxnet – attaque visant des systèmes de contrôle dans l'industrie

Un nouveau *ver informatique* a été découvert à la mi-juin 2010. Transmis par *clé USB*, il parvenait à infecter un système Windows 7 entièrement à jour. C'était possible dans la mesure où il intègre notamment deux pilotes équipés de fonctions *Rootkit* et munis des *signatures numériques* ordinaires, quoique probablement volées, de deux entreprises différentes, ce qui lui permettait de s'installer dans le système sans mise en garde. Personne ne se doutait alors que ce virus éclipserait tous les autres en 2010.[22] Des analyses ont montré qu'il utilisait, pour se diffuser, les lacunes de sécurité déjà exploitées par le ver Conficker et plusieurs failles de Windows n'ayant pas encore été corrigées. Le ver Stuxnet peut se propager par le gestionnaire d'impression (spooler) et par les réseaux partagés, et il possède en outre une composante poste à poste (*peer-to-peer, P2P*) lui permettant d'effectuer des mises à jour réciproques avec d'autres systèmes infectés du même réseau. De cette manière, Stuxnet peut s'actualiser même au sein des réseaux privés d'accès à Internet, dès qu'une version plus récente fait son apparition.

Outre qu'il cherche à exploiter dans Windows quantité de vecteurs d'infection, Stuxnet renferme un code lui permettant de manipuler des applications servant à la programmation des systèmes de contrôle industriel (soit les *automates programmables industriels, API* – en anglais *programmable logic controllers, PLC*). Ces applications sont infectées par Stuxnet, qui parvient ainsi à se propager et à contaminer des API. Stuxnet touche déjà ici à son but, soit entraver le fonctionnement de certains API. Ce n'est que si un système remplit certains critères spécifiques que Stuxnet déploie l'effet prévu et manipule le processus en cours. Stuxnet dissimule sa présence non seulement dans les systèmes Windows, mais aussi dans toutes les autres composantes attaquées. A titre d'exemple, la configuration d'origine des API est sauvegardée pour qu'en cas de manipulation, le programme affiche non pas le code modifié mais une configuration en apparence intacte. De même, les données communiquées par les API aux systèmes de surveillance pendant la phase d'exploitation sont modifiées pour ne pas révéler le sabotage de l'installation concernée.

Le mode opératoire sophistiqué de Stuxnet reste unique à ce jour. Autre particularité de ce virus, il se montre très sélectif et n'infecte pas tous les systèmes, mais seulement ceux possédant des caractéristiques spécifiques. La programmation ne vise pas à utiliser les ordinateurs capturés pour toutes sortes d'activités cybercriminelles ou à endommager des systèmes informatiques. Stuxnet cherche au contraire à identifier des systèmes bien précis,

[22] http://www.heise.de/thema/Stuxnet; http://www.spiegel.de/thema/stuxnet/; (état: 10 janvier 2011) http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html; (état: 10 janvier 2011) http://www.symantec.com/business/theme.jsp?themeid=stuxnet; (état: 10 janvier 2011); http://www.langner.com/en/blog (état: 10 janvier 2011).

lui permettant d'attaquer et de manipuler des systèmes spécifiques. Stuxnet a servi à mener une attaque très ciblée.

4.2 Wikileaks

La plate-forme de divulgation (whistleblowing) Wikileaks a commencé à occuper les esprits bien avant 2010. Depuis 2007, Wikileaks offre aux internautes du monde entier la possibilité de lui transmettre anonymement des documents confidentiels, censurés ou à caractère non public. Wikileaks les soumet à un examen qui, à l'en croire, satisfait aux principes éthiques et aux règles déontologiques du journalisme, puis les publie tout à la fois dans une version récrite en style journalistique ou simplement commentée, ainsi qu'à l'état brut. La démarche est relativement simple: la publication simultanée d'articles et de sources documentaires vise à réaliser une transparence maximale. En ce sens, Wikileaks ne procède pas à une sélection interne des informations reçues, mais publie tout après un premier tri. Le lecteur doit ainsi pouvoir décider lui-même s'il souhaite ou non prêter foi aux informations proposées. L'idée est de le préserver de l'arbitraire d'un média fonctionnant selon les principes classiques, et donc qui présélectionne les histoires et décide lui-même lesquelles il publiera au bout du compte, sur la base de réflexions à caractère journalistique, éthique ou commercial.

Les incidents des six derniers mois liés à la publication progressive par Wikileaks de quelque 250 000 dépêches du Département d'Etat américain ont mis en lumière plusieurs problèmes distincts. Tout d'abord, un nouveau débat portant sur les médias et l'éthique s'est concentré cette fois sur l'acceptabilité de la démarche consistant à livrer purement et simplement au public des documents classifiés, au nom du principe de l'information complète. La question des intentions et motifs de Julian Assange, (co)fondateur de Wikileaks, a également joué ici un rôle. Que penser de la focalisation des activités de Wikileaks sur la personne d'Assange, des priorités établies par Wikileaks en matière d'information, contrairement à son propre credo, ainsi que du choix sélectif effectué par Assange de quelques maisons d'édition autorisées à collaborer et auxquelles ont été accordés des droits exclusifs, en flagrante contradiction avec l'idée première de Wikileaks? Il s'agit là toutefois d'une discussion touchant à l'éthique des médias et à la philosophie, qui n'a pas sa place ici.

Dans ce contexte, deux événements relèvent clairement de la sûreté de l'information. D'une part, il importe de savoir comment 250 000 dépêches diplomatiques classifiées ont pu parvenir jusqu'à Wikileaks. On ignore toujours si une seule personne ou plusieurs sources ont fourni ces documents et d'autres encore. Il semble toutefois que les autorités gouvernementales américaines aient volontairement pris de gros risques, par souci d'une mise en réseau meilleure et plus efficace. Ainsi, des documents possédant toutes sortes de niveaux de classification semblent avoir figuré sur le même réseau sécurisé, auquel un nombre élevé d'utilisateurs possédaient des droits d'accès relativement étendus. Si ces soupçons devaient se confirmer, le vol de documents serait un exemple classique de stratégie inadaptée en matière de sûreté de l'information, thème déjà abordé à plusieurs reprises dans les rapports semestriels de MELANI[23]. L'enjeu concret est de ne pas se limiter à garantir la sécurité des canaux d'information, des supports de sauvegarde des données et des réseaux. Compte tenu de la valeur spécifique de telle ou telle information, il faut au contraire introduire des mesures de sûreté plus poussées, dans le cadre d'un processus bien informé de gestion des risques. Une stratégie à caractère purement technique qui, selon une

[23] MELANI, rapports semestriels 2009/1, chapitre 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=fr (état: 10 janvier 2011) et 2009/2, chapitre 5.1 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=fr (état: 10 janvier 2011).

approche «one size fits all», ne comporterait ni restrictions spécifiques, ni droits d'accès personnalisés et dûment gérés en fonction de la valeur effective de telle ou telle information, aboutira fatalement à une perte totale des informations en question.

D'autre part, et il s'agit du second incident lié à Wikileaks, il y a eu la mobilisation lancée par Anonymous Operation et visant expressément à punir virtuellement les ennemis présumés de Wikileaks. L'épisode est décrit au chapitre 3.2.

Les incidents se rapportant à la publication de documents par Wikileaks sont révélateurs des nombreux problèmes posés par la sûreté de l'information. La remise à des tiers de documents classifiés constitue un défi croissant pour les TIC. Bien souvent, on néglige la sûreté en profondeur des informations, en se contentant de perfectionner au mieux l'environnement technique. Or cette approche crée un gros risque et ne tient compte ni de la problématique du délit d'initié, ni du fait que les informations n'ont pas toutes la même valeur et donc qu'il faut veiller à protéger de façon optimale en premier lieu les informations confidentielles et non le réseau sur lequel elles sont archivées.

Les actes de représailles ayant suivi le débat sur Wikileaks rappellent à quel point les institutions et les particuliers sont vulnérables et les cyberattaques comportent presque toujours un risque de dommages collatéraux, à l'instar des actions menées en Suisse contre des exploitants de sites pornographiques[24]. Quant aux attaques dont PostFinance a fait l'objet, qui relèvent clairement du code pénal, elles montrent que leurs auteurs n'ont guère été sensibilisés à la gravité de leurs actes et qu'ils méconnaissent le droit. L'intervention dans plusieurs pays des autorités de poursuite pénale contre les complices de telles cyberattaques mérite donc d'être saluée.

4.3 SSL et authentification à deux facteurs – sécurité pour sa propre clientèle

En octobre 2010, le programmeur Eric Butler a publié sur son site une extension très intéressante du navigateur Firefox, appelée Firesheep[25].
A la conférence annuelle Toorcon de San Diego, Butler a analysé[26] le risque provenant des promoteurs du *Web 2.0*, à commencer par Facebook. A chaque accès à un site comme Facebook, le serveur génère un témoin de connexion (cookie) contenant les nom et mot de passe de l'utilisateur.

En l'absence de communication cryptée avec son destinataire et si l'utilisateur se sert d'un réseau public sans fil, p. ex. s'il se trouve avec son ordinateur portable dans un bâtiment public (hôtel, restaurant, aéroport, etc.) ou à une conférence où un tel réseau est proposé, le cookie généré risque d'être volé et utilisé pour usurper l'identité de l'utilisateur. L'expression technique utilisée ici est *sidejacking*. Pour se prémunir contre ce genre d'attaque, une liaison cryptée doit être établie entre l'utilisateur et son destinataire. Google a réglé le problème dès janvier 2010 dans son service de messagerie (Gmail). Facebook, site n° 1 en 2010, ne l'a toujours pas fait.

[24] MELANI rapport semestriel 2009/2, chapitre 3.3
http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=fr (état: 10 janvier 2011) .

[25] http://codebutler.com/firesheep (état: 10 janvier 2011).

[26] http://codebutler.github.com/firesheep/tc12/#1 (état: 10 janvier 2011).

Pour prouver à quel point le *sidejacking* est aisé à pratiquer, Butler a publié Firesheep. Une fois cette extension installée, il suffit de se connecter à un réseau sans fil ouvert, de lancer l'application et d'attendre qu'un utilisateur se connecte à Facebook. Il ne reste plus qu'à dérober le cookie généré pour accéder à Facebook, avec le compte de sa victime. Comme il est punissable d'agir de la sorte avec les comptes de tiers, l'usage de Firesheep est vivement déconseillé.

Le scénario ci-dessus illustre un problème connu de longue date. Jusque-là, il fallait toutefois disposer de certaines connaissances pour dérober un cookie. Avec Firesheep, c'est devenu un jeu d'enfant. Les utilisateurs se connectant à Internet via un réseau public sans fil veilleront donc à consulter uniquement des sites fonctionnant selon le protocole *SSL*. Il incombe aux entreprises d'offrir cette prestation, que l'utilisateur ne peut introduire lui-même. Par ailleurs, MELANI signale une recrudescence des attaques visant les prestataires Internet se limitant à un seul facteur d'authentification. Cela vaut par exemple pour les sites d'enchères en ligne, pour les comptes de messagerie et pour divers systèmes de paiement. D'où l'importance de signaler aux entreprises qu'une authentification à deux facteurs réduit le risque de voir leur site compromis. Une telle mesure leur permet de surcroît, ainsi qu'à leur clientèle, d'éviter des pertes substantielles.

4.4 Incidents liés au négoce des droits d'émission

Dès le début de l'année 2010, les sites des registres d'échange de quotas d'émissions ont fait l'objet d'attaques de phishing, consistant à transférer de manière illicite des droits d'émission.[27] L'une des entreprises lésées a poursuivi en dommages-intérêts la République fédérale allemande, faisant valoir que les normes de sécurité de l'autorité compétente laissaient à désirer.[28]
L'organisme allemand chargé des échanges de quotas d'émissions de carbone (Deutsche Emissionshandelsstelle, DEHSt) a annoncé, dans un communiqué daté du 16 novembre dernier, que le registre des émissions de CO_2 serait doté d'un mécanisme d'*authentification à deux facteurs* via smsTAN.[29]

Le même jour, la filiale roumaine d'un cimentier suisse a subi un transfert non autorisé de 1,6 million de certificats d'émission émanant du Registre national roumain. Des escrocs avaient espionné les données d'accès de cette société à l'aide d'un cheval de Troie. Le maliciel utilisé, portant le nom de Nimkey, sévissait surtout jusque-là contre la clientèle des banques américaines. Or ses propriétés (p. ex. vol de certificats numériques privés, enregistrement des frappes au clavier, copie des données archivées) se prêtent également à l'interception d'informations portant sur l'accès à d'autres services – a fortiori si elles se limitent à un nom d'utilisateur et à un mot de passe. L'apparition dans ce contexte de Nimkey a conduit divers registres européens d'échange de quotas d'émissions à suspendre provisoirement toutes leurs activités en novembre.

Début décembre, de nombreuses entreprises ont reçu de l'European Climate Registry un courriel les invitant à ouvrir un compte sur un site Web, soit à y valider leurs données d'ouverture de session. La Commission européenne et les registres nationaux ont pris leurs

[27] Voir MELANI rapport semestriel 2010/1, chapitre 4.9 http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=fr (état: 10 janvier 2011).

[28] http://www.heise.de/security/meldung/Datenklau-bei-Emissionsrechten-kommt-vor-Gericht-1098072.html (état: 10 janvier 2011).

[29] http://www.dehst.de/cln_153/nn_1662430/SharedDocs/Mailings/DE/2010/10-11-16__smsTAN.html (état: 10 janvier 2011).

distances, rappelant qu'il s'agit non pas d'un registre officiel mais d'une simple offre de droit privé, et qu'ils ne pouvaient donc pas juger de son sérieux et de son utilité – le site est toujours en ligne.[30]

La Commission européenne vise à accroître les normes de sécurité des registres d'échange de quotas d'émissions. Dans une phase ultérieure, il est prévu de consigner tous les échanges dans un seul registre communautaire.[31] En attendant leur fusion, les registres nationaux sont tenus d'offrir une protection suffisante et d'introduire des procédures plus sûres. Certains l'ont déjà fait.

Comme indiqué dans des rapports semestriels antérieurs[32], on constate que les attaques cybercriminelles se reportent toujours plus des services de e-banking sur des services ou plates-formes (de négoce) moins bien protégés. La menace est d'autant plus grande que les services ont pour seule protection un nom d'utilisateur et un mot de passe et qu'ils permettent, directement ou indirectement, de gagner de l'argent. Outre le négoce des droits d'émission, les escrocs s'intéressent aux systèmes de paiement en ligne, aux plates-formes de vente aux enchères, aux fournisseurs de messagerie et aux réseaux sociaux.

4.5 Cyberdéfense et nouveau concept stratégique de l'OTAN

Du 16 au 18 novembre 2010, l'OTAN a mené un exercice intitulé Cyber Coalition 2010.[33] Les tests portaient sur les procédures et la coordination entre les divers acteurs chargés d'intervenir en cas de cyberattaque contre l'OTAN et ses Etats membres. Il s'agissait du troisième exercice du genre.

Au sommet de l'OTAN de Lisbonne, organisé les 19 et 20 novembre 2010, les chefs d'Etat et de gouvernement des Etats membres ont adopté pour le Traité de l'Atlantique Nord un nouveau concept stratégique, assimilant les cyberattaques à une menace sérieuse. L'OTAN vise à développer systématiquement son aptitude et celles de ses membres à prévenir et détecter les cyberattaques, à s'en défendre et à s'en relever. Il est également prévu de renforcer et de mieux coordonner les capacités nationales de cyberdéfense. De même, il s'agit de développer la capacité des Etats à contribuer à leur propre sécurité énergétique, y compris par la protection des infrastructures énergétiques critiques.

Une question n'a toutefois pas trouvé de réponse au sommet de Lisbonne, à savoir s'il faut assimiler – et le cas échéant quand – les cyberattaques à des attaques armées qui requièrent une réaction groupée (casus foederis) en vertu de l'art. 5 du Traité de l'OTAN. Il est prévu d'élaborer d'ici juin 2011 la politique OTAN de cyberdéfense, de même qu'un plan de travail destiné à renforcer les cybercapacités.

Dans les langues officielles de l'OTAN, soit l'anglais et le français, il est question de cyberdéfense («cyber defence»), terme que la Représentation permanente de l'Allemagne auprès de l'OTAN a choisi de traduire par protection contre la cybercriminalité («Schutz vor

[30] Le European Climate Registry avait envoyé un courriel analogue en été 2009. Le domaine «europeanclimateregistry.eu» est enregistré depuis décembre 2008 au nom d'une personne domiciliée à Bruxelles.

[31] Directive 2009/29/CE du 23 avril 2009, point 38.

[32] Voir par exemple: MELANI rapport semestriel 2008/2, chapitre 3.6 http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=fr (état: 10 janvier 2011).

[33] http://www.nato.int/cps/en/SID-70CABE49-11886860/natolive/news_69805.htm

Computerkriminalität») dans la déclaration finale du sommet et dans le concept stratégique.[34] Cela pourrait être un indice que les parties au Traité ne se sont pas (encore) mises d'accord sur la réaction adéquate à une cyberattaque – militaire ou peut-être plutôt civile. Nul ne conteste en revanche que l'armée doive être en mesure de protéger ses infrastructures.

4.6 Essor des vers USB

Les supports de données *USB* rencontrent un succès croissant comme moyen de propagation de logiciels malveillants. Stuxnet[35] et Conficker[36] ne sont ici que la pointe de l'iceberg. Les clés et périphériques USB sont toujours meilleur marché et leur usage toujours plus fréquent. En outre, beaucoup de systèmes informatiques sont moins bien protégés contre les vers USB que, par exemple, contre ceux diffusés par le Web ou par messagerie électronique. Selon l'entreprise espagnole Panda Security, 25 % des vers ayant fait leur apparition en 2010 étaient conçus pour se propager via USB[37]. Ce constat ressort d'une étude menée auprès de 10 470 entreprises implantées en Europe, en Amérique du Nord et en Amérique latine. Il faut dire que de nombreux postes de travail ont omis de désactiver le fichier autorun.inf, qui permet aux programmes de démarrer automatiquement. Cette fonction rend aisée l'installation des maliciels, dès que le périphérique USB est raccordé à l'ordinateur.

La plupart du temps, le ver USB est associé à d'autres vecteurs d'infection. Le support USB sert en premier lieu à franchir le pare-feu des entreprises. Une fois le maliciel introduit dans le réseau de l'entreprise, les obstacles à sa propagation seront bien moindres.

Pour juger des conséquences que peut avoir une clé USB privée, il suffit de repenser au maliciel qui, en 2008 est parvenu à s'introduire dans le réseau du Pentagone. Au Moyen Orient, un soldat avait branché une clé USB infectée à un ordinateur faisant partie du réseau militaire américain. De là, le maliciel s'est propagé par de nombreux réseaux internes, avant d'accéder à un domaine protégé du réseau.[38] Le virus Conficker a lui aussi circulé dans divers réseaux d'entreprises, infectant des hôpitaux et des réseaux militaires.

Les supports de stockage USB sont un vecteur de propagation des virus particulièrement adapté aux entreprises, ce qui les rend dangereux. Entre-temps, toutes les entreprises ont adopté de bonnes méthodes de défense de leurs réseaux et dans la plupart des cas, la messagerie électronique fait également l'objet d'une surveillance antivirus centralisée. Or si un virus parvient à s'introduire dans le réseau d'une entreprise en contournant son pare-feu, via une clé USB branchée sur l'ordinateur d'un collaborateur, il a ensuite le champ libre. Il s'agit ainsi d'un vecteur adéquat pour les attaques ciblées et notamment contre les systèmes bien isolés. La probabilité qu'un collaborateur connecte une fois une clé ou un autre appareil USB (appareil photo, smartphone, etc.) tant sur son ordinateur privé que sur celui du travail est réelle. Or même les contrôles en amont des clés USB par plusieurs antivirus ne garantissent pas une protection complète, sachant que les antivirus échouent généralement face aux maliciels diffusés en petites quantités dans le cadre d'attaques ciblées.

---

[34] http://www.nato.diplo.de/Vertretung/nato/de/04/NATO__Gipfel__Lisboa__1911_Seite.html (état: 10 janvier 2011).

[35] Voir chap. 4.1 et 5.1 du présent rapport.

[36] Voir http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=fr, chapitre 4.2 (état: 10 janvier 2011).

[37] http://press.pandasecurity.com/news/25-of-new-worms-in-2010-are-designed-specifically-to-spread-through-usb-devices/ (état: 10 janvier 2011).

[38] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (état: 10 janvier 2011).

4.7 Ver informatique «Here you have» – Iraq Resistance

Le 9 septembre 2010, un ver informatique inconnu a commencé à se propager sur Internet et a perturbé la messagerie de plusieurs entreprises américaines. Il envoyait des courriels ayant pour objet «Here you have» et pour texte «This is The Document I told you about, you can find it Here», ou alors une variante intitulée «Just For you» avec pour texte «This is The Free Download Sex Movies, you can find it Here». Or le «Here» contenait à chaque fois un lien au code malveillant. Le lien avait beau prétendre renvoyer à un document ou fichier vidéo, les victimes cliquant sur le lien chargeaient en réalité le maliciel sur leur ordinateur, puis étaient priées d'exécuter le fichier correspondant. Le ver se diffusait par la suite en utilisant les droits d'accès et envoyait le courriel muni du lien malveillant à tous les contacts du carnet d'adresses. Au-delà de sa diffusion et des courriels ainsi générés, qui ont pu surcharger certains serveurs, le ver ne commettait toutefois aucun dégât particulier.

Une personne se faisant appeler Iraq Resistance (*nickname*, pseudonyme) et prétendant faire partie du groupe jusque-là inconnu Tariq bin Ziyad Brigades for Electronic Attack (TbZBEA) a revendiqué la paternité du virus. Son but n'était toutefois pas de causer un maximum de dégâts. Dans son message de revendication publié sur YouTube, le pirate a souligné ne pas être un terroriste.[39] L'action devait être comprise comme une protestation: d'abord contre l'invasion américaine de l'Irak, ensuite contre l'annonce du projet de brûler des exemplaires du Coran le 11 septembre 2010 aux Etats-Unis (projet abandonné, mais pour d'autres raisons).

La méthode consistant à dérober les données du carnet d'adresses des systèmes infectés et à envoyer des courriels invitant à cliquer sur un lien est une forme simple mais éprouvée de subversion psychologique (*social engineering*). Les courriels inspireront d'autant plus confiance que leur expéditeur est connu et que le texte de son message est suffisamment général pour paraître plausible à un grand nombre de destinataires.
En 2000 (virus I LOVE YOU) et en 2001 (virus Anna Kurnikova), des vers informatiques similaires, recourant à des méthodes analogues pour se propager, avaient été mis en circulation. Par conséquent, une règle élémentaire consiste à traiter avec prudence les courriers électroniques non attendus (même lorsque l'expéditeur est connu) et comportant des liens ou des annexes et, en cas de doute, à demander à l'expéditeur de quoi il s'agit. Ces derniers temps, les documents PDF envoyés en pièces jointes ont constitué un vecteur d'infection toujours plus prisé. Or le simple fait de cliquer sur un lien aboutissant à une page spécialement préparée ou d'ouvrir un fichier est susceptible d'infecter un système.

Ce ver baptisé Here you have avait été envoyé dans le cadre d'une cyberprotestation à mobiles politiques et religieux. Si en plus de son mécanisme de propagation il avait renfermé des instructions visant à corrompre de nombreuses données, l'affaire aurait été beaucoup plus grave pour certaines entreprises.

4.8 Désactivation par la police néerlandaise d'un vaste réseau de zombies

Lundi 25 octobre 2010, la police néerlandaise a bloqué les serveurs de contrôle du réseau de zombies Bredolab. Plus de 30 millions d'ordinateurs auraient été infectés. La police a déconnecté au total 143 serveurs ayant servi à piloter Bredolab. En parallèle, un individu de

[39] http://www.youtube.com/watch?v=IkMifFGqt78 (état: 10 janvier 2011).

27 ans a été arrêté à l'aéroport d'Erevan. Il est soupçonné d'être le cerveau des opérations. Les enquêteurs avaient analysé en détail l'infrastructure du réseau au cours des semaines précédentes.

L'exploitant du réseau visait avant tout à répandre un maliciel. A cet effet, il misait sur les infections de sites Web. Après avoir infecté un ordinateur, son maliciel y recherchait le nom d'utilisateur et le mot de passe des administrateurs de sites. Les données trouvées étaient utilisées à leur tour pour infecter d'autres sites Web. Le processus était entièrement automatisé. Les serveurs entre-temps désactivés étaient gérés par l'exploitant néerlandais Leaseweb. En règle générale, les serveurs sont coupés du réseau aussitôt après leur découverte. Dans le cas d'espèce, Leaseweb a toutefois poursuivi ses activités sur ordre de la police, pour lui permettre d'analyser le réseau.

Le ou les pirates avaient pour spécialité de générer le plus vaste réseau de zombies possible, afin de pouvoir en louer ou vendre certaines parties. Comme Bredolab est un programme de téléchargement (downloader), il peut ensuite introduire n'importe quel virus sur l'ordinateur infecté.

MELANI a déjà signalé, dans une lettre d'information du 9 avril 2010, l'existence de ce virus et le risque accru de voir son ordinateur infecté lors de la simple visite d'un site Internet[40]. Le récent outil de contrôle des sites Web exploité par MELANI pour vérifier si les sites en «.ch» sont infectés avait décelé un grand nombre de victimes de Bredolab. Les exploitants ou fournisseurs d'accès ont été contactés par la suite, afin d'éliminer les infections constatées.

La police néerlandaise a opté pour une approche inédite afin de mettre en garde les utilisateurs d'un ordinateur infecté. Elle se sert des serveurs Command & Control, afin d'afficher à l'écran des machines en question une fenêtre contextuelle (*pop-up*) contenant un message d'avertissement.

4.9 ZeuS et SpyEye – fusion des principaux chevaux de Troie du e-banking?

Le cheval de Troie ZeuS est probablement le principal maliciel à s'en prendre aujourd'hui aux applications de e-banking. De nombreux rapports, articles et activités ont été consacrés à la question[41].

Dès le début de 2010, un autre maliciel spécialisé dans le e-banking et portant le nom de SpyEye a fait parler de lui. Une fonction appelée ZeuS Killer Code lui servait à déterminer si un ordinateur à infecter accueillait déjà ZeuS. Le cas échéant, le rival était éliminé. D'où une véritable guerre entre ces deux chevaux de Troie. L'auteur de SpyEye, connu sous les pseudonymes de Gribodemon et Harderman[42], est devenu célèbre par la suite dans les forums clandestins en annonçant, en juillet dernier, que l'auteur de ZeuS lui avait cédé le code de son maliciel ainsi que la gestion de sa clientèle:

---

40 http://www.melani.admin.ch/dienstleistungen/archiv/01107/index.html?lang=fr (état: 10 janvier 2011).

41 Le site de Brian Krebs, journaliste spécialisé dans la cybercriminalité, renfermait p. ex. quinze articles consacrés aux exactions commises par ZeuS au semestre écoulé: http://krebsonsecurity.com (état: 10 janvier 2011). Le site https://zeustracker.abuse.ch/ (état: 10 janvier 2011) répertorie plus de 500 C&C ZeuS, dont le taux d'identification moyen par les principaux antivirus se situe à 36,85 %.

42 Une interview de cette personne est publiée sur le blog MalwareIntelligence: http://www.malwareint.com/docs/spyeye-analysis-ii-en.pdf (état: 10 janvier 2011).

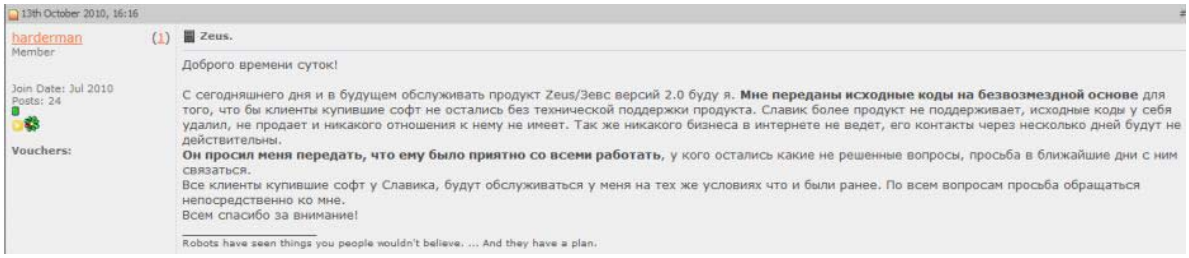

Fig. 6: Message où un certain Harderman annonce sur un forum, en juillet 2010, que l'auteur de ZeuS lui a cédé le code de son maliciel et la gestion de sa clientèle.

Dans diverses communications ultérieures, Harderman a donné à entendre que les travaux de la version 2 de ZeuS ne seraient pas poursuivis. La communauté pouvait néanmoins s'attendre à la mise au point d'un nouveau maliciel, né de la fusion de SpyEye et ZeuS.

4.10 Démantèlement de l'organisation de blanchiment d'argent J1 Network

L'organisation J1 Network a été démasquée parce qu'elle blanchissait de l'argent sale provenant d'activités cybercriminelles. Son nom tient au fait qu'elle recrutait ses membres principalement parmi les étudiants étrangers au bénéfice d'un visa J1 d'établissement aux Etats-Unis. Divers groupes criminels sévissant dans le cyberespace recouraient à ses services. C'était notamment le cas de bandes s'en prenant aux activités de e-banking pour détourner en ligne de l'argent de comptes bancaires. Le FBI a signalé avoir arrêté 37 personnes affiliées à cette organisation[43].

Fig. 7: Acteurs du réseau J1 recherchés par le FBI.

[43] Le communiqué du FBI à New York figure sous http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo093010.htm (état: 10 janvier 2011).

Les accusés, dont la plupart séjournaient sur sol américain grâce à un visa d'étudiants, avaient ouvert des comptes auprès de différents établissements financiers. Ils utilisaient à cet effet de faux passeports. Après avoir reçu l'argent dérobé sur les comptes en ligne, ils en gardaient un certain pourcentage pour eux. Le reste était envoyé en Russie.

Le FBI a démantelé cette organisation. Il estime à près de trois millions de dollars la somme totale blanchie de cette manière.

4.11 Agents financiers pour cartes de crédit

Le courriel ci-dessous a été envoyé à la fin de décembre 2010. Rédigé dans un allemand approximatif, il encourageait ses destinataires à déployer une activité d'agent financier pour cartes de crédits (*moneymule*). Les personnes intéressées recevraient par poste des cartes de crédit volées ou falsifiées, afin d'y prélever de l'argent à transférer au chef criminel ou à un autre agent financier, après déduction d'une commission. Le courriel répondait aux questions fréquentes et signalait dès la première phrase la possibilité de poursuites pénales:

Exemple n'existant qu'en allemand!

Subject: Unternehmensfuhhrung sucht Teammitglieder

Eine Arbeit fur jemanden der sich im Klaren ist, dass falls was schief gehen sollte er im bestenfalls mit einer Bewahrungsstrafe auskommt , im schlimmsten ....

Ich bin in diesen Business seit 2002, mit mir hat eine Menge Leute gearbeitet , aber nur 2 wurden verhaftet und auch die nur wegen Ihrer Gierigkeit und Dummheit. Jeder einzelne der geschnappt wird, ist nicht nur ein finanzieller Verlust, sondern auch eine grosse Gefahr fur die gesamte Mannschaft. Deswegen sind folgende Regel zu befolgen:

1. Die Vorschriften werden strengstens eingehalten. Das Geld wird nur in den von mir bestimmten Bankautomaten zu der von mir angesagten Zeit abgehoben. Es wird nur die abgesprochene Summe abgehoben. Die Vorschriften fur das Erhalten der Kreditkarten und fur die Gelduebergabe werden strengstens befolgt. 2. Das Geld ist ehrlich abzugeben (keine Tauschungsversuche) 3. Nur anonyme Simkarten benutzen, dieses Telefon fur Anrufe der Freunde und Verwandte nicht verwenden 4. Sich nie mit *Arbeitskollegen* dieses Businesses treffen, wenn sich einer mit dir treffen moechte, arbeitet er zu 99% fur die Bullen 5. Wenn du keine Disziplin hast, die Regeln nicht einhalten kannst, bzw. mich fur paranoid haltst - dann sollen wir keine Zusammenarbeit auch versuchen.

Arbeitsbeginn
Du hollst die Kreditkarte ab. Wo das sein wird gebe ich am Telefon durch (meist bei dir in der Stadt oder in einer Grossstadt in deiner Umgebung. Zusammen mit der Karte erhalst du eine genaue Anweisung wo, wann und wie viel Geld abzuheben ist. Die Anweisung ist 100% genau auszufuhren, davon hangt unser Verdienst und auch deine Sicherheit ab. Fur die erste Karte musst du eine Pfandsumme von 300 Euro hinterlassen. Dies ist fur die Sicherheit, dass falls du alles abhebst und verschwindest, ich meine Kosten fur die Kreditkartenbeschaffung und die Transportkosten zu dir, decke. Du erhalst diese Pfandsumme bei der ersten Abhebung zurück, also bei den ersten Bankautomaten. Fur das erste mal erhallst du eine Kreditkarte und die dazugehorige Pin mit einen Abhebelimit von 1500 Euro. Hebst so viel ab, wie es in der Anweisung angegeben wird. Aus den abgehobenen Geld erhallst du 600 Euro , - 300 als Pfandruckgabe und 300 als dein Verdienst. Das restliche Geld ubergibst du an mich, wie das geschehen soll schreibe ich dir per sms. Weiter erhallst du 2-4 Karten pro Woche (Pfand brauche ich nicht mehr). Zum Anfang werden die Karten mit einen kleineren Guthaben sein 1000 bis 2000 Euro, davon erhallst du 300 bis 600 Euro als deine Provision. Spater, wenn unsere Zusammenarbeit gut verlauft und du alle Regel befolgst, arbeitest du mit Karten mit maximalen Guthaben, wo du pro Karte bis zu 1500 Euro verdienen kannst.

Um die Arbeit starten zu konnen, brauchst du eine anonyme Simkarte die du in jeden zweiten Internetkafe oder Callcenter erhalten kannst. So bald du diese hasst, teilst du mir die Nummer an meine Email: mit. Weiter schreibe ich dir eine Sms was du weiter zu tun hasst.

Gleich die Antworten auf meisstgestellte Fragen:
1. Was fur Garantien habe ich, dass Sie mit meinen 300 Euro nicht verschwinden?

An.: Gar keine, aber anders wird es nicht gehen. Wenn du Angst um 300 Euro hasst (vielleicht ist es eine grosse Summe fur dich) dann hoere ich von dir zu 100% nichts mehr, so bald du um die 5000 Euro abgehoben hasst.

2. Ich habe keine 300 Euro, kann ich als Garantie meinen Pas, meinen Studentenausweis, mein Wort, meine Freundin , meinen Arsch, etc. hinterlassen?

An: NEIN, ich stelle jeden Tag einen neuen Mitarbeiter an, meine Ausgaben pro Kartenzubereitung und den Transport zu dir sind ca. 300 Euro und falls du mit der Karte verschwindest habe ich 300 Euro Verlust- das muss nicht sein.

P.S So lange du nicht probierst an Geld zu kommen, weisst du nicht wo fur du geboren bist. Dein Leben lang auf Hartz 4 zu sitzen bzw. fur 1000 Euro im Monat deinen Arsch aufzureissen oder einige Male deinen Mut zusammen zu nehmen und vom Leben alles zu bekommen versuchen. Die, welche Mut und Nerven genug haben, diese Arbeit an zu nehmen, werden in ca. einen halben Jahr zu wohlhabenden Menschen und kriegen mit, dass das Geld nicht alles ist. Bevor du also meinen Angebot annimst uberlege ernsthaft ob du es wirklich brauchst und durchziehen kannst!!!

Les agents financiers (moneymules) sont rares et d'autant plus recherchés par les criminels. Normalement, on se sert d'eux pour blanchir de l'argent issu de versements bancaires frauduleux. Des histoires plus ou moins plausibles sont inventées, pour que la victime ne se doute pas que les transactions sont illégales et relèvent du blanchiment. Le cas d'espèce est différent, puisque l'escroc invite ouvertement à commettre un délit et donne de surcroît des conseils pour éviter de se faire attraper. En effet, le risque d'être découvert est moindre avec une carte de crédit. Alors qu'avec e-banking l'agent financier est le destinataire de l'argent détourné et que, repéré dès le premier versement frauduleux, il disparaît très vite de la circulation, il est plus difficile ici d'identifier l'auteur du forfait. Aussi le courriel ne vise-t-il pas à recruter des personnes naïves, mais s'adresse à des criminels potentiels. Il n'est pas exclu non plus qu'il s'agisse d'une forme d'arnaque à l'avance de frais et que la personne intéressée n'entende plus jamais parler de son «employeur» après avoir versé la taxe d'accès de 300 euros. En pareil cas, l'escroc ne risque guère d'être dénoncé, la victime ayant elle-même cherché à commettre des actes criminels.

5 Tendances / Perspectives

5.1 Stuxnet – premiers chevaux de Troie visant les systèmes SCADA

Au début, les systèmes *SCADA* ne ressemblaient guère aux technologies usuelles de l'information et de la communication. Ils étaient isolés des réseaux informatiques, utilisaient des systèmes et des logiciels propriétaires et possédaient leurs propres protocoles de communication avec l'ordinateur central. L'accès aisé à des appareils relativement avantageux, incluant une interface avec le protocole Internet, a abouti ces dernières années à d'importants changements dans ce domaine. Désormais, les thermomètres, les mesureurs de pression, les pompes, les interrupteurs et autres équipements de terrain possèdent fréquemment leur propre adresse IP et utilisent le protocole *TCP/IP* pour communiquer avec l'ordinateur central. Or l'avantage du recours à ces produits standard et meilleur marché se repaie, dans la mesure où les systèmes SCADA sont désormais exposés aux menaces bien connues d'Internet: les maliciels et les pirates (hackers) ont fait leur apparition. Dans ce contexte, l'accent est mis en priorité sur les contacts internationaux et sur un renforcement ciblé de la collaboration entre l'Etat et les exploitants d'infrastructures d'information critiques, de façon à échanger rapidement des informations sur les nouveaux risques et les mesures de défense à prévoir. MELANI est en étroit contact avec les entreprises électriques suisses et participe aux échanges internationaux d'informations, notamment dans le cadre d'EuroSCSIE (European SCADA and Control Systems Information Exchange).

Malgré bien des spéculations visant à déterminer qui se cache derrière le virus Stuxnet, on ignore toujours qui en est le «père» – et on ne le saura probablement jamais. L'avantage de ce type d'attaques est qu'il est extrêmement difficile, voire impossible, de remonter jusqu'à leur auteur. D'où la possibilité d'obtenir un effet important avec un minimum de risque.

Comme dans cette attaque les arguments financiers ne jouent qu'un rôle secondaire et la motivation semble être de nature plutôt politique, il est tentant d'y voir une intervention étatique. Les possibilités offertes par l'espionnage ou le sabotage électronique sont d'ailleurs connues de longue date par les services de renseignement, qui en font eux-mêmes usage. Stuxnet n'est que le premier cas à bénéficier d'une audience planétaire. A la différence des terroristes, les Etats sélectionnent avec soin leurs cibles et n'attaquent que les installations dont la défaillance est jugée indispensable pour protéger leurs intérêts nationaux. Moyennant une motivation aussi forte et des ressources suffisantes, tout système risque un jour d'être infiltré et saboté. Tout indique que des attaques similaires se reproduiront.

5.2 DDoS – contexte et motivations

Dans le cyberespace, les attaques par déni de service distribué ou attaques DDoS (Distributed Denial of Service), consistant à inonder la victime de messages envoyés simultanément par de nombreux systèmes, poursuivent des buts différents. Au début, il s'agissait de purs actes de vandalisme. Les motivations ont changé entre-temps. On observe par exemple des attaques DDoS servant d'instrument de vengeance, visant à nuire à la concurrence, relevant du racket ou poursuivant des mobiles politiques. Alors que les attaques de moindre importance sont généralement tues et ne parviennent pas à la connaissance du public, on trouve régulièrement des attaques DDoS de grande envergure visant à attirer l'attention (des médias). Les sites ou serveurs Web font partie des cibles privilégiées. Mais les serveurs de messagerie, les serveurs DNS, les routeurs et les pare-feu, ou d'autres types de services Internet ne sont pas épargnés. Les lignes qui suivent décrivent les différentes motivations des auteurs.

Attaques politiques

Les attaques à caractère politique ne constituent pas un phénomène nouveau. Les pirates recourent à toutes sortes de moyens illégaux – ou du moins douteux – pour donner une visibilité accrue à leurs requêtes. Tant les attaques DDoS que la défiguration de sites Web sont fréquentes dans ce contexte.

L'exemple le plus connu d'attaque DDoS à mobiles politiques est l'agression dont l'Estonie a été victime en 2007. Suite à une polémique portant sur le déplacement d'un monument érigé à Tallin et figurant un soldat soviétique inconnu, divers sites Web estoniens sont tombés en panne pendant des semaines entières. Des attaques DDoS ont également été lancées comme mesures de soutien à un conflit. Lors des affrontements de 2008 ayant pour enjeu les Républiques dissidentes d'Ossétie du Sud et d'Akhasie, de nombreux sites des autorités géorgiennes ont été paralysés ou défigurés. Les cyberattaques se sont concentrées sur les sites du gouvernement géorgien. Un an après l'offensive russe, des attaques DDoS ont été observées contre Twitter, Facebook et LiveJournal. Elles visaient un *blogueur* géorgien[44] ayant pour pseudonyme Cyxymu[45], aux blogs très critiques à l'égard de la politique russe au Caucase.[46] Une attaque DDoS, elle aussi vraisemblablement à caractère politique, a malmené en avril 2008 le service de diffusion de Radio Free Europe en Biélorussie, soutenu financièrement par les Etats-Unis. L'attaque a débuté à la date de l'anniversaire de la catastrophe atomique de Tchernobyl. Ce jour-là, la radio retransmettait en direct une action de protestation menée à Minsk pour rappeler la détresse des victimes et pour dénoncer la

[44] http://news.cnet.com/8301-27080_3-10305200-245.html (état: 14 février 2011).

[45] http://cyberinsecure.com/distributed-denial-of-service-attack-takes-down-twitter/ (état: 14 février 2011).

[46] http://wwwguardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia (état: 14 février 2011).

décision du gouvernement de construire une nouvelle centrale nucléaire. Au plus fort de l'attaque, l'émetteur aurait reçu jusqu'à 50 000 requêtes par seconde.

Les attaques DDoS à mobiles politiques n'ont pas épargné la Suisse. La première sans doute a eu lieu en 2007. A l'époque, le site des Services du Parlement (parlement.ch) n'a pas fonctionné normalement pendant plusieurs jours. Il était inondé de requêtes nécessitant de longues listes de résultats, ce qui ralentissait le temps de réponse du serveur. Si le motif exact de cette cyberattaque n'a jamais été élucidé, le choix de la cible suggère une arrière-pensée politique, ou du moins l'absence de dessein financier.[47] Trois ans plus tard, en novembre 2010, les sites Web de quatre partis gouvernementaux étaient attaqués. Là aussi, on peut y voir des mobiles politiques, d'autant plus que l'agression précédait de peu le scrutin de l'initiative sur le renvoi (voir chapitre 3.1). Par contre, la motivation de l'attaque DDoS lancée en décembre 2010 contre PostFinance après la fermeture du compte de Julian Assange, fondateur de Wikileaks, ne fait aucun doute. Les sympathisants de Wikileaks y avaient été encouragés à télécharger et utiliser un programme appelé LOIC (Low Orbit Ion Canon), qui avait inondé de demandes le site de PostFinance (voir chapitre 3.2). La même méthode avait déjà été observée dans l'attaque DDoS lancée contre l'Estonie. A l'époque, les forums russophones avaient fait circuler un script qui avait bombardé de requêtes ping les adresses IP et les serveurs DNS de quelque 18 sites Web estoniens.

Chantage et dommages à la concurrence

Les entreprises réalisant une grande part de leurs activités par Internet subissent un grave manque à gagner en cas de panne de l'infrastructure Web. Et si la panne devait se prolonger plusieurs jours, leur survie est menacée. Les pirates l'ont compris et utilisent leurs réseaux de zombies pour rançonner les entreprises actives dans Internet. La procédure s'apparente au racket. L'exemple qui suit montre comment peut se présenter une lettre de chantage.

Sehr geehrter Shop-Admin,

am , um 12:00 Uhr werden wir Ihren Shop für 30 Minuten unerreichbar für Sie und Ihre Kunden machen.

Dies hat folgenden Grund:

Wir werden Ihren Online Shop mit einfachen DDoS attackieren, so dass weder Sie, noch Ihre Kunden Zugriff auf Ihre Webseite, geschweige denn auf den Server haben.

Dies wird nur ein kleiner Testlauf sein damit Sie sehen wie ernst es uns ist!

Wir bieten Ihnen hiermit die Option an, weder die Testattacke noch den folgenden DDoS zu bekommen, indem Sie bis morgen 300 Euro in Form eines Ukash Vouchers (an jeder Tankstelle zu erhalten) uns via eMail, an die angegebene E-Mail Adresse (@) senden.

Informationen über Ukash finden Sie auch auf http://www.ukash.com oder an Ihrer Tankstelle.

Sollte bis morgen 11:45 Uhr kein Ukash Code eingegangen sein, so werden wir um Punkt 12:00 Uhr den DDoS starten, anfangs nur für 30 Minuten. Falls Sie nicht zahlen wird Ihr Service für längere Zeit offline bleiben was ihren Umsatz wohl stark sinken lassen wird.

Fig. 8: Lettre de chantage adressée à un propriétaire de boutique en ligne.

L'exploitant de la boutique en ligne a la possibilité soit de payer, soit de faire face à la cyberattaque, avec l'aide de son fournisseur d'accès. L'opération peut toutefois s'avérer très délicate, selon la taille du réseau de zombies engagé, et aboutir à une dénonciation du

[47] MELANI, rapports semestriels 2007/2, chapitre 4.1
http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état: 14 février 2011)

contrat par le fournisseur. A ce jour, les attaques DDoS observées en Suisse visaient principalement l'industrie du sexe. Dès l'automne 2007, divers sites de la branche érotique ont notamment été attaqués par un réseau de zombies. Leurs propriétaires ont eu beau changer à plusieurs reprises de fournisseur d'accès, leur portail est resté inaccessible pendant plusieurs mois. Les fournisseurs d'accès Swisscom et Cablecom ont eux aussi été en butte à des attaques DDoS. Ces agressions ne visaient toutefois pas l'hébergeur lui-même, mais certains de ses clients[48].

Le danger de telles attaques tient à ce qu'elles affectent le reste de l'infrastructure et risquent, dans le pire des cas, de déstabiliser tout le réseau. Dans le monde réel, on peut les comparer à un attentat lancé contre un occupant précis d'un bâtiment. Pour être sûr de l'atteindre, on rase tout l'édifice. Les autres personnes ayant la malchance de s'y trouver à ce moment subiront elles aussi des dommages corporels, car les agresseurs n'hésitent pas à causer des dommages collatéraux.

Actes de vengeance

Entre cybercriminels, le déni de service est depuis longtemps un moyen de se défaire de concurrents embarrassants ou de convaincre ses clients potentiels d'opter pour ses propres réseaux ou services. Les concurrents ou les commentaires déplaisants sont durement sanctionnés. Outre leurs rivaux, les pirates ont dans le collimateur les entreprises de sécurité informatique. Ainsi, le virus Storm Worm était doté d'un mécanisme lui permettant de lancer des attaque DDoS contre les antivirus en ligne, afin d'éviter la découverte de son propre réseau de zombies. Autre exemple, les experts d'IBM/ISS étaient parvenus à élucider la structure d'un réseau de zombies. Peu après, la liaison Internet de cette société a subi une attaque DDoS qui l'a rendue plusieurs jours inaccessible.[49]

Comme les attaques ne se concentrent pas toujours sur un objectif spécifique (généralement un site) mais s'en prennent à l'infrastructure de l'hébergeur, d'autres sites ou réseaux en pâtissent. Dans le meilleur des cas, ces acteurs non impliqués ne subiront qu'un préjudice financier. Au pire des cas, leurs processus critiques qui dépendent du réseau attaqué seront perturbés ou interrompus.

5.3 Mobile (in)security

Le ver Cabir, se diffusant par l'interface Bluetooth, a été le premier virus sur smartphone à faire parler de lui, en 2004. Il n'a guère causé de sérieux dommages, à ceci près que comme il était constamment à la recherche d'appareils joignables par *Bluetooth*, l'accumulateur se déchargeait à grande vitesse.

On a longtemps cru que les *smartphones* n'étaient pas une cible attrayante pour l'industrie des maliciels. Outre le nombre élevé de systèmes d'exploitation, les sceptiques faisaient valoir la difficulté des maliciels à se propager et l'absence de modèles d'affaires spécifiques parmi les cybercriminels. Or la diffusion croissante de smartphones et de téléphones mobiles

[48] MELANI, rapports semestriels 2009/1, chapitre 3.4 http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=fr (état: 14 février 2011) et 2009/2, chapitre 3.3 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=fr (état: 14 février 2011).

[49] http://www.tecchannel.de/sicherheit/news/1737083/storm_worm_schlaegt_zurueck_it_security_forscher_angegriffen/ (état: 17 février 2011).

dotés de fonctions analogues à un ordinateur, de même que la sauvegarde de données sensibles sur ces appareils, en font une cible toujours plus attrayante pour les escrocs.

En outre, le risque d'incidents dus à des maliciels comme on en connaît avec les ordinateurs augmente, avec la concentration du marché et la montée en puissance de certains systèmes d'exploitation pour téléphones mobiles[50]. Le réveil est venu en août 2010 d'une importante faille de sécurité PDF touchant iPhone, qui a attiré l'attention des médias. En cas d'ouverture avec le navigateur Safari Mobile d'un fichier PDF modifié, les restrictions mises en place par Apple sur les appareils iPhone, iPad ou iPod Touch subissaient un débridage (*jailbreak*). Il va de soi qu'une telle faille est intéressante pour les escrocs. En août également, le premier cheval de Troie SMS a affecté le système d'exploitation Android. Une fois installé, ce maliciel déguisé en lecteur multimédia envoyait des SMS payants. Son installation avait beau être complexe et exiger de l'utilisateur de multiples manipulations, beaucoup de personnes sont tombées dans le panneau. D'autres virus sont apparus depuis sur les téléphones Android, comme un maliciel se faisant passer pour Angry Birds[51], le jeu Tap Snake qui n'est pas qu'un simple jeu mais un logiciel d'espionnage[52], ou plus récemment Geinimi[53].

ZeuS Mitmo: Man-in-the-mobile

D'autres innovations se préparent dans la clandestinité. Ainsi, tout indique que ZeuS, sans doute le cheval de Troie le plus répandu dans le domaine du e-banking, tire également profit de la communication mobile. S21, société espagnole spécialisée dans la sécurité informatique, a récemment publié un article sur une variante de ZeuS s'en prenant aux systèmes d'authentification à deux facteurs qui utilisent comme second canal le téléphone mobile[54]. L'internaute infecté par cette version spéciale de ZeuS est prié de répondre pendant sa session de e-banking à différentes questions concernant son téléphone mobile, dont le n° dudit téléphone. Puis la victime est informée que pour des raisons de sécurité, son établissement financier lui délivre un nouveau certificat destiné à son téléphone mobile (dont l'escroc connaît désormais le numéro), qu'il lui faudra installer. Ce prétendu certificat infecte aussi le téléphone mobile. Lors de la transaction de e-banking, quand la banque envoie par SMS le code d'authentification, la communication ne sera pas visible du client. Elle parvient à la place à l'escroc, qui n'a plus qu'à ouvrir sa propre session de e-banking.

A l'avenir, les utilisateurs du e-banking feront probablement toujours plus leurs transactions via leur téléphone mobile. D'où de nouveaux défis pour les établissements financiers, et pas seulement parce que les téléphones mobiles n'offrent pas encore le même niveau de protection qu'un ordinateur «normal». L'authentification à deux facteurs où le code TAN est transmis par SMS offre de nouvelles possibilités de leurrer l'utilisateur du e-banking, vu que le smartphone n'est pas utilisé comme canal d'authentification indépendant. Ces dangers ont beau ne pas être encore imminents, il faut néanmoins inclure dès maintenant de telles considérations dans la planification de la prochaine génération d'authentification pour le e-banking.

Applications d'espionnage pour téléphones mobiles

[50] http://www.zeit.de/digital/mobil/2011-02/nokia-microsoft-wp7 (état: 17 février 2011).

[51] http://www.heise.de/security/meldung/Android-Luecken-ermoeglichen-heimliche-Installation-von-Apps-1134661.html (état: 10 janvier 2011).

[52] http://www.f-secure.com/weblog/archives/00002011.html (état: 14 février 2011).

[53] http://blog.mylookout.com/2010/12/geinimi_trojan/ (état: 14 février 2011).

[54] http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html (état: 14 février 2011).

De nombreuses applications publiées au deuxième semestre 2010 permettent d'espionner les conversations, les messages et d'autres données personnelles (agenda, GPS, etc.) des appareils mobiles. Outre les programmes déjà connus FlexiSpy et SpyPhone, de nouveaux noms ont fait leur apparition, comme Phone Creeper ou Remote iPhone Spy. La mise au point de nombreuses applications à des fins d'espionnage soulèvent plusieurs questions: ces fonctions, ou d'autres analogues, sont-elles intégrées à d'autres applications en apparence anodines? Dans quel cadre est-il permis d'utiliser des logiciels d'espionnage? L'arrestation en Roumanie de 50 personnes ayant utilisé ce genre d'applications pour téléphones mobiles donne un élément de réponse à la dernière question[55]. Le plus souvent, il s'agissait de surveiller son conjoint ou un concurrent.

Au-delà des smartphones: attaques contre les GSM et SMS of Death

Les smartphones ont beau être entourés d'un intense battage publicitaire, ils ne représentent pour le moment que 19%[56] du marché mondial de la téléphonie mobile. Les chercheurs Collin Mulliner et Nico Golde ont donc exposé au Chaos Communication Congress[57] un scénario envisageable pour attaquer les téléphones mobiles «normaux», qui dominent largement le marché mondial. L'attaque reposait sur un simple SMS, préparé pour transporter le code *binaire* de l'agression. Les opérateurs de téléphonie mobile tirent d'ailleurs eux aussi parti de ce principe pour procéder à la configuration des téléphones mobiles ou pour y installer des services supplémentaires. L'attaque présentée au congrès avait pour effet de bloquer définitivement le téléphone mobile.

L'attrait du téléphone mobile comme cible d'attaques de maliciels et d'opérations de vol de données tient à deux grands facteurs. D'abord, plus le téléphone mobile remplit les fonctions de base d'un ordinateur (accès à Internet, sauvegarde de données sensibles, réalisation de transactions financières, etc.), plus il devient une cible lucrative pour les cybercriminels. Ensuite, par analogie aux maliciels s'en prenant aux ordinateurs, on peut considérer que l'attrait d'une telle attaque augmente au fur et à mesure que le «public-cible» s'élargit. Autrement dit, le taux de pénétration toujours plus élevé des téléphones mobiles modernes en fait une cible toujours plus attrayante. Au vu de cette évolution, les problèmes de sécurité soulevés par Internet affecteront toujours plus à l'avenir la communication mobile. Les smartphones deviendront au cours des prochaines années de véritables petits ordinateurs personnels. Aujourd'hui déjà, la frontière entre smartphone, tablette électronique et Notebook est devenue floue. Il existe toutefois une différence au niveau de la protection offerte par de tels systèmes. Alors que sur les ordinateurs les programmes de sécurité sont devenus la norme, ils sont quasiment inexistants dans le cas des smartphones. En outre, plus de 85 % des téléphones mobiles utilisés dans le monde sont des «feature phones», soit des appareils simples n'offrant qu'un petit nombre de fonctions, p. ex. la lecture des fichiers MP3, et surtout ne permettant pas d'effectuer des mises à jour[58]. Or expérience à l'appui, les mises à jour ne sont pas activées tout de suite même sur les smartphones. A cet effet, il faut raccorder le smartphone à l'ordinateur, car elles ne se font pas en arrière-plan via le réseau, comme pour les stations fixes.

[55] http://www.theregister.co.uk/2010/07/01/romanian_spyware_arrests/ (état: 14 février 2011).

[56] http://www.gartner.com/it/page.jsp?id=1466313 (état: 10 janvier 2011).

[57] Chaos Communication Congress (Berlin, 27 au 30 décembre 2010).

[58] http://www.wired.com/threatlevel/2010/12/simplest-phones-open-to-%25E2%2580%259Csms-of-death%25E2%2580%259D/ (état: 10 janvier 2011).

5.4 Cloud Computing – précautions à prendre

L'expression *cloud computing* (informatique dans les nuages), décrivant une solution permettant aux particuliers, aux entreprises et aux administrations de gérer leurs documents, leurs applications, etc. ne date pas d'hier. Le principe est relativement simple et, à y voir de plus près, il s'agit d'un retour aux débuts de l'informatique et des réseaux. Au lieu de systèmes client aboutis, où le système d'exploitation local gère tout – des applications aux documents –, l'ordinateur privé ou du bureau y fait office de terminal. Les programmes de traitement de texte, les données et les autres applications nécessaires sont centralisés sur un serveur distant interconnecté par Internet. L'avantage d'une telle solution va de soi. Au lieu d'une dispersion des efforts d'administration entre les divers ordinateurs et les programmes et données s'y trouvant, il devient possible de se concentrer sur les systèmes centraux. Les cycles de correction des erreurs (patch) ne concernent plus qu'un système et chaque utilisateur relié dispose toujours des applications les plus récentes et entièrement à jour. De même, il devient aisé d'accéder de partout aux documents, qui n'existent plus seulement localement dans le cadre d'un *partage réseau* ou sur un seul ordinateur.

Ce modèle soulève toutefois des questions et des réserves en matière de sécurité, dont on a déjà abondamment parlé. La propriété de l'information est de fait cédée et la sécurisation des données repose sur le bon vouloir d'un tiers. En ce sens, la tendance à l'informatique dans les nuages marque un retour à la confiance aveugle accordée aux techniciens et aux experts en sécurité informatique. Or une telle évolution était plutôt en recul ces dernières années. De façon générale, les entreprises et les administrations ont de moins en moins considéré la sécurité des réseaux et de l'informatique comme une simple fonction de soutien, pour y voir un enjeu stratégique. D'où un conflit d'objectifs classique à prévoir, dans un proche avenir, entre l'abaissement des coûts de transaction et le renforcement de la sécurité technique visés, d'une part, et la tendance à privilégier la sûreté de l'information au sein des entreprises en misant sur des mesures de protection d'ordre technique, humain et physique, d'autre part.

En outre, certains problèmes se posent aussi aujourd'hui au niveau des prestataires de *cloud computing*. Dans la plupart des cas, les données des clients et les services proposés ne donnent pas toujours lieu à une gestion statique à un seul et même emplacement, mais sont répartis entre plusieurs centres de calcul et regroupés en fonction des besoins. D'où l'impossibilité de savoir précisément où se trouve tel ou tel document à un moment donné. Cette situation soulève encore des questions juridiques, car selon le pays où un document spécifique se trouve à un moment donné, la législation applicable n'est pas la même.

5.5 Monopoles du réseau – un problème de sécurité?

Un petit nombre d'acteurs-clés du réseau sont en mesure d'influencer l'évolution d'Internet et des infrastructures du réseau[59]. En 2010, plusieurs records ont été battus dans ce domaine. D'où la question de l'impact de telles concentrations sur la sécurité.

[59] Il suffit de penser à l'initiative de Google de créer une infrastructure en fibre de verre permettant aux Américains de surfer en moyenne 100 fois plus vite qu'auparavant. – http://googleblog.blogspot.com/2010/02/think-big-with-gig-our-experimental.html (état: 10 janvier 2011). On peut également penser au but de Mark Zuckerberg, le père de Facebook, de faire de sa plate-forme le portail d'entrée du Web (http://www.wired.co.uk/news/archive/2010-11/04/facebook-mobile-platform (état: 10 janvier 2011) http://www.spiegel.de/wirtschaft/unternehmen/0,1518,719920,00.html (état: 10 janvier 2011)

Google a enregistré un nouveau record, générant presque 6,4 % de tout le trafic Internet[60]. Si Google était un fournisseur de services Internet, il se classerait selon Arbor Networks comme deuxième fournisseur de la planète (le n° 1 étant celui qui assure une grande partie du transit de Google).

Facebook est devenu le site le plus consulté aux Etats-Unis[61], détrônant le poids lourd de la branche qu'est Google.

Aux dires de BitTorrent[62], qui distribue les programmes de partage de fichiers BitTorrent et µTorrent, cent millions d'utilisateurs se servent de l'un de ces deux logiciels développés par ses soins. De son côté, le système de gestion de contenu Drupal jouit d'ores et déjà de la confiance de 1 % de tous les sites Internet, qui l'ont choisi pour actualiser leur contenu[63].

Selon Twitter, près de 7000 tweets ont été publiés par seconde au Japon, le 31 décembre 2010 à minuit. L'entreprise a réalisé une spectaculaire carte du monde illustrant, par zone horaire, le nombre de tweets postés pour Nouvel An[64].

Infections par des maliciels

La présence d'une page infectée sur une plate-forme fréquentée constitue sans doute le cauchemar de tout expert en sécurité informatique. Les incidents liés à des serveurs de publicités (ad servers) compromis vont dans ce sens (voir chap. 3.13). S'il parvient ainsi à infecter le site d'un grand journal, un cyberpirate peut être sûr de la portée de son acte. De son côté, le ver Koobface est conçu pour le réseau social Facebook, dont il a déjà infecté d'innombrables visiteurs. Il se propage par d'infection «drive-by» et par des messages invitant leur destinataire à télécharger et exécuter un fichier. Les *plates-formes P2P* constituent un vecteur d'infection souvent sous-estimé. Outre les documents mis au point par un pirate, les films, les morceaux de musique ou les logiciels provenant de réseaux P2P sont susceptibles de contenir un cheval de Troie ou un injecteur (dropper). Un autre risque provient des systèmes de gestion de contenu (CMS) les plus souvent utilisés, comme Drupal ou WordPress. Une faille de sécurité d'un tel logiciel (comme cela s'est déjà produit avec WordPress) rendrait des centaines de milliers de sites Web vulnérables aux cyberattaques. On pourrait également penser à une attaque visant le service de noms de domaine (*domain name service, DNS)* de sites importants, afin qu'il communique à ses utilisateurs des copies préparées des sites demandés dans le but d'infecter leur système[65].

Utilisation des données personnelles

De grandes entreprises comme Facebook collectent une énorme quantité de données. Google StreetView a non seulement photographié les rues pour établir sa propre carte, mais

---

http://www.ustream.tv/recorded/3848950 (état: 10 janvier 2011)
http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas (état: 10 janvier 2011).

60 http://asert.arbornetworks.com/2010/10/google-breaks-traffic-record/ (état: 10 janvier 2011).

61 http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/ (état: 10 janvier 2011).

62 http://www.bittorrent.com/pressreleases/2011/01/03/bittorrent-inc-grows-to-over-100-million-active-monthly-users-massive-user- (état: 10 janvier 2011).

63 http://buytaert.net/drupal-7.0-released (état: 10 janvier 2011).

64 http://www.flickr.com/photos/twitteroffice/5330386295/ (état: 10 janvier 2011).

65 Un cas célèbre, datant de la fin de 2009, concerne Twitter (http://www.wired.com/threatlevel/2009/12/twitter-hacked-redirected/ (état: 10 janvier 2011). Si au lieu d'un message de défiguration les visiteurs avaient trouvé une copie du site de Twitter, l'attaque aurait pu avoir des conséquences dramatiques.

également relevé des données sur les raccordements à Internet sans fil présents sur son passage[66]. Des sites comme Groupon.com recueillent des données importantes sur leurs propres utilisateurs, comme leur géolocalisation et leurs préférences. Foursquare.com sait précisément qui se trouve où à quel moment[67]. D'un côté, cela permet d'établir le profil d'une personne et de ses habitudes, sur la base des données de quelques sites. De l'autre, on ne sait pas grand-chose sur les données collectées par de telles entreprises et sur l'usage qu'elles en font. Quant aux internautes, ils sont toujours plus enclins à diffuser leurs données personnelles sur les principaux sites Web.

L'émergence de ces géants de la toile soulève de nombreuses questions. Outre la sécurité des données ainsi que des utilisateurs, elles portent sur l'évolution d'Internet. Cette dernière dépend toujours plus de groupes qui gagnent beaucoup d'argent et dont on ne sait rien, ou pas grand-chose.

6 Glossaire

Le présent glossaire contient tous les termes indiqués en *lettres italiques*. Un glossaire plus complet est publié à l'adresse:
http://www.melani.admin.ch/glossar/index.html?lang=fr

AdServer	Un AdServer a pour finalité de diffuser des publicités pour des annonceurs et de mesurer l'impact de la publicité en ligne. Ce terme désigne tant le serveur hébergeant un logiciel AdServer que ce logiciel.
(three-way) handshake	L'établissement d'une connexion en trois étapes (3-way handshake) décrit la procédure à suivre pour établir sans perte de données une connexion entre deux hôtes. Ce terme s'utilise le plus souvent, mais pas uniquement, en technique des réseaux (demande de connexion du client, demande de confirmation du serveur, confirmation du client).
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Agent financier	Un agent financier est un intermédiaire légal effectuant des opérations de courtage en devises. Depuis peu, cette notion s'utilise aussi à propos de transactions financières illégales.
Application	Programme informatique permettant d'effectuer une tâche déterminée. Les traitements de texte et les navigateurs Web sont des exemples d'applications.
Attaque DDoS	Attaque par déni de service distribué (Distributed Denial-of-Service attack) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux

[66] MELANI rapport semestriel 2010/1, chapitre 4.5
http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=fr (état: 10 janvier 2011).

[67] http://www.zdnet.com/blog/feeds/foursquares-privacy-loopholes/2607 (état: 10 janvier 2011).

	systèmes.
Authentification à deux facteurs	Au moins deux des trois facteurs d'authentification sont exigés: un élément que l'on connaît (p. ex. mot de passe, code PIN, etc.) un élément que l'on détient (p. ex. certificat, jeton, liste à biffer, etc.) un élément qui nous est propre (p. ex. empreinte digitale, scanner rétinien, reconnaissance vocale, etc.)
Automate programmable industriel (API)	Un automate programmable industriel (en angl. programmable logic controller, 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.
Barre d'outils	Rectangle étroit contenant les boutons, symboles, menus, etc. représentant les fonctions les plus courantes d'un logiciel.
Blog	Un blog est un type de site Web censé donner régulièrement (web log signifie journal de bord sur le Web) le point de vue de son auteur sous forme de billets (courts textes) ou d'articles (textes plus longs) sur une multitude de sujets.
Bluetooth	Technologie permettant d'établir une communication sans fil entre deux équipements terminaux, mise en œuvre surtout dans les téléphones mobiles, les ordinateurs portables, les PDA (assistants numériques personnels) et les périphériques d'entrée (p.ex. la souris).
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.
CERT	Computer Emergency Response Team. Le terme CERT (ou CSIRT, Computer Security Incident Response Team) désigne un organisme chargé de la coordination et de l'adoption de mesures liées aux incidents relevant de la sécurité informatique.
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
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.
Cloaking	Le cloaking (de l'anglais: dissimulation) est une technique utilisée par les cyberpirates pour optimiser leur positionnement dans les moteurs de recherche. Elle consiste pour le serveur Web ainsi programmé à présenter un contenu de page Web différent selon que le client distant est un robot de moteur de recherche ou un internaute humain.

Cloud Computing	L'informatique dans les nuages (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les TIC ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises 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 dans le 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).
Cookie	Témoin de connexion. Petit fichier texte enregistré sur l'ordinateur de l'internaute à l'occasion de sa visite sur une page Web. Les témoins permettent par exemple de mémoriser les réglages personnels pour un site Internet. Il est cependant aussi possible de les utiliser abusivement, notamment pour établir un profil détaillé des habitudes de l'internaute.
Critical Infrastructure Protection / Critical Information Infrastructure Protection (CIP / CIIP)	Protection des infrastructures vitales / Protection de l'infrastructure d'information vitale. Volet important de la politique de sécurité et de la planification de la défense nationale. Terme générique recouvrant les concepts ou stratégies de protection des infrastructures vitales / de l'infrastructure d'information vitale.
Domain Name System (DNS)	Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
DNS Amplification Attack	Attaque par déni de service (attaque Denial of Service, DoS), utilisant des serveurs DNS publics comme amplificateurs.
Fichier binaire	Un fichier binaire n'est pas assimilable à un fichier texte et ne peut être lu directement par un éditeur de texte. Les fichiers binaires peuvent contenir du langage machine, du son, des images, etc.
General Packet Radio Service (GPRS)	Le general packet radio service (service général de radiocommunication par paquets) est un service de transmission numérique des données par ondes radioélectriques, offert sur un réseau mobile de type GSM et utilisant la commutation de paquets.
Hypertexte	Un système hypertexte est un système contenant des nœuds liés entre eux par des permettant de passer automatiquement d'un nœud à un autre. Un document hypertexte est donc un document qui contient des hyperliens et des nœuds. Le Web est aujourd'hui le système hypertexte le plus vaste et le plus

	utilisé. Les hyperliens du Web sont contenus dans des documents hypertextes généralement écrits en langage HTML (HyperText Markup Language), présentés sous la forme de pages Web.
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.
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.
Keyword Stuffing	Le keyword stuffing (bourrage de mots-clés) est une technique abusive visant à optimiser le classement dans les résultats des moteurs de recherche. La répétition excessive de mots-clés (keywords) sur une page Web ou dans les balises d'un site a pour but de tromper le moteur et de forcer le référencement.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Linkfarm	Le principe de la ferme de liens (linkfarm) consiste à créer des sites voire des domaines entiers se renvoyant les uns vers les autres, pour améliorer l'indice de popularité d'un site Web en augmentant le nombre de liens pointant sur lui.
Malware	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Navigateur	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Opera, Firefox et Safari.
Open source	Open Source est une palette de licences pour des logiciels dont le code source est accessible au public, dans une optique de développement communautaire.
Partage réseau	Un partage réseau désigne un appareil ou des informations figurant sur un ordinateur auxquels il est possible d'accéder à distance depuis un autre ordinateur, via un réseau.
Peer to Peer (P2P)	Il s'agit d'une architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux échanges de données.
Phishing	Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les

	pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées.
Pop-up	Un pop-up, ou fenêtre contextuelle, désigne un élément qui s'affiche automatiquement devant la fenêtre de navigation d'un site. Son nom vient de ce que ces éléments surgissent (angl. «pop up») et masquent d'autres éléments affichés.
Programmable logic controller (PLC)	Traduction anglaise d'automate programmable industriel (API).
Proof of Concept (PoC)	Démonstration brève, et pas nécessairement complète, du bien-fondé d'une idée ou d'une méthode. A titre d'exemple, les exploit codes sont souvent publiés sous forme de PoC, pour souligner les conséquences d'une faille de sécurité.
Pseudonyme	Par pseudonyme (nickname), on entend le nom d'emprunt (généralement bref) utilisé par un utilisateur pour ses interventions dans des forums ou lors de dialogues en ligne.
Resolver	Un résolveur (resolver) est un module logiciel simple installé sur un ordinateur client DNS. Il sert d'interface entre l'application du client et les serveurs de noms, en effectuant des requêtes de résolution de noms.
Rootkit	Ensemble de programmes et de techniques permettant d'accéder sans être remarqué à un ordinateur pour en prendre le contrôle.
Scareware	Le terme scareware désigne des logiciels vendus par des sociétés éditrices ayant su provoquer chez les clients potentiels du stress ou de la peur. Il s'agit d'une forme automatisée de subversion psychologique. Si la victime tombe dans le panneau et se croit menacée, il lui est suggéré de télécharger un logiciel payant pour éliminer le virus fictif. Parfois la personne se croyant victime de cyberpirates est elle-même amenée à effectuer des maneuvres rendant possible une telle attaque.
Secure Sockets Layer Protocole (SSL)	Secure Sockets Layer Protocole permettant de communiquer en toute sécurité sur Internet. SSL s'emploie aujourd'hui p. ex. pour les transactions financières en ligne.
Sidejacking	Technique des cyberpirates consistant à intercepter la communication en ligne entre deux parties. On parle aussi de détournement de session par vol de cookie.
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.).
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des

	données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Texte masqué	Texte caché sur un site Web. L'utilisation p. ex. d'une police de caractères transparente le rend indétectable à l'œil nu.
Top Level Domain (TLD)	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».
Transmission Control Protocol / Internet Protocol (TCP/IP)	La suite TCP/IP est l'ensemble des protocoles utilisés pour le transfert des données sur Internet. Bien qu'il s'agisse d'une famille de protocoles, le terme protocole TCP/IP s'est imposé.
Universal Serial Bus Bus (USB)	Universal Serial Bus. Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
USB Memory Stick	Clé mémoire USB. Petit dispositif de stockage des données connecté à l'interface USB d'un ordinateur.
Ver	A la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur.
Virus	Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager.
Web 2.0	L'expression Web 2.0 désigne certaines technologies et des du Web qui ont suivi la forme initiale du Web, en particulier les interfaces permettant aux internautes d'interagir (partager, échanger, etc.) de façon simple, à la fois avec le contenu et la structure des pages, mais aussi entre eux.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.

7 Annexe

7.1 DDoS – analyse d'un phénomène toujours plus fréquent

Une attaque par déni de service (denial of service, DoS) a pour but de rendre un service inaccessible aux utilisateurs autorisés, ou du moins de ralentir l'exécution de leurs opérations. On parle d'attaque par déni de service distribué (distributed denial of service, DDoS) lorsqu'une victime subit une attaque coordonnée de nombreux systèmes lui envoyant simultanément des messages. Ces cyberattaques impliquent généralement des ordinateurs infectés et faisant partie d'un réseau de zombies. Le chapitre 5.2 a examiné les mobiles sous-jacents aux attaques DDoS. Le présent chapitre vise à donner un aperçu plus complet de la technique sous-jacente à ce genre d'attaques et des principaux moyens permettant d'en limiter les dégâts.

Attaques DoS – méthodes et fonctionnement

De façon générale, on peut distinguer deux types d'attaques DoS. Les unes visent à mettre hors service un système, à force de solliciter ses ressources de calcul et mémoire (protocol-based et application-based). Les autres cherchent à saturer le réseau par des requêtes bidon, afin d'entraver le trafic légitime de données (flood-based). Parmi les cyberattaques recensées par Arbor Networks en 2009, 45 % ont été menées par inondation (flood-based), contre 49 % d'attaques applicatives (application-based).[68]

Les attaques applicatives (application-based ou protocol-based) font notamment appel aux techniques suivantes:

SYN flooding
Une attaque SYN flood tire parti du protocole de connexion TCP/IP (*handshake*). Un client envoie, pour établir ce type de connexion – p. ex. pour accéder à un site Web – une requête SYN au serveur concerné. Celui-ci accepte en envoyant un message SYN-ACK (synchronize-acknowledgement), normalement suivi de la réponse ACK du client. La connexion est alors établie[69]. Les deux parties ont ainsi suivi la procédure d'établissement d'une connexion en trois étapes (three-way handshake ou 3-step handshake). Si la machine d'un client supprime la dernière étape du message ACK, le serveur attend un certain temps cette réponse et réserve ainsi des ressources à ce client. Une attaque DoS consiste à générer des milliers de connexions incomplètes (message SYN seulement). Le serveur doit ainsi mobiliser ses ressources pour maintenir toutes les connexions établies. Jusqu'au moment où il est saturé et ne peut plus accepter aucune requête, même légitime.

Flot de processus
La technique suivante, qui fonctionne par exemple avec les serveurs Web Apache 1.x et Apache 2.x, montre qu'il est possible de paralyser un serveur Web même avec des ressources de réseau limitées. A chaque demande de page Web, le serveur lance un processus qui s'achève une fois la demande satisfaite, autrement dit une fois que le site a été entièrement chargé. Si le client cherche à établir un maximum de connexions et à les

[68] «Worldwide Infrastructure Security Report», Arbor Networks 2009, http://www.arbornetworks.com/dmdocuments/ISR2009_EN.pdf (état: 10 janvier 2011).

[69] Nous avons simplifié le système servant à établir une liaison. Pour en savoir plus, il est recommandé de lire «Computer Networks» d'Andrew S. Tanenbaum.

maintenir ouvertes le plus longtemps possible, il arrive un moment où le nombre maximum de processus parallèles est atteint, où les nouvelles requêtes ne sont plus autorisées et où le site n'est plus accessible.[70] Une telle attaque s'avère intéressante dans la mesure où elle n'exige pas une grande bande passante. En outre, on trouve sur Internet des programmes comme Slowloris qui lancent ce genre d'attaques et dont l'utilisation est simple (y c. via un serveur mandataire ou dans Tor)[71].

Ping de la mort (ping of death (PoD) et attaques par amplification (smurf)
Une technique connue de longue date consiste à envoyer un paquet ping malformé[72]. Dans une attaque de type smurf, un pirate envoie des pings (requêtes d'écho ICMP) à l'adresse de diffusion d'un réseau. L'expéditeur a substitué à sa véritable adresse celle de sa victime. Selon la configuration du routeur, la requête sera acheminée à travers le réseau et tous les ordinateurs qui en font partie seront contraints de répondre à la victime. Les routeurs qui tolèrent une telle façon d'agir ont une fonction amplificatrice (smurf amplifier). Selon le nombre d'ordinateurs connectés à un tel réseau, le facteur d'amplification d'une simple requête peut être énorme.

Attaques applicatives (application attack)
Une autre forme d'attaques est ciblée sur les fonctions des serveurs Web qui absorbent d'importantes ressources. A l'instar de la fonction de recherche d'un site ou des systèmes de gestion de contenu (content management system, CMS, p. ex. WordPress ou Drupal) qui créent la page au moment de la recherche (à la différence des pages statiques disponibles sur le serveur). L'impact d'une attaque lancée contre de telles pages sera naturellement beaucoup plus grand.

Quant aux attaques par inondation (flood-based), elles sont lancées à partir d'un nombre élevé d'ordinateurs (généralement des machines infectées faisant partie d'un réseau de zombies; d'autres sont toutefois sciemment utilisées pour lancer des cyberattaques). Les requêtes accaparent toute la bande montante du serveur, pour qu'il ne plus puisse plus envoyer cette page ou fournir le service demandé. L'efficacité de ce type d'attaque dépend de la bande passante du serveur. En règle générale, un grand réseau de zombies sera en mesure de mener des attaques à plus grande échelle. Diverses techniques permettent toutefois d'en accroître l'impact, afin que même des réseaux de zombies de petite ou moyenne taille puissent servir à des cyberattaques spectaculaires.

Attaques DNS
Il existe trois manières différentes de répondre à une requête DNS:

- serveur faisant autorité: le serveur contient l'ensemble des données de la zone, où il puise le fichier demandé;
- requête récursive: le serveur interroge d'autres serveurs de noms pour répondre;
- requête itérative: le serveur transmet une référence à d'autres serveurs de noms.

En cas de requête récursive, le *résolveur* soumet une requête récursive au serveur de noms qui lui est attribué. Si un serveur de noms ne possède pas lui-même l'information souhaitée, il contacte d'autres serveurs jusqu'à ce qu'il reçoive une réponse positive, ou une réponse négative d'un système faisant autorité. Au fond, un serveur de noms ne devrait accepter que les requêtes provenant de clients locaux ou autorisés. Dans les faits, de nombreux serveurs DNS acceptent des requêtes quelle qu'en soit la source. Le cas échéant, on parle de

[70] http://www.securityfocus.com/archive/1/456339/30/0/threaded (état: 10 janvier 2011).

[71] http://vimeo.com/7618090 (état: 10 janvier 2011).

[72] http://insecure.org/sploits/ping-o-death.html (état: 10 janvier 2011).

résolveurs ouverts (open resolvers)[73]. L'astuce consiste à envoyer des requêtes à des résolveurs ouverts en indiquant comme adresse de réponse l'adresse de la victime. La victime recevra ensuite une masse de réponses DNS qu'elle n'a pas sollicitées. En outre, seule l'adresse IP du serveur de noms apparaît et non celle de l'agresseur. Cette anonymisation de l'attaque rend d'autant plus difficile une défense efficace. Une technique destinée à accroître l'impact de telles attaques réside dans l'*amplification DNS.* Dans certains cas, les serveurs de noms réagissent à de brefs paquets de requêtes par de très longs paquets. Une requête de 60 octets peut ainsi recevoir une réponse de plus de 4000 octets, soit un facteur d'amplification de plus de 65. En outre, la fragmentation IP nécessite davantage de ressources de calcul. C'est l'extension du système DNS en EDNS qui a permis ce type d'attaques. Jusque-là, la longueur maximale d'un paquet DNS était limitée à 512 octets (soit un facteur d'amplification inférieur à 10). Or il ressort d'une étude déjà ancienne (2005)[74] que 75 % des requêtes DNS externes sont des interrogations non autorisées, et donc permettant des attaques par empoisonnement[75] ou DoS.

L'utilisation des réseaux P2P permet aussi un effet d'amplification. En pareil cas, le serveur de la victime est indiqué comme unique source d'un fichier connu (film, album ou autre), si bien que les utilisateurs du réseau P2P demandent le fichier souhaité à cette adresse IP. Différents chercheurs ont étudié la question[76].

On constate également que les attaques réalisées à l'aide de réseaux de zombies ont gagné en efficacité. Par exemple, les pirates n'utilisent pas en même temps toutes les machines du réseau. D'où un effet accru et plus durable si les machines appartenant aux divers sous-groupes du réseau (provenant d'une autre région géographique, avec leurs propres fournisseurs d'accès) sont engagées de façon aléatoire, en ne générant qu'un trafic modéré. Une telle tactique ralentit le processus de filtrage des adresses IP par la victime.

Attaques DoS – contre-mesures

Le CERT du gouvernement néerlandais a récemment publié un document passant en revue les mesures utiles pour se protéger contre les attaques DoS[77]. Le premier point signalé relève non pas de la technique, mais de l'organisation de la *communication d'entreprise*: ce qu'une entreprise communique, et la manière dont elle le fait, s'avère indiscutablement un facteur décisif. Une stratégie de communication peut servir de première mesure contre les attaques DoS, ou alors être à l'origine de telles attaques. Il suffit de penser à ce qui est arrivé à PostFinance en décembre 2010: l'annonce du blocage du compte de Julian Assange a déplu au mouvement Anonymous, qui a lancé une attaque DDoS. Autrement dit, il faut évaluer au préalable les risques et les conséquences de sa communication au grand public.

Des mesures techniques peuvent être prises à l'entrée du réseau, ou alors directement au niveau du fournisseur d'accès:

---

[73] Le texte de Randal Vaughn et Gadi Evron «DNS Amplification Attacks» vaut la peine d'être lu http://www.isotf.org/news/DNS-Amplification-Attacks.pdf (état: 10 janvier 2011).

[74] http://dns.measurement-factory.com/surveys/sum1.html (état: 10 janvier 2011).

[75] Voir chapitre 7.3 du rapport MELANI 2008/2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=fr (état: 10 janvier 2011).

[76] http://www.pank4j.com/research/p2pddos.pdf (état: 10 janvier 2011) et http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5254891%2F5273826%2F05273837.pdf%3Farnumber%3D5273837&authDecision=-203 (état: 10 janvier 2011).

[77] http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html (état: 10 janvier 2011).

Analyser en détail le trafic:
Il s'agit d'une première mesure visant à cerner la composition du trafic entrant des serveurs. Sur cette base, il devient possible de déterminer ce qu'il y a lieu de filtrer. Parmi les applications les plus utilisées pour l'analyse des trafics (flux Netflow) figurent notamment des outils open source tels que NFSen[78] et NFDump[79].

Filtrage des paquets expédiés et limitation des requêtes:
Identifier les paquets malveillants[80] et les filtrer pour que le serveur ne réagisse qu'aux requêtes autorisées. Limiter la fréquence des requêtes autorisées par adresse IP, pour éviter que tous les ordinateurs zombies ne génèrent des centaines de requêtes à la seconde.

Scrubbing:
Mettre en place un système complexe répartissant les messages entre plusieurs serveurs, pour gérer les pics de trafic. Comme variante, utiliser des services CDN (content delivery network, réseau de diffusion de contenu) comme Akamai[81].

Equilibrage de charge (load balancing) et fonction de cache:
Utiliser différents serveurs affiliés à plusieurs réseaux (fournisseurs d'accès) et se partageant le trafic entrant. Le cas échéant, exploiter aussi la fonction de cache des serveurs reverse proxy, comme par exemple nginx[82] ou squid[83].

Utiliser la redirection dynamique (dynamic rerouting):
Cette méthode communique aux ordinateurs attaquants qu'il n'existe pas de route valable (null route, blackhole route) pour contacter la machine de la victime.

N'admettre que le trafic autorisé par le protocole:
Si les requêtes autorisées par le serveur Web sont toujours reçues sur les ports TCP:80 et TCP:443, il est possible de bloquer le port 80 UDP, dont le protocole http n'a pas besoin.

Demander au fournisseur d'accès
s'il met à disposition des solutions comme IDMS[84] ou RTBH (Remotely Triggered Black Hole[85]) pour déjouer les attaques DoS.

---

78 http://nfsen.sourceforge.net/ (état: 10 janvier 2011).

79 http://nfdump.sourceforge.net (état: 10 janvier 2011).

80 L'attaque du mouvement Anonymous contre différentes cibles reposait sur le programme LOIC (Low Orbit Ion Cannon). Celui-ci mentionnait «wikileaks.org» comme champ d'information des paquets TCP et UDP. Il a ainsi été possible de définir des règles de filtrage.

81 http://www.akamai.com (état: 10 janvier 2011).

82 http://nginx.net/ (état: 10 janvier 2011).

83 http://www.squid-cache.org/ (état: 10 janvier 2011).

84 http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigation-systems/download.html (état: 10 janvier 2011).

85 http://www.google.ch/url?sa=t&source=web&cd=1&sqi=2&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.cisco.com%2Fen%2FUS%2Fprod%2Fcollateral%2Fiosswrel%2Fps6537%2Fps6586%2Fps6642%2Fprod_white_paper0900aecd80313fac.pdf&rct=j&q=remotely%20triggered%20black%20hole&ei=1iMwTZPZO4ztsgbq8P2lCg&usg=AFQjCNEZ-kPQ3RiLBBecuEFuKAQ2fQO4OQ&cad=rja (état: 10 janvier 2011).