Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2013/II (juillet – décembre)

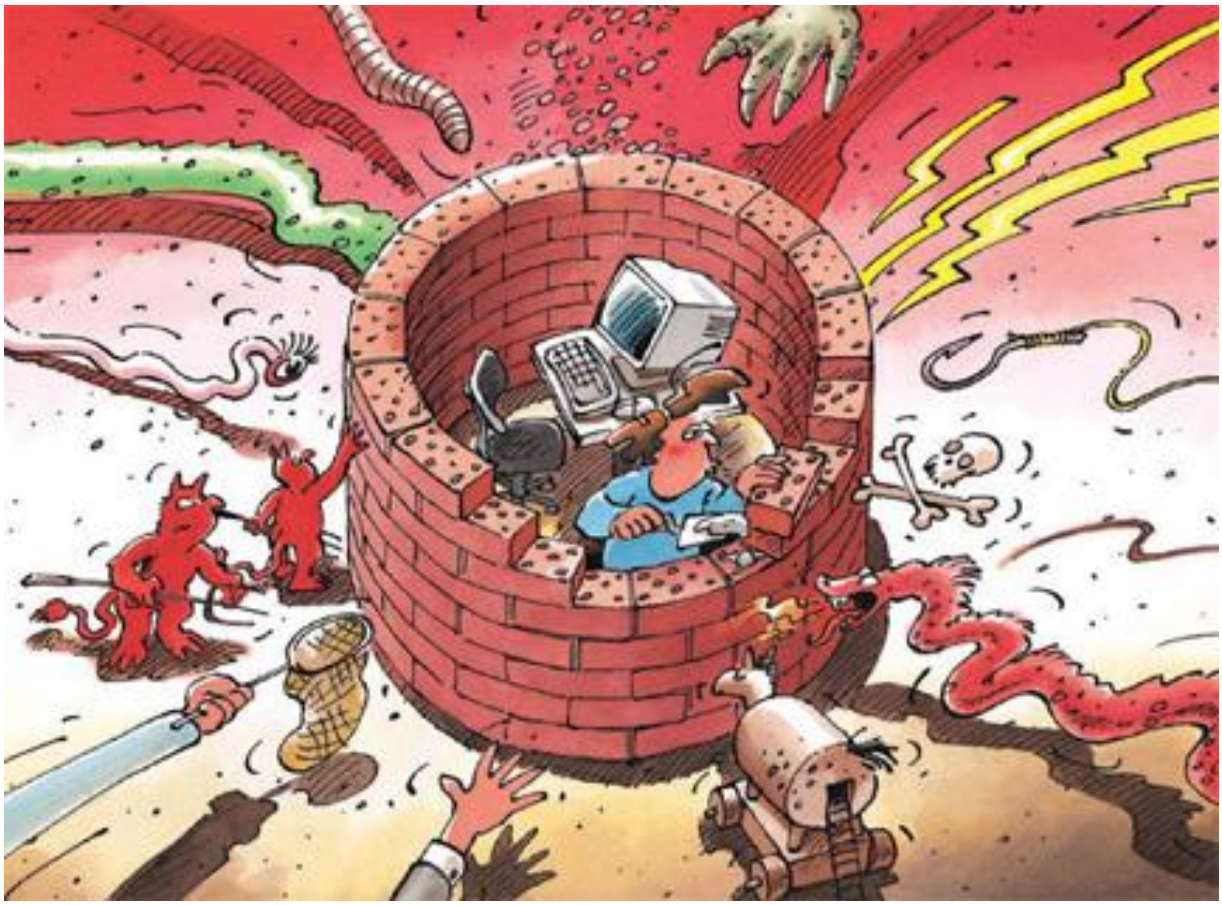


Table des matières

1 Temps forts de l'édition 2013/II

- **Nouvelles révélations sur la NSA et le GCHQ**
  Au deuxième semestre 2013, on a beaucoup reparlé des pratiques tant américaines (National Security Agency, NSA) que britanniques (General Communication Headquarter, GCHQ) figurant dans les documents divulgués par Edward Snowden. Il en ressort que ces services de renseignement enregistrent des données à grande échelle et de façon systématique. Ces découvertes confirment les problèmes créés par un média transnational comme Internet, auquel chacun a la possibilité et le droit de participer librement, tandis que les Etats agissent et édictent des lois nationales comme ils l'entendent, sans se soucier de leurs conséquences globales.

  ► Situation sur le plan international: chapitre 4.1
  ► Tendances / Perspectives: chapitre 5.1

- **Bitcoin: succès et rançon du succès**
  Bitcoin est une monnaie électronique décentralisée, dont le fonctionnement ne dépend d'aucun émetteur central. Elle se démarque par là des devises traditionnelles, ainsi que de nombreuses autres monnaies électroniques. La popularité croissante de Bitcoin soulève de nombreuses questions, tant au niveau sécuritaire qu'à propos du statut légal et de la réglementation de telles devises.

  ► Tendances / Perspectives: chapitre 5.2

- **Essor des rançongiciels**
  Parmi les rançongiciels (*ransomware*, maliciel utilisé comme moyen de chantage) figurent des chevaux de Troie, qui bloquent l'ordinateur infecté et publient une annonce prétendument issue d'une autorité de police. Une infection bien plus lourde de conséquences, due à Cryptolocker, a été observée en Suisse pour la première fois en novembre 2013. Ce maliciel crypte, et donc rend inaccessibles à la victime, toutes les données stockées sur son disque dur et sur les supports de données lui étant raccordés.

  ► Situation en Suisse: chapitre 3.1

- **Spectaculaires vols de données**
  Des vols portant sur des millions de jeux de données ont à nouveau été rendus publics. De son propre aveu, Adobe s'est fait dérober les données de 38 millions de clients – mots de passe et informations bancaires. La chaîne de magasins Target a connu le même sort. Les informations publiées font état du vol des détails de 40 millions de cartes de crédit et débit, ainsi que des données personnelles concernant 70 millions de clients.

  ► Situation internationale: chapitre 4.3, chapitre 4.4

- **Systèmes de contrôle industriels et domotiques – Toujours plus de systèmes raccordés à Internet**
  L'achat de systèmes dotés d'une fonction de consultation et de pilotage à distance, tout comme l'ajout d'une interface de communication à une installation existante, s'est banalisé et ne coûte plus très cher. D'où l'importance de se soucier, au-delà des fonctionnalités et de la convivialité des solutions d'accès à distance, de la protection offerte contre les manipulations non autorisées. MELANI a publié en octobre 2013 une liste de contrôle destinée à la protection des systèmes de contrôle industriel.

  ► Situation internationale: chapitre 4.7

2 Introduction

Le dix-huitième rapport semestriel (juillet à décembre 2013) 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 premiers mois de l’année 2013. 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.

Pour la première fois, le **chapitre 5** passe en revue dans un sous-chapitre les principales interventions parlementaires se rapportant à la sûreté de l’information.

3 Situation en Suisse de l'infrastructure TIC

3.1 Chantage dû à Cryptolocker & Cie

Les rançongiciels (*ransomware*), maliciels utilisés pour extorquer de l'argent au propriétaire de l'ordinateur infecté, existent depuis longtemps déjà. Les plus répandus sont des chevaux de Troie qui publient sur la machine bloquée une annonce prétendant provenir d'une autorité de police, comme l'Office fédéral allemand de la police criminelle ou le Département fédéral de justice et police (DFJP). La victime est priée de s'acquitter d'une amende, sous prétexte que des données illégales figureraient sur son ordinateur. Ce type de maliciel s'avère bénin par rapport à d'autres rançongiciels: il n'inflige aucun dommage aux fichiers de l'ordinateur, qu'il est relativement aisé de déverrouiller ensuite.

Il est généralement possible d'éliminer le maliciel en analysant l'ordinateur avec la dernière version d'un *antivirus Live CD*. Des instructions sur la manière de créer et d'utiliser un tel CD figurent sur le site du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI).[1]

Une infection bien plus lourde de conséquences, due à Cryptolocker, a été observée en Suisse pour la première fois en novembre 2013. Ce maliciel crypte, et donc rend inaccessibles à la victime, toutes les données stockées sur son disque dur et sur les supports de données lui étant raccordés. Tout porte à croire que ce maliciel est plutôt peu répandu en Suisse. Pourtant, derrière chaque cas se cache une histoire personnelle dramatique: des particuliers ont ainsi perdu tout leur passé numérique. Quant aux PME, les données commerciales disparues peuvent menacer leur survie, si elles n'ont pas fait de *backup* ou si la sauvegarde de leurs données est défectueuse.

Cryptolocker semble se répandre à travers l'annexe infectée de courriels ou, sur des pages spécialement préparées, lors d'infections par «drive-by download». Dans quelques cas, la machine était déjà infectée par un autre maliciel, qui a chargé plus tard Cryptolocker. Des imitateurs ont entre-temps développé et mettent en circulation des logiciels similaires.

Après l'infection, les escrocs transmettent une demande d'argent à leur victime. En contrepartie, ils promettent d'envoyer la *clé* permettant de restaurer ses fichiers. Divers antivirus parviennent certes déjà à trouver et à éliminer le maliciel. Or c'est généralement trop tard, les fichiers se trouvant sur l'ordinateur ayant déjà été cryptés. Le vrai problème réside donc moins dans l'élimination du maliciel que dans la restauration des données d'origine. Dans les anciens rançongiciels intégrant un cryptage des données de l'utilisateur, la clé était une valeur programmée par défaut, qu'il était facile d'extraire du *code source*. Ce n'est plus le cas avec Cryptolocker: une clé différente est générée par victime et est sauvegardée sur un *serveur de commande et contrôle* (C&C Server). Il ne semble donc pas y avoir pour le moment de méthode permettant de décrypter les données sans la clé, que les pirates sont seuls à connaître. MELANI déconseille toutefois d'entrer en matière et d'envoyer de l'argent aux criminels. En effet, rien ne garantit qu'ils enverront réellement à la victime la clé nécessaire pour décrypter ses données, et il n'est pas exclu que les escrocs exploitent la bonne volonté manifestée par elle pour formuler de nouvelles exigences.

[1] Instructions du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) sur la manière de créer un Live CD: www.cybercrime.admin.ch/content/kobik/fr/home/dokumentation/informationen/2012-07-06.html

MELANI a déjà pris des mesures avec les fournisseurs de services Internet (ISP) afin de réduire la menace due à Cryptolocker.

Cryptolocker souligne clairement l'importance d'effectuer régulièrement des sauvegardes externes (*backups*) et de s'assurer de leur qualité.

Le facteur aggravant dans le cas de Cryptolocker tient à ce qu'il s'en prend aussi aux disques durs externes raccordés à l'ordinateur. Dans un cas particulièrement tragique, Cryptolocker a sévi pendant un processus de sauvegarde et détruit à la fois les données originales et celle du backup. Il est donc recommandé d'utiliser deux disques durs externes à tour de rôle et de ne les raccorder qu'au moment de la sauvegarde.

Jusqu'ici, les *lecteurs réseau* ne sont pas victimes de ce cryptage, tant qu'ils ne sont associés à aucune *lettre de lecteur*. Mais le maliciel sera certainement perfectionné, de façon à inclure peut-être un jour cette fonction et d'autres encore.

3.2 Bannières publicitaires répandant des maliciels

Les *AdServers* ont pour finalité de diffuser des publicités en ligne. La publicité peut émaner de différents annonceurs ou réseaux publicitaires. Parmi les AdServers bien connus et souvent utilisés figurent OpenX, et le logiciel se basant sur OpenX Revive Adserver. Un AdServer constitue une cible de choix pour les escrocs, en facilitant la diffusion des maliciels, sous forme de publicité manipulée, via plusieurs sites Web parfois très fréquentés. Une tactique répandue consiste à ajouter à la bannière publicitaire un *Iframe*. Soit un élément *HTML* permettant d'insérer des contenus Web externes – p. ex. sous forme de renvoi à une page déjà infectée.

Pour aggraver les choses, des lacunes de sécurité plus nombreuses ont été découvertes au semestre passé dans OpenX. Le risque est d'autant plus réel que dans bien des cas, les administrateurs ne procèdent pas régulièrement aux mises à jour.

C'est ainsi qu'une faille de sécurité découverte en juillet 2013 dans l'AdServer OpenX permet aux cybercriminels d'introduire n'importe quel script ou du code HTML (*cross-site scripting*). En août 2013, on a appris que la version en libre accès d'OpenX contenait depuis longtemps une *porte dérobée*. Les utilisateurs de cette version installaient automatiquement cette porte dérobée que les escrocs avaient aménagée dans le logiciel pour parvenir à leurs fins, et dont ils se servaient activement. En septembre, une autre faille d'OpenX et de Revive a été identifiée, permettant à n'importe quel utilisateur enregistré d'exécuter sur le serveur le *code PHP* de son choix. En décembre enfin, une dernière grave lacune identifiée concernait à la fois OpenX et Revive. Elle permettait d'accéder directement à la banque de données du serveur (*injection SQL)* et d'y manipuler les données de l'AdServer sans même en posséder les données d'accès.

En Suisse, différents sites parfois très consultés ont été victimes d'incidents. MELANI recommande de façon générale de régulièrement mettre à jour tous les logiciels exposés à Internet, et de prévoir pour eux une gestion de cycle de vie (*life cycle management*). Il convient par ailleurs de régulièrement vérifier leurs fichiers journaux et d'en examiner les

anomalies. Les mesures de protection des systèmes de gestion de contenu (*content management system, CMS)*[2] valent par analogie pour les AdServers. Enfin, il existe une liste de contrôle[3] des principales opérations à effectuer régulièrement avec OpenX et Revive.

3.3 Sites Web compromis plusieurs fois

Le lancinant problème des *pages de phishing* se pose encore. Alors que dans le passé les cybercriminels créaient des domaines ad hoc pour placer leurs pages de phishing, ils préfèrent aujourd'hui traquer les vulnérabilités des sites Internet existants et, le cas échéant, y créer une page de phishing (généralement dans un sous-répertoire). Comme signalé dans le dernier rapport semestriel MELANI[4], la découverte de sites Web présentant des *vulnérabilités* demande peu d'efforts. Beaucoup d'exploitants de sites négligent d'actualiser régulièrement leurs *logiciels d'application* – p. ex. systèmes de gestion de contenu (CMS).

L'une des priorités de MELANI consiste à éliminer au plus vite du réseau Web les pages de phishing en activité. Dès qu'une telle page est repérée, MELANI écrit à l'adresse de contact de l'hébergeur (*cellule abus*), en le priant de désactiver le site Web en question. Selon l'usage international, chaque hébergeur dispose aujourd'hui d'une cellule abus, qui prend note des annonces de sites frauduleux.

Les processus et délais de réaction en vue de la désactivation des sites frauduleux ne sont toutefois pas réglés de façon uniforme et varient fortement. Alors que certains fournisseurs bloquent aussitôt de tels sites, d'autres informent d'abord leur propriétaire, en l'invitant à adopter les mesures nécessaires. Ces fournisseurs n'interviennent qu'en cas d'absence de réaction dans le délai qu'ils ont fixé.

La disponibilité des cellules abus varie également beaucoup d'un cas à l'autre. Alors que certains hébergeurs fournissent un service 24h/24, d'autres ne travaillent qu'aux heures de bureau. D'où des retards, notamment si l'hébergeur se trouve dans une autre zone horaire ou si l'incident de phishing survient le week-end ou un jour férié.

Or tout comme la vitesse de réaction et la disponibilité, la manière de traiter les incidents varie d'un cas à l'autre. A supposer qu'une faille de CMS ait servi à placer une page de phishing, il ne suffit pas de supprimer cette page. En outre, il faut faire comprendre au propriétaire du site Web qu'il doit absolument actualiser ses applications. S'il omet de le faire, les mêmes sites Web feront à tout moment l'objet de réclamations à cause de la réapparition de pages de phishing ou de maliciels. Un cas observé au deuxième semestre 2013 en Suisse le montre bien: entre octobre et décembre 2013, le même site Web suisse a servi à trois reprises à placer des pages de phishing contre divers prestataires de services financiers ou sociétés de cartes de crédit.

Les hébergeurs n'ont aucune obligation de créer une cellule abus. Mais si la surveillance d'un réseau laisse à désirer, il sera rapidement placé sur une liste noire (*black list*). C'est notamment le cas pour les pourriels. Si un polluposteur sévit sur un réseau et si le

[2] MELANI, Listes de contrôle et instructions: Mesures de prévention pour les systèmes de gestion de contenu (CMS) http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=fr (état: le 20 février 2014).

[3] https://checkpanel.com/checklist-templates/openx-maintenance (état: le 20 février 2014).
https://checkpanel.com/checklist-templates/revive-maintenance (état: le 20 février 2014).

[4] MELANI, rapport semestriel 2013/1, chapitre 5.4:
http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

fournisseur d'accès n'intervient pas, il arrive fréquemment qu'un filtre antipourriel bloque sa plage d'adresses *(IP range)*, et donc que ses clients ne puissent plus envoyer de courriels. Ce principe n'est toutefois pas appliqué systématiquement aux pages de phishing, et donc les hébergeurs disposent d'une marge de manœuvre pour traiter ce genre de cas.

3.4 Professionnalisation de l'arnaque à l'avance de frais

Comme dans le cas des données de cartes de crédit, les vols de données d'accès aux comptes de messagerie se multiplient. Or à quoi peuvent bien servir ces données? Les précédents rapports semestriels ont déjà signalé la variante de courriels consistant en faux appels au secours, dont l'expéditeur prétend être bloqué à l'étranger et en proie à de grandes difficultés.[5] Comme le compte est tombé aux mains d'un pirate, celui-ci peut faire croire à sa victime que la communication émane bel et bien de la personne connue d'elle. La victime est ensuite pressée de verser une somme d'argent.

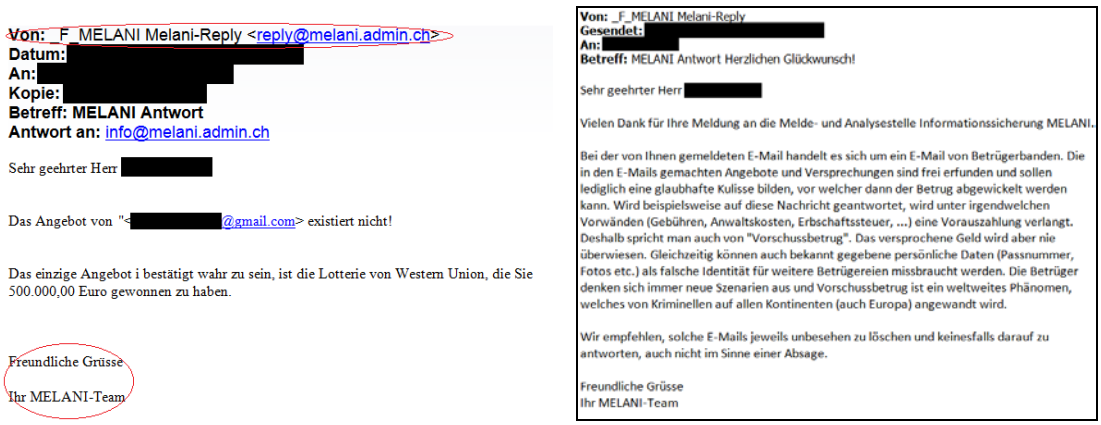
Une autre variante régulièrement observée consiste à passer au crible les courriels, à la recherche d'une communication avec un établissement financier. Les escrocs tenteront ensuite de reprendre contact avec l'employé de banque concerné pour le persuader d'effectuer un paiement. Cette variante a beau être surtout observée à l'étranger, on en trouve aussi des cas isolés en Suisse.

MELANI a découvert à fin 2013 une variante bien plus perfide. Tout avait commencé par un simple courriel d'arnaque à l'avance de frais. Un tel message fait à chaque fois miroiter à la victime de juteux bénéfices ou une grosse somme prélevée sur un héritage. Si la victime a mordu à l'hameçon, elle est invitée à verser des avances prétendument nécessaires (impôts sur les bénéfices, sur les successions ou les transactions, etc.). Elle ne verra toutefois jamais la couleur de l'argent promis.

Dans le cas d'espèce, la victime sceptique avait décidé de demander à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) si le courriel était authentique et s'il fallait donner suite à l'offre reçue. Comme toujours en pareil cas, MELANI l'a invitée dans une réponse standard à ne pas donner suite à ce genre de courriels, à les effacer et surtout à ne jamais prendre contact avec les escrocs. Chose surprenante, la victime a réagi en demandant une nouvelle fois par écrit si MELANI pensait vraiment que l'opération était en ordre et qu'il fallait payer d'avance les taxes réclamées.

Intriguée par ce malentendu, MELANI a téléphoné à l'auteur du message pour bien expliquer que ce courriel était frauduleux et qu'il ne fallait en aucun cas effectuer de paiement. Il s'est avéré lors de cet appel que les pirates avaient manipulé le courriel de MELANI dans la boîte aux lettres de la victime pour l'encourager à verser de l'argent. Les escrocs disposaient donc, pour cette manipulation, de l'accès nécessaire à son compte de messagerie.

[5] MELANI rapport semestriel 2012/1, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: le 20 février 2014).



Von: _F_MELANI Melani-Reply <reply@melani.admin.ch>
Datum: [redacted]
An: [redacted]
Kopie: [redacted]
Betreff: MELANI Antwort
Antwort an: info@melani.admin.ch

Sehr geehrter Herr [redacted]

Das Angebot von "<[redacted]@gmail.com> existiert nicht!

Das einzige Angebot i bestätigt wahr zu sein, ist die Lotterie von Western Union, die Sie 500.000,00 Euro gewonnen zu haben.

Freundliche Grüsse

Ihr MELANI-Team

Von: _F_MELANI Melani-Reply
Gesendet: [redacted]
An: [redacted]
Betreff: MELANI Antwort Herzlichen Glückwunsch!

Sehr geehrter Herr [redacted]

Vielen Dank für Ihre Meldung an die Melde- und Analysestelle Informationssicherung MELANI.

Bei der von Ihnen gemeldeten E-Mail handelt es sich um ein E-Mail von Betrügerbanden. Die in den E-Mails gemachten Angebote und Versprechungen sind frei erfunden und sollen lediglich eine glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Wird beispielsweise auf diese Nachricht geantwortet, wird unter irgendwelchen Vorwänden (Gebühren, Anwaltskosten, Erbschaftssteuer, ...) eine Vorauszahlung verlangt. Deshalb spricht man auch von "Vorschussbetrug". Das versprochene Geld wird aber nie überwiesen. Gleichzeitig können auch bekannt gegebene persönliche Daten (Passnummer, Fotos etc.) als falsche Identität für weitere Betrügereien missbraucht werden. Die Betrüger denken sich immer neue Szenarien aus und Vorschussbetrug ist ein weltweites Phänomen, welches von Kriminellen auf allen Kontinenten (auch Europa) angewandt wird.

Wir empfehlen, solche E-Mails jeweils unbesehen zu löschen und keinesfalls darauf zu antworten, auch nicht im Sinne einer Absage.

Freundliche Grüsse
Ihr MELANI-Team

Fig. 1: Courriel falsifié par des escrocs (à gauche) et courriel original de MELANI (à droite).

3.5 Relevés bancaires envoyés à la fausse adresse

Une erreur de programmation a généré, à la banque Coop, l'envoi d'un certain nombre de relevés de compte de fin d'année aux mauvais destinataires. La banque a élucidé entre-temps les causes de ces envois erronés, liés à l'introduction d'un nouvel aperçu des points du programme Supercard auquel participe l'établissement. Les clients ayant reçu par erreur les décomptes d'autres personnes ont été priés de les retourner à l'expéditeur. La banque Coop a promis de prendre toutes les mesures utiles pour éviter qu'une telle erreur ne se répète.

A Bâle-Ville, siège de la banque, le Ministère public a annoncé l'ouverture d'une enquête policière pour soupçon de violation par négligence du secret bancaire.

Ce cas n'est pas une première. En février 2014 par exemple, l'entreprise d'audit financier PricewaterhouseCoopers (PWC) avait dans un cas similaire envoyé certains certificats de salaire aux mauvais employés.[6] Dans les TIC, la tendance est à l'usage de programmes toujours plus complexes, comportant un nombre croissant de fonctions. Or il va de soi que le risque d'erreur augmente proportionnellement aux lignes de programmation. A fortiori si les applications ne peuvent être modifiées ou actualisées qu'en phase d'exploitation. Car malgré tous les essais réalisés en amont sur les systèmes test, il n'est pas possible de tester toutes les interactions que comportent de tels programmes.

3.6 Vol de données du système Schengen: la Suisse également touchée

En décembre, différents médias suisses ont relayé une information faisant état d'un vol de données ayant touché la base SIS (système d'information Schengen). Le SIS est un système d'information dans lequel peuvent être signalés les objets volés et les personnes recherchées par la police à des fins d'extradition, sous le coup d'une interdiction d'entrée ou encore portées disparues. Les autorités policières et douanières des pays membres de l'Espace Schengen ont accès à cette base de données.

[6] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/PWCMitarbeiter-erhalten-Lohnausweise-der-Kollegen/story/26934239 (état:le 20 février 2014).

L'accès indu a eu lieu en 2012, à travers une faille de sécurité chez la société gérant la base de données pour la police danoise. De par la nature transnationale du SIS, une faille concerne potentiellement d'emblée des données saisies par l'ensemble des pays ayant accès au système. La Suisse a ainsi été informée en mai 2013 de la faille. Il s'avère que sur les 1,2 million de données volées, 26'478 ont été entrées par les autorités suisses. Le fichier subtilisé contient des données personnelles ainsi que des données codées faisant notamment référence aux raisons de l'entrée dans la base. Ces dernières ne sont pas directement interprétables, et il n'est donc en principe pas possible de lier des actes à des personnes figurant dans la liste. La faille concerne uniquement le système SIS 1, remplacé dès mai 2013 par SIS 2.

Les détails de l'attaque (méthode utilisée, faille) et les motivations des auteurs sont encore peu clairs et ne seront vraisemblablement pas rendus publics avant la fin des investigations menées au Danemark. Les autorités danoises ont cependant précisé avoir corrigé la faille utilisée. Différents éléments ont par ailleurs été révélés par les autorités allemandes, dans le cadre d'une réponse aux questions d'un député. Ces dernières avancent l'hypothèse d'une attaque peu ciblée et ne visant pas spécifiquement SIS, mais ayant exploité une faille sur un serveur contenant également d'autres données. Deux hackers, danois et suédois, seraient impliqués.

Cet incident illustre la question capitale de la spécification et de l'implémentation des systèmes d'échange international de données délicates et sensibles. Bien souvent, les décisions politiques prises à propos de tels systèmes précisent en premier lieu le genre de données à échanger. Les exigences techniques liées à implémentation sont soit traitées comme si elles étaient d'importance secondaire, soit laissées au bon vouloir de chaque pays. Au risque qu'une mise en œuvre imparfaite dans un Etat membre affecte aussi les données d'autres pays. Il faudra dorénavant insister, dans tout projet d'échange d'informations, afin qu'au-delà des données à échanger, un standard minimum obligatoire pour tous les pays soit aussi défini au préalable quant à la sûreté de l'information ou aux modalités de traitement et de transmission technique.

3.7 NZZ inaccessible – problèmes techniques

Le 19 août 2013, certains visiteurs n'ont pas pu accéder au site Web de la NZZ. L'incident a d'abord été attribué à une cyberattaque. Or selon Swisscom, cette panne partielle était due à une erreur lors de la prolongation de l'enregistrement du domaine entre le registraire Network Solutions et Swisscom.

Le domaine ip-plus.net de Swisscom était enregistré à ce moment-là auprès de la société Network Solutions. Or celle-ci ayant stoppé le service de ce *domaine* le 19 août 2013 à 12h40, il n'a plus été possible de résoudre ip-plus.net, devenu inactif. Et comme les *services DNS* d'entreprises tierces – dont NZZ – fonctionnaient sous ce domaine, leurs sites sont logiquement aussi devenus inaccessibles. Swisscom a certes résolu le problème dès 15h25. De son côté le service informatique de NZZ avait aussitôt supprimé, parmi les inscriptions DNS à disposition, tous les serveurs touchés par la panne, pour les remplacer par des serveurs fonctionnant. Mais comme les mauvaises configurations restent à chaque fois stockées 24 heures dans le serveur de noms et dans l'antémémoire (*Internet Explorer Cache*), il a fallu attendre jusqu'à 24 heures pour que tous les services refonctionnent normalement.[7]

[7] http://www.nzz.ch/aktuell/digital/nzz-dns-1.18135806 (état: le 20 février 2014).

Suite à cet incident, Swisscom a immédiatement mis en place des mesures afin d'éviter qu'un évènement similaire ne se reproduise.

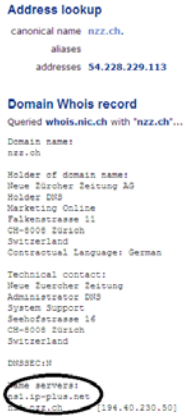


Fig. 2: Données Whois de la NZZ affichées par le serveur DNS d'ip-plus.net

Le système de noms de domaine (DNS) rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP il suffit aux utilisateurs de composer un nom d'adresse (URL). Sans serveur DNS, Internet continuerait à fonctionner, mais il faudrait indiquer à la place des URL les numéros IP. Tout au sommet de la hiérarchie figurent les serveurs racine, qui renseignent sur le Top-Level-Domain ou domaine de premier niveau (p. ex. .com, .net, .ch). Les niveaux inférieurs (domaines de second niveau) sont administrés par une foule de prestataires Internet, petits ou grands. Une panne ou une manipulation peuvent être lourdes de conséquences, surtout quand il s'agit comme ici d'un important serveur DNS d'une grande entreprise.

3.8 Victoire suisse à la première Coupe des Alpes de cybersécurité

Afin de prévenir une pénurie de spécialistes en cybersécurité tout en facilitant la tâche des milieux économiques à la recherche de talents, l'association Cyber Security Austria (CSA) a lancé en 2012 le Défi de la cybersécurité. Lors de cette compétition organisée avec l'appui du Kuratorium Sicheres Österreich (KSÖ) et des services de renseignement de l'armée, des centaines d'écoliers se sont affrontés sur Internet pour gagner une place en finale.

L'association Swiss Cyber Storm, placée sous l'égide de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et de l'association Swiss Police ICT, a repris l'idée en 2013.[8] D'où la décision d'organiser, sous le patronage de Cyber Security Austria, une compétition internationale – en élargissant au passage le champ des participants aux étudiants. La Coupe des Alpes de cybersécurité était née.

Sa première édition a eu lieu du 5 au 7 novembre 2013 à Linz. Après une première journée consacrée à des activités visant à forger l'esprit d'équipe et à amener les participants à mieux se connaître, la compétition proprement dite s'est déroulée le deuxième jour. Pendant plus de onze heures, les deux équipes d'Autriche et de Suisse se sont efforcées de déchiffrer des codes, de trouver des failles de sécurité et d'accéder à des téléphones

[8] MELANI rapport semestriel 2013/1, chapitre 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

portables et à des tablettes. Il ne suffisait pas d'attaquer l'adversaire, il fallait encore prendre des mesures pour empêcher tout accès illicite. L'équipe suisse a finalement remporté la compétition, recevant le trophée du vainqueur lors d'une cérémonie organisée au Musée d'histoire militaire de Vienne, en présence de nombreux invités des milieux politiques, militaires et économiques.

Ni l'idée de créer, sous la forme d'une compétition de cybersécurité, une plateforme destinée à la recherche de talents et à l'encouragement de la relève, ni le succès de la première Coupe des Alpes de cybersécurité ne sont passés inaperçus. Ainsi l'Allemagne participera à la prochaine édition. En Suisse, les épreuves de qualification se dérouleront à nouveau dans le cadre de la conférence Swiss Cyber Storm, dont la cinquième édition aura lieu le 22 octobre 2014 au KKL (Centre de la culture et des congrès de Lucerne). Les écoliers et les étudiants intéressés peuvent d'ores et déjà s'inscrire à l'adresse www.verbotengut.ch.

3.9 Apparition de maliciels sur les systèmes Linux

Les maliciels ne s'en prennent pas qu'aux systèmes Windows (Microsoft) et OSX (Apple), mais aussi à Unix / Linux. Au deuxième semestre 2013, MELANI a appris que divers systèmes Unix / Linux avaient été infectés par un *rootkit* sophistiqué du nom d'Ebury. Les pirates s'étaient introduits, d'une manière qui n'a pas encore été élucidée, dans ces systèmes afin d'y installer le *rootkit* Ebury. La tactique consiste habituellement à modifier le démon SSH (*SSH-daemon*) installé sur le système de la victime pour se faire livrer les données d'accès de tous les utilisateurs s'annonçant par la suite au système infecté via SSH. En outre, le rootkit Ebury dérobe les clés SSH privées présentes dans le système. Grâce aux données d'accès dérobées, les pirates peuvent en tout temps accéder au système infecté et l'utiliser à des fins illégales, comme l'hébergement (*hosting*) de *serveurs C&C* ou l'envoi de *pourriels*.

Comme Ebury est un maliciel doté des fonctions de rootkit, il est très difficile à détecter sur les systèmes compromis. En outre, Ebury utilise comme canal de communication entre la machine infectée et les criminels un protocole DNS. L'infection s'avère d'autant plus difficile à découvrir dans bien des cas.

Des compléments d'information sur Ebury et sur la manière de détecter ce maliciel figurent sur le site de l'organisme allemand CERT-Bund.[9]

Les logiciels libres (*open source*) passent souvent, à juste titre, pour être une alternative à l'emploi des solutions qualifiées de «propriétaires». Or la logique voulant que l'*open source* soit transparent, et donc plus sûr, est réductrice. Il est vrai que tout le monde peut analyser le code source de tels programmes afin d'en traquer les erreurs. Mais dans l'hypothèse où, faute de l'avoir trouvée, la communauté ne corrigerait pas une faille, les solutions *open source* demeurent un vecteur d'attaque. D'où l'importance, en cas d'usage professionnel de telles solutions, de faire tester le logiciel par une équipe interne en réfléchissant aux priorités de l'entreprise, afin de ne pas dépendre des intérêts de la communauté Open Source. Tout raisonnement économique effectué préalablement au choix entre une solution Open Source ou un *système propriétaire* devrait tenir compte de cette réalité.

[9] https://www.cert-bund.de/ebury-faq (état: le 20 février 2014).

3.10 Attaques par amplification NTP – infrastructures suisses compromises

Ces derniers mois à nouveau, les attaques par déni de service distribué (*Distributed Denial Of Service*, DDoS) ont fait partie des méthodes les plus prisées par les pirates pour limiter sinon empêcher l'accès à certains services ou sites Web. Différentes variantes entrent en ligne de compte: le deuxième semestre 2013 a été marqué non seulement par une forte recrudescence des attaques par amplification DNS[10], renforcées par un facteur de 20 à 50 (voir rapport semestriel MELANI 2013/1[11]), mais aussi par un détournement analogue, pour lancer des attaques DDoS, du *protocole NTP* servant à synchroniser l'horloge locale via Internet. L'astuce des pirates consiste à demander des données aux serveurs NTP, en falsifiant l'adresse de l'expéditeur. Bien plus volumineuse que la question, la réponse parviendra à l'adresse faussement prise pour celle de l'expéditeur, alors qu'il s'agit de la victime. Et comme les réponses consistent en des données légitimes provenant de serveurs autorisés, il est très difficile de neutraliser ce genre d'envois. Les attaques NTP sont plus redoutables encore que celles par amplification DNS, avec un facteur de renforcement de 500 parfois.[12] MELANI a eu la confirmation que plusieurs serveurs NTP basés en Suisse avaient déjà servi à mener ce genre de cyberattaques.

Les attaques NTP font appel à la commande «monlist» – activée par défaut sur les anciens appareils.[13] Cette commande publie une liste des 600 dernières *adresses IP* s'étant connectées au serveur NTP. Moyennant une falsification de l'adresse d'origine de la requête, il est possible de transmettre cette liste complète à la victime.

Pour éviter qu'une machine mal configurée ne serve à lancer de telles attaques, il est possible de désactiver la fonction «monlist» ou d'employer la dernière version de NTP, sur laquelle la prise en charge de cette commande est désactivée par défaut.

Face à la recrudescence des attaques DDoS, il est recommandé à chaque entreprise dont l'activité commerciale dépend de l'accessibilité de son site Web et/ou de sa connexion à Internet de vérifier les risques inhérents à ce genre d'attaques et de prévoir des mesures de défense. Outre l'adoption de mesures techniques de détection et de prévention, il faut aussi typiquement évaluer les capacités de son fournisseur Internet, ainsi que ses obligations contractuelles en cas d'incident.

[10] Une attaque par amplification DNS consiste à adresser à des serveurs publics (résolveurs DNS) des requêtes DNS truquées. Comme l'adresse IP source a été falsifiée, les réponses parviendront à l'adresse IP de la victime et non à l'expéditeur réel du paquet de données.

[11] MELANI rapport semestriel 2013/1, chapitre 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

[12] http://www.zdnet.de/88184056/rekord-ddos-angriff-europa-erreicht-400-gbits/?ModPagespeed=noscript (état: le 20 février 2014).

[13] https://www.us-cert.gov/ncas/alerts/TA14-013A (état: le 20 février 2014).

4 Situation internationale de l'infrastructure TIC

4.1 Nouvelles révélations sur la NSA et le GCHQ

Au deuxième semestre 2013, divers journalistes ayant eu accès aux documents d'Edward Snowden ont continué d'alimenter le débat public sur les pratiques des services de renseignement, notamment américains (National Security Agency, NSA) et britanniques (General Communication Headquarter, GCHQ). Après les premières révélations concernant Prism, XKeyscore et Tempora, dont MELANI avait parlé dans son précédent rapport semestriel[14], l'image s'est confirmée au deuxième semestre d'un enregistrement à grande échelle et systématique des données par les services de renseignement américains et britanniques. On a ainsi appris que par analogie au programme britannique Operation Tempora, la NSA gère un programme du nom d'Upstream[15] afin d'accéder aux données transitant par les réseaux à fibres optiques. En 2013, la NSA aurait déboursé 278 millions de dollars pour cette collaboration avec les entreprises de télécommunication américaines.[16] Par ailleurs, un projet commun à la NSA et au GCHQ, connu sous le nom de code Muscular, vise à intercepter les connexions aux centres de calcul de Google et Yahoo.[17] Le document publié estime à 181 millions les jeux de données capturés en 30 jours. Autre ordre de grandeur, une présentation datée de 2012 montre que la NSA aurait infecté avec des maliciels, au niveau mondial, 50 000 réseaux informatiques pour accéder à des données sensibles.[18] Enfin, un document publié en janvier 2014 fait état de 100 000 ordinateurs infiltrés par la NSA.[19]

Les débats n'ont pas uniquement porté sur l'ampleur de telles pratiques, mais également sur les cibles visées. En effet, la NSA avait toujours prétendu agir au nom de la lutte contre le terrorisme. Or des chefs d'Etat et des diplomates ayant été pris pour cibles, il est rapidement apparu que les investigations avaient aussi une composante politique. En Amérique latine, la mise sous écoute de la présidente brésilienne Dilma Rousseff, de son homologue mexicain Peña Nieto et de son prédécesseur Felipe Calderón a suscité l'indignation.[20] Au niveau international, il a beaucoup été question de la surveillance des communications lors du sommet du G8/G20 de Toronto[21], et en Europe la mise sous écoute du téléphone mobile de la chancelière allemande Angela Merkel a fait les gros titres.[22]

---

14 MELANI rapport semestriel 2013/1, chapitre 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

15 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (état: le 20 février 2014).

16 http://www.heise.de/newsticker/meldung/Ueberwachungsaffaere-NSA-zahlt-Hunderte-Millionen-Dollar-an-Provider-1945984.html (état: le 20 février 2014).

17 http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (état: le 20 février 2014).

18 http://www.spiegel.de/netzwelt/netzpolitik/nsa-soll-50-000-netzwerke-weltweit-infiltriert-haben-a-935335.html (état: le 20 février 2014).

19 http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (état: le 20 février 2014).

20 http://www.bbc.co.uk/news/world-latin-america-23938909 (état: le 20 février 2014).

21 http://www.spiegel.de/netzwelt/netzpolitik/kanada-erlaubte-nsa-spionage-bei-g-8-gipfel-a-936255.html (état: le 20 février 2014).

22 http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html (état: le 20 février 2014).

Une autre action de piratage rendue publique était baptisée Operation Socialist[23]. Il s'agissait d'une attaque contre la filiale de Belgacom BICS (joint-venture de Belgacom, de Swisscom et du groupe sud-africain MTM). Parmi les gros clients de cette entreprise télécom figurent la Commission européenne, le Conseil de l'Union européenne et le Parlement européen.

Operation Socialist / attaque contre BICS

Au moment des divulgations concernant la NSA, Belgacom avait mené sa propre enquête et constaté la présence d'une attaque, d'abord attribuée à la NSA. Après de nouvelles révélations, les soupçons se sont reportés sur le GCHQ, les Britanniques ayant repris la technologie américaine. Le projet au nom de code «Operation Socialist» visait à espionner Belgacom et à connaître en détail son infrastructure. Selon la présentation divulguée, les ordinateurs du personnel de Belgacom avaient été infectés de manière ciblée, puis des tentatives avaient été faites pour accéder aux routeurs centraux permettant l'itinérance (*roaming*).

Ce cas concerne directement la Suisse, puisque Swisscom possède une participation de 24 % dans BICS. Or Swisscom appartient à hauteur de 51 % à la Confédération, et donc aux contribuables suisses.

Norme de cryptage corrompue?

L'un des principaux enjeux de la sûreté de l'information est de savoir dans quelle mesure les programmes et normes de cryptage sont encore dignes de confiance. Il a surtout été question de la norme Dual_EC_DRBG, générateur de nombres aléatoires développé par la NSA qui, en réalité, ne s'en remettrait pas uniquement au hasard. En décembre 2013, on a appris que la NSA aurait versé dix millions de dollars à la société RSA-Security pour qu'elle intègre par défaut ce générateur controversé dans son logiciel BSAFE, commercialisé dans le monde entier.[24] RSA a certes démenti ces affirmations, mais la NSA n'a pas jugé utile de réagir.

Limites du cryptage – Bullrun et Edgehill

Il ressort des données publiées que le GCHQ comme la NSA s'attaquent de façon très systématique au défi du décryptage.[25] [26] Ces deux services secrets ont apparemment mis en place, au cours des dernières années, toute une série de mesures et techniques destinées à déjouer les solutions de cryptage. Un aspect évoqué plus haut consiste à affaiblir les générateurs aléatoires. Une fois ceux-ci manipulés, le cryptage a beau sembler résistant, il devient possible de le percer avec une puissance de calcul relativement modeste. Une autre possibilité consiste à acquérir des clés pour décrypter en temps réel ou plus tard les données cryptées.

Enfin, on sait depuis décembre 2013 que la NSA parvient à casser l'algorithme de chiffrement de flux (*stream cipher*) A5/1, soit la méthode la plus utilisée au niveau mondial

[23] http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (état: le 20 février 2014).

[24] http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (état: le 20 février 2014).

[25] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (état: le 20 février 2014).

[26] https://www.schneier.com/blog/archives/2013/10/defending_again_1.html (état: le 20 février 2014).

pour crypter les flux de données entre un téléphone mobile et une antenne-relais.[27] D'où la possibilité d'écouter les appels et de lire les messages transmis.

La NSA aurait encore la possibilité de s'immiscer dans les systèmes et d'y recueillir les données avant leur cryptage. Cette tâche incombe à une division ad hoc de la NSA, appelée TAO (Tailored Access Operation).[28]

D'autres thèmes ont été beaucoup discutés dans le contexte de l'affaire Snowden:

Royal Concierge

L'hebdomadaire allemand Spiegel a publié en novembre 2013 un article sur le programme de surveillance Royal Concierge, exploité par le service de renseignement britannique GCHQ. Il permet de surveiller au niveau mondial les réservations faites dans au moins 350 hôtels de luxe et d'y constater la présence de diplomates ou hauts fonctionnaires.[29]

Piratage indirect de TOR

Le *service d'anonymisation* TOR intéresserait beaucoup la NSA, selon une présentation elle aussi publiée par Snowden. La NSA n'a certes pas obtenu un accès direct au réseau TOR pour en découvrir tous les utilisateurs. Mais il paraît possible d'espionner des utilisateurs individuels de ce service, en tirant parti de failles des navigateurs Firefox. La présentation précise toutefois que ce ne serait possible qu'au prix d'une analyse manuelle, et encore pour un petit nombre d'utilisateurs de TOR.[30]

Follow the Money – SWIFT

L'opinion publique suisse s'est surtout offusquée que la NSA puisse espionner le fournisseur de services financiers SWIFT. Un des trois centres de calcul de SWIFT se trouve en effet à Diessenhofen en Thurgovie. Jusqu'à 15 millions de transactions financières s'y font par jour. Il a même été dit dans ce contexte que la NSA entretiendrait une division baptisée «Follow the Money», chargée d'espionner les données financières. SWIFT a toutefois déclaré qu'il n'y avait aucune raison de penser que son réseau ait été victime de la moindre effraction illégale.[31]

La stratégie SIGINT («Signals Intelligence Strategy»), adoptée par la NSA en février 2012 et publiée dans le New York Times en novembre 2013, aide à mieux comprendre la manière d'agir des services de renseignement américains:
«Ensure Signals Intelligence provides THE decisive edge in advancing the full spectrum of U.S. national security interests.» In order to fulfil this vision, it is ready to «Defeat adversary

---

[27] http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (état: le 20 février 2014).

[28] http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html (état: le 20 février 2014).

[29] http://www.spiegel.de/netzwelt/netzpolitik/royal-concierge-britischer-geheimdienst-ueberwacht-diplomatenhotels-a-933997.html (état: le 20 février 2014).

[30] http://www.zdnet.de/88171545/nsa-arbeitet-sich-an-anonymisierungsdienst-tor-ab/?ModPagespeed=noscript (état: le 20 février 2014).

[31] http://www.nzz.ch/aktuell/schweiz/swift-bestreitet-nsa-spionage-1.18151215 (état: le 20 février 2014).

cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere».[32]

Autrement dit, la NSA devrait être à même de se procurer en tout temps et partout les données de n'importe qui. Les publications et données divulguées jusqu'ici confirment qu'il ne s'agit pas de paroles en l'air. Bien au contraire, la NSA et ses partenaires suivent à la lettre cette stratégie. Il est encore trop tôt pour juger de l'impact qu'auront ces révélations sur le développement d'Internet.[33] Mais des voix autorisées prédisent déjà la fin du Web sous sa forme actuelle. A l'avenir, les utilisateurs d'Internet, que ce soit à titre professionnel ou privé, devront sérieusement prendre en compte les révélations de Snowden et leur impact au niveau de l'évaluation du risque.

4.2 APT - renouvellement des méthodes

«NetTraveler» est une *APT* («advanced persistent threat») ayant été exposée par Kaspersky en juin 2013. Les cibles étaient des sociétés actives dans l'industrie, dans la production d'énergie, les télécommunications et les nouvelles technologies, ou alors des entités gouvernementales. Puis en septembre, Kaspersky a livré quelques éléments témoignant d'un renouvellement de cette APT, qui intègre désormais de nouveaux vecteurs d'attaques. Si par le passé, NetTraveler a déjà largement fait usage de *spear phishing* pour diffuser du code malicieux, l'utilisation d'une méthode de type *watering hole* n'avait pas été observée jusque-là[34]. L'exploitation d'une faille de sécurité du logiciel *Java,* révélée par les chercheurs de FireEye, est également nouvelle.

L'opération Molerats a été rendue publique par la société FireEye en octobre 2012. Elle visait des cibles gouvernementales en Israël, mais également en Palestine, et aurait été menée depuis le Moyen-Orient. Ce groupe semblait alors privilégier XtremeRAT, maliciel répandu et souvent associé à des attaquants originaires de la région. De nouvelles révélations faites par FireEye en août 2013 attestent que désormais, ce même groupe utilise Poison Ivy dans le cadre d'attaques menées aux Etats-Unis et au Moyen-Orient. Poison Ivy est un autre maliciel très répandu, souvent associé à des acteurs chinois. Son utilisation par des attaquants originaires d'une autre zone géographique est par contre inédite.

Ces deux exemples témoignent de la grande capacité d'adaptation et de l'opportunisme dont font preuve les groupes menant des attaques de type APT. Les méthodes et outils utilisés par ces groupes ne sont pas figés, mais peuvent évoluer et être redéfinis en fonction des circonstances ou de la cible. Toute analyse doit dûment prendre en compte cette capacité de renouvellement.

Ce constat a notamment une implication au stade de l'attribution d'une attaque. C'est tout un faisceau d'éléments qu'il faut prendre en considération avant de se risquer à émettre un jugement. Une approche trop mécanique, basée uniquement sur les modus operandi et les outils utilisés, s'avère généralement hasardeuse. On ne peut faire abstraction des motifs et intentions, de l'identité des victimes et des conséquences.

---

[32] http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?pagewanted=all (état: le 20 février 2014).

[33] Voir à ce sujet le chapitre 5.1 du présent rapport

[34] MELANI rapport semestriel 2013/1, chapitre 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

4.3 Vol de millions de données de clients d'Adobe

L'un des plus spectaculaires vols de mots de passe jamais commis a été annoncé au début d'octobre. La victime était Adobe. Alors qu'il était question dans un premier temps de 2,9 millions de données de clients, mots de passe et données de cartes de crédit, Adobe a corrigé quelques semaines plus tard le chiffre à 38 millions.[35] Un autre fichier apparu, d'une taille de 3,8 GB, renfermerait même 150 millions de données d'utilisateurs et de mots de passe *hachés*. Mais Adobe n'a pas confirmé officiellement ces allégations. Selon Adobe, le vol a porté sur des données de cartes de crédit et des mots de passe cryptés. Pour décrypter les données, il fallait une clé de sécurité (*3DES*), que les pirates ne sont probablement pas parvenus à dérober. Ils ont néanmoins pu voir sans cryptage les indices de mots de passe, dont certains étaient suffisamment explicites. Par exemple, l'indice «1-6» correspondait à la combinaison chiffrée «123456». Et comme la clé 3DES utilisée était toujours la même, tous les mots de passe identiques se présentaient de la même façon une fois cryptés, ce qui a permis de regrouper les mots de passe identiques. Ces indices ont servi à dresser la liste des 100 mots de passe les plus fréquents, et à la publier.[36] On ne peut que s'étonner du nombre élevé d'utilisateurs ayant choisi un mot de passe très simple. Cette négligence peut être due à un manque de sensibilisation aux risques, ou alors au fait que les clients jugent certains comptes ou mots de passe «sans valeur» – soit qu'ils les destinent à un seul achat, soit qu'ils pensent que les comptes en question ne renferment pas de données à protéger.

Une fois l'attaque connue, Adobe a réinitialisé tous les mots de passe. Les 38 millions de clients directement concernés selon Adobe ont été informés par courriel et invités à changer de mot de passe.

Outre les données des utilisateurs, les pirates pourraient s'être procuré les *codes source* des produits Adobe ColdFusion, Acrobat et Photoshop. L'attaque remonterait à août 2013.

Indépendamment de tous les ennuis que cause un tel incident, une bonne communication avec la clientèle s'avère importante pour limiter au maximum les dommages. Adobe a réinitialisé tous les mots de passe et envoyé à ses clients un courriel d'information sur l'attaque, en les invitant à choisir un nouveau mot de passe.

L'envoi de tels courriels doit être mûrement réfléchi. D'abord, ils risquent bien de servir de modèles à de nouvelles attaques (phishing). Ensuite, les internautes sont devenus très méfiants et prompts à croire que de tels courriels invitant à changer de mot de passe sont frauduleux. MELANI a ainsi reçu de nombreux messages de citoyens se demandant si ce courriel d'information émanait réellement d'Adobe. Enfin, une communication désinvolte risque de rendre les clients imprudents, le jour où ils recevront un courriel d'arnaque.[37]

En pareil cas, il faut garder à l'esprit que les utilisateurs ne réservent pas un mot de passe à un seul service, mais qu'ils le reprennent pour d'autres. Autrement dit, le vol d'un mot de passe avec l'adresse électronique correspondante permet aux pirates d'accéder à d'autres prestations en ligne.

35 http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ (état: le 20 février 2014).

36 http://stricture-group.com/files/adobe-top100.txt (état: le 20 février 2014).

37 MELANI rapport semestriel 2012/1, chapitre 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: le 20 février 2014).

4.4 Attaques visant les points de vente Target

En décembre, plusieurs articles confirmés par un communiqué de presse de la chaîne de magasins Target ont rendu publique l'attaque de très grande ampleur dont cette dernière a été victime. Les informations publiées font état du vol des détails de 40 millions de cartes de crédit et débit, ainsi que des données personnelles concernant 70 millions de clients.

L'attaque a eu lieu pendant la période extrêmement active commercialement qui précède les fêtes de fin d'année, entre le 27 novembre et le 15 décembre. Target a d'abord communiqué de manière extrêmement lapidaire sur l'incident. Ce n'est que petit à petit, au fil des recherches et révélations publiées par différentes sources, qu'il a été possible de reconstruire en partie les circonstances de l'attaque et les méthodes utilisées. Lors de la rédaction du présent rapport, certains aspects restaient cependant toujours incertains.

Les premières analyses, confirmées par Target, précisent que l'intrusion a eu lieu par un maliciel ayant infecté les terminaux de *points de vente*.[38] En l'occurrence, les soupçons se portent sur le maliciel BlackPOS ou une de ses variantes, qui aurait été vraisemblablement implémenté par des bandes criminelles d'Europe de l'Est. Ce maliciel parvient à copier les données contenues sur la bande magnétique de la carte, dans les instants qui suivent son utilisation sur le terminal de paiement, alors qu'elles sont contenues en clair dans la mémoire vive (*RAM*). Cette méthode, connue sous le nom de ram scraping, avait déjà fait l'objet de mises en garde, notamment par des communiqués de VISA au cours de l'été.[39] Les questions centrales de l'exfiltration des données et de la compromission initiale («entry point») n'ont obtenu des éléments de réponse qu'après plusieurs semaines et suite à différentes révélations et prises de position. L'entreprise Target a tout d'abord imputé l'intrusion à un vol de données d'accès au réseau chez l'un de ses fournisseurs. Des révélations successives ont ensuite désigné un fournisseur précis, en l'occurrence une entreprise gérant son système de chauffage et d'air conditionné. Les données d'accès auraient été obtenues suite à l'envoi de courriels contenant un maliciel spécialisé dans le vol de mots de passe. Les autorisations dont disposait ce fournisseur auraient alors permis aux criminels d'accéder au système de paiement pour y installer le maliciel chargé d'intercepter les données.

Ce cas a été suivi en janvier par la révélation d'une attaque similaire ayant touché la chaîne de magasins Neiman Marcus. Là encore, des données issues de la bande magnétique des cartes de crédit utilisées ont été saisies juste après utilisation. Les deux cas semblent recourir à des méthodes proches, sans que l'on puisse affirmer pour l'instant avec certitude que les mêmes criminels étaient à l'œuvre. Enfin, différentes sources relèvent que plusieurs autres enseignes seraient touchées, sans que ces dernières aient été identifiées jusqu'ici.

Le piratage ayant visé Target, mais également d'autres cas similaires, rappellent les risques posés par l'utilisation de cartes de crédit fonctionnant avec une simple bande magnétique. Ce système, encore très répandu aux Etats-Unis, bénéficie d'un niveau de sécurité nettement inférieur aux systèmes fonctionnant par carte à puce et *PIN*. En effet, il est relativement facile d'intercepter les données d'une telle carte de crédit. La plupart du temps, les données ainsi saisies sont revendues à travers des sites et forums spécialisés, avec comme but final la fabrication de cartes de crédit falsifiées.

[38] MELANI a parlé des failles des terminaux de points de vente (POS) dans son rapport semestriel 2012/2, au chapitre 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: le 20 février 2014).

[39] http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (état: le 20 février 2014).

Une autre problématique soulevée par cet incident est celle des prestataires de services intervenant sur le réseau de l'entreprise et possédant des droits élargis. Comme cela a été démontré ici, ces derniers sont autant de points d'entrée potentiels pour une attaque.

4.5 Deuxièmes cartes SIM et conséquences

Il avait été question, dans le dernier rapport semestriel, d'attaques contre les téléphones mobiles permettant aux pirates d'intercepter les transactions sécurisées de e-banking par le protocole *mTAN*[40]. On sait depuis octobre 2013 que d'autres attaques exploitent les failles non pas techniques mais organisationnelles. Des escrocs ont ainsi réussi en Allemagne, selon divers témoignages rendus publics, à compromettre des applications de e-banking protégées par mTAN grâce à une deuxième *carte SIM* (subscriber identity module). Il leur avait suffi de se faire envoyer une carte SIM additionnelle à l'adresse de leur choix, pour dérober et utiliser à leur guise les codes mTAN.

Une carte SIM garantit que la communication se fait avec l'autorisation de l'utilisateur. Si une personne est en possession de cette carte, elle peut en principe accéder au réseau de téléphonie mobile au nom de l'utilisateur légitime. Selon la politique de l'opérateur, il est possible ou non d'utiliser en parallèle plusieurs cartes SIM. A supposer qu'il n'accepte qu'une seule carte, les deux cartes SIM se perturbent la plupart du temps.

Outre cette restriction technique, l'enjeu organisationnel est de savoir quelles mesures de sécurité les opérateurs de téléphonie prévoient lors de la remise de cartes SIM. Et comme la téléphonie mobile donne accès à un nombre croissant de services essentiels, la sécurité des appareils ainsi que des opérateurs de téléphonie mobile passe au premier plan.

4.6 Algorithme DES piraté et conséquences pour les cartes SIM

En juillet 2013 Karsten Nohl, ingénieur allemand expert en cybersécurité, a publié les premiers résultats de ses recherches sur la sécurité des cartes SIM. Il en ressort que plusieurs millions de cartes SIM utilisées dans le monde présenteraient une faille de sécurité et risqueraient d'être compromises. Un pirate un peu malin pourrait p. ex. usurper l'identité de l'utilisateur, espionner ses appels ou manipuler les paiements effectués par l'infrastructure de téléphonie mobile.[41]

Les réseaux des opérateurs de téléphonie mobile communiquent régulièrement avec les cartes SIM, à l'insu de leurs propriétaires. L'accès à distance aux données des cartes SIM s'effectue par liaison radio, selon la technologie OTA (*over the air*). D'où la possibilité d'installer des mises à jour ou d'échanger des informations. Or Karsten Nohl remet en question le cryptage censé protéger la communication entre l'opérateur et la carte SIM. Concrètement, il s'agit de la norme de chiffrement DES (Data Encryption Standard), développée dès les années 1970 et que certaines applications continuent d'utiliser. L'algorithme DES, qui utilise des clés de 56 bits seulement, était depuis longtemps devenu

[40] MELANI rapport semestriel 2013/1, chapitre 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

[41] https://srlabs.de/rooting-sim-cards/ (état: le 20 février 2014). http://www.heise.de/security/artikel/DES-Hack-exponiert-Millionen-SIM-Karten-1920898.html (état: le 20 février 2014).

obsolète. Selon Nohl, il serait possible de découvrir la clé de chiffrement de certaines cartes SIM utilisant la norme DES.

Une fois en possession de cette clé, le pirate a la possibilité de lancer une série d'attaques contre la carte SIM et son propriétaire. Nohl est parvenu à infiltrer un quart des cartes SIM testées, en s'engouffrant dans cette faille de sécurité. On estime qu'au niveau mondial, 500 millions de cartes SIM sont encore exposées à ce risque. Les cartes plus récentes, basées sur la norme de chiffrement ayant remplacé DES, sont à l'abri de telles attaques.

La faille de sécurité publiée risque d'occasionner de sérieux dommages aux utilisateurs d'une carte SIM protégée par la méthode DES. Le marché suisse n'est pas concerné. Consultées par MELANI, les entreprises suisses de télécommunication ont confirmé que la norme DES n'est plus utilisée en Suisse.

4.7 Systèmes de contrôle industriels et domotiques

SCI reliés au réseau et installations domestiques télécommandées

MELANI a déjà signalé à maintes reprises les risques que comporte la tendance à raccorder au réseau toujours plus d'appareils de pilotage des processus physiques, dans l'industrie productive comme en domotique.[42] Cette évolution technique multiplie les possibilités d'accéder aux systèmes à distance, d'en consulter les données voire de contrôler les appareils en question. Les systèmes dotés d'une fonction d'interrogation et de commande à distance sont désormais répandus et avantageux, tout comme l'intégration aux installations existantes d'une interface de communication. Une telle offre répond fréquemment à un désir de la clientèle. Il est commode d'enclencher le chauffe-eau ou de rendre la température agréable avant son arrivée dans son appartement de vacances ou encore de s'assurer, à partir d'une tablette tactile ou d'un smartphone, que l'on a bien éteint la cuisinière et toutes les lumières à la maison. Les gérants immobiliers apprécient également de pouvoir surveiller et piloter à distance les systèmes domotiques. Il en va de même pour les microcentrales hydroélectriques et autres installations sans personnel présent en permanence, dont les exploitants apprécient de pouvoir en contrôler le bon fonctionnement et d'y opérer certains réglages depuis chez eux.

Or tout système prévoyant un *accès à distance* légitime s'expose à des accès abusifs, soit directement soit par infiltration d'un appareil agréé, sachant que «tout ce qui est accessible par le réseau peut être piraté.»[43] La mise en réseau des systèmes de contrôle industriels ainsi que le pilotage de la domotique par les TIC suscitent toujours plus l'intérêt des experts en sécurité. Ces dernières années, diverses failles de sécurité ont été identifiées dans de tels produits ou dans leurs paramètres.[44]

Les systèmes avec réglage à distance s'acquittent de multiples tâches, et d'éventuelles manipulations peuvent avoir des conséquences fâcheuses: si un chauffe-eau est éteint, les habitants devront prendre des douches froides; l'allumage inutile des projecteurs d'éclairage d'un stade occasionne un gaspillage d'électricité et d'argent; et en cas de blocage d'une ligne de production industrielle, toute l'usine risque d'être paralysée, situation catastrophique pour l'entreprise comme pour la main-d'œuvre.

---

42 Par exemple: MELANI rapport semestriel 2013/1, chapitre 4.5: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

43 «If you can ping it, you own it!» Kyle Wilhoit, The SCADA That Didn't Cry Wolf, 2013.

44 http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities (état: le 20 février 2014).

Enfin, on pourrait imaginer un scénario d'enclenchement et de déclenchement coordonnés d'un maximum d'appareils, qui compromettrait la stabilité du réseau électrique. Il est donc indispensable de veiller non seulement au bon fonctionnement et à la convivialité des solutions d'accès à distance, mais aussi à leur protection contre toute manipulation interdite.

Les TIC soutiennent en premier lieu les processus opérationnels. Néanmoins, le recours aux TIC a toujours aussi des implications physiques et procédurales à ne pas perdre de vue.

MELANI a publié en octobre 2013 une liste de contrôle visant à protéger les systèmes de contrôle industriels.[45]

Bonnes pratiques de l'OSCE visant à réduire les cyberrisques du secteur énergétique

L'Organisation pour la sécurité et la coopération en Europe (OSCE) a publié à l'intention des Etats et des entreprises énergétiques privées un guide pour mieux protéger leurs infrastructures contre d'éventuels attentats cyberterroristes.[46] Le titre a beau se référer à une problématique spécifique, le document l'examine sous un angle très large et recommande des mesures générales, également valables dans d'autres secteurs de l'industrie et dont les effets sur la prévention et la résilience vont bien au-delà des attentats terroristes. L'OSCE plaide pour une meilleure prise de conscience (awareness rising) grâce à la formation, pour une coopération accrue de tous les acteurs et pour davantage d'échanges d'information. De nombreuses voix plaident pour de telles mesures, que l'OSCE a formulées ici pour le secteur de l'énergie non nucléaire. L'atome a certes été volontairement écarté pour éviter tout conflit de compétences avec les régulateurs de ce domaine – mais les recommandations de l'OSCE sont également dignes d'intérêt pour les exploitants de centrales nucléaires.

Tous les acteurs européens du secteur très fragmenté, mais toujours plus interconnecté de l'alimentation en énergie partagent une même responsabilité quant à la sécurité d'approvisionnement. L'enjeu paraît d'autant plus essentiel que beaucoup d'autres secteurs sont tributaires d'un approvisionnement énergétique stable, en électricité notamment. Pour compliquer les choses, les réseaux électriques intelligents en plein essor accroissent les risques: les dispositifs supplémentaires de contrôle-commande à distance ont beau offrir aux fournisseurs de nouvelles possibilités bien commodes, ils donnent aux acteurs mal intentionnés des opportunités supplémentaires de s'immiscer dans l'approvisionnement énergétique. D'où la nécessité de tenir dûment compte de la sécurité des composantes «intelligentes» de l'approvisionnement énergétique.

4.8 Conflit syrien – guerre de l'information 2.0

La Syrian Electronic Army (SEA) est un groupe de pirates favorables au régime du président syrien Bashar al-Asad. Mais ses liens avec le pouvoir restent flous. A ses propres dires, la SEA ne ferait pas partie du gouvernement et ne bénéficierait d'aucun soutien étatique. Elle serait plutôt formée de patriotes luttant sur Internet contre des comptes rendus jugés mensongers de la guerre civile syrienne.
Durant le semestre écoulé, la SEA s'est acharnée sur les sites d'information (New York Times, BBC News, Al-Jazeera, etc.) et a même réussi à compromettre les comptes Twitter

[45] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=fr (état: le 20 février 2014).

[46] «Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace», http://www.osce.org/atu/103500 (état: le 20 février 2014).

d'agences de renseignement comme Reuters et Associated Press (AP), afin d'y déployer sa propre propagande ou d'y répandre de fausses nouvelles.[47]

«La vérité est la première victime de la guerre», relevait le poète grec Eschyle il y a 2500 ans. L'apparition d'Internet et en particulier des médias sociaux a «démocratisé» la conduite de la guerre de l'information. Toute intervention étatique est devenue superflue. Il suffit désormais, pour diffuser aux quatre coins de la planète des informations – vraies ou mensongères –, d'un raccordement Internet et d'un fait divers qui frappe les esprits.

Il est aisé d'infiltrer, par des méthodes comme le *spear phishing*, les comptes de médias sociaux et les autres canaux d'information qui identifient par leurs seuls noms d'utilisateur et mot de passe leurs visiteurs, qui pourront le cas échéant faire un travail de désinformation. Il faudrait donc protéger autant que possible les canaux et plateformes d'information sensibles par un mécanisme d'*authentification à deux facteurs*.

Outre ces mesures techniques, il importe d'analyser et de définir préalablement les moyens et canaux qui permettraient de démentir ou corriger le plus efficacement possible les fausses nouvelles, afin d'éviter tout climat de panique aux conséquences funestes.

4.9 Attaques DDoS pour brouiller les pistes

Une tendance apparue en 2013 est celle *d'attaques* par déni de service distribué *(DDoS)* de relativement faible intensité, cherchant à faire diversion. Le phénomène, relayé par divers experts ou articles, se base en particulier sur des cas ayant touché des banques américaines. Tandis que les responsables de sécurité étaient occupés à traiter l'attaque par déni de service sur le site Web de l'entreprise ou son portail e-banking, une autre attaque plus sérieuse était à l'œuvre simultanément. En l'occurrence, les attaques visaient le système de virement de la banque et non pas des comptes de particuliers. En outre, l'énorme quantité de requêtes figurant dans le fichier journal complique l'analyse de l'incident.

Une attaque DDoS, bien qu'il faille la traiter comme telle, doit également inciter à élever le niveau d'attention face à la potentialité d'autres attaques. A fortiori si l'attaque est de relativement faible intensité.

4.10 Pirates et contrebandiers à la fois

Entre 2011 et 2013, plusieurs conteneurs maritimes ont «disparu» du port d'Anvers. L'enquête menée par les autorités de poursuite pénale a révélé que des contrebandiers s'étaient servis des conteneurs légaux pour leur trafic de stupéfiants. Concrètement, les criminels s'étaient introduits dans les systèmes informatiques des entreprises logistiques afin d'y découvrir l'emplacement des conteneurs où était cachée la drogue et de les dérober avant que leurs propriétaires légitimes en prennent possession.

Tout avait commencé par de simples courriels de subversion psychologique (*social engineering*), invitant les employés à ouvrir une *annexe* et du même coup à installer des

[47] Voir rapport semestriel MELANI 1/ 2013, chapitre 4.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

programmes d'espionnage. La découverte de ces incidents a conduit les entreprises logistiques touchées à renforcer leur sécurité informatique. Les pirates se sont alors introduits physiquement dans leurs bureaux pour y installer du matériel manipulé, afin de continuer d'obtenir les informations requises – notamment les codes de sécurité permettant aux chauffeurs d'accéder au site et d'y chercher certains conteneurs.

Dans de nombreux secteurs économiques, l'infrastructure informatique est devenue indispensable à la planification et à la bonne exécution du travail. En particulier, les tâches logistiques complexes seraient impossibles à maîtriser sans systèmes informatiques. En outre, de nombreuses sociétés logistiques souhaitent connaître en tout temps l'emplacement de leurs livraisons et de leurs véhicules. Si l'allocation des ressources et la fourniture des prestations y gagnent en efficience, ces renseignements se prêtent également à des actions criminelles ciblées. Sans compter que les manipulations de telles données risquent d'entraver la bonne marche des affaires. Les systèmes TIC restent pourtant un moyen parmi d'autres de soutenir certains processus d'exploitation. Il est dès lors prioritaire que les directions d'entreprises soient pleinement conscientes de l'impact de tels systèmes sur le monde réel et sur leurs procédures de travail.

Comme tout marché, le marché noir d'Internet a entamé un processus de spécialisation et de professionnalisation. Cette tendance est observable depuis plusieurs années. Les pirates ne sont plus seulement de jeunes curieux cherchant à explorer les limites du possible, mais toujours plus des techniciens avertis et désireux de monnayer leurs aptitudes. Dans le cas d'espèce, les contrebandiers semblent avoir recruté les pirates par Internet. Le marché au noir d'Internet permet visiblement de trouver du personnel capable d'accomplir n'importe quelle besogne.

4.11 Tour de vis bruxellois contre les cybercriminels

Les cybercriminels encourent désormais des peines plus sévères dans l'Union européenne. En adoptant la directive 2013/40/UE, le Parlement européen a décidé le 12 août 2013 de durcir les sanctions applicables aux attaques contre les systèmes d'information. Le but est notamment d'harmoniser la législation et les mesures répressives des Etats membres, sachant que les attaques et les escroqueries ont souvent un caractère international et que de telles pratiques sont sanctionnées différemment d'un pays à l'autre. L'uniformisation du cadre pénal crée en outre les bases nécessaires à une fructueuse coopération judiciaire.

La directive prévoit des peines d'emprisonnement d'au moins deux ans. La création de *réseaux de zombies* sera passible d'au moins trois ans d'emprisonnement. Les criminels qui s'attaquent à des infrastructures critiques comme les centrales électriques, les réseaux de transport ou les réseaux publics s'exposent à au moins cinq ans d'emprisonnement. Il en va de même pour les infractions commises non individuellement, mais dans le cadre d'une organisation criminelle, ou des cyberattaques qui causent un préjudice grave.

La directive énonce en outre des obligations spécifiques aux autorités tant policières que judiciaires. Les Etats membres sont priés d'échanger des informations sur les cyberattaques, afin de garantir le bon fonctionnement des réseaux. Pour améliorer encore ces échanges d'information, les services compétents devront apporter une réponse aux demandes urgentes dans un délai de huit heures.

Cette nouvelle orientation a essentiellement pour but l'harmonisation de principe des normes pénales en vigueur dans les Etats membres. Expérience à l'appui, les poursuites se heurtent souvent, dans les cas d'activité cybercriminelle transfrontière, à des limites formelles liées aux différences d'approche des pays en matière de procédure pénale. Sera-t-il en outre

possible de durcir les sanctions pénales? Tout dépendra de la volonté des Etats membres de transposer fidèlement ce cadre général dans leur droit interne.

5 Tendances / Perspectives

5.1 Tournant en vue pour Internet ou statu quo?

Au fur et à mesure de la publication de documents attestant des pratiques de la NSA et d'autres services de renseignement, des voix se sont exprimées ces derniers mois sur l'avenir du réseau Internet. Comme on pouvait s'y attendre, les avis vont dans toutes les directions. Dans un article Bruce Schneier[48], expert en sécurité, dénonce une trahison fondamentale d'Internet et des valeurs que ce média symbolise. Il souligne le paradoxe voulant que par leurs actes les Etats-Unis – leader du monde libre – aient conforté dans leurs opinions les Etats totalitaires qui, depuis toujours, ont aspiré à une nationalisation d'Internet. La crainte d'une «balkanisation d'Internet» conduit déjà Vinton Cerf, vice-président de Google, à prédire le déclin du Web sous sa forme actuelle.[49] Avec le repli national qui s'annonce et l'hétérogénéité croissante du marché qui s'ensuivra, Internet perdra à ses yeux tout intérêt économique pour les entreprises. Même ses adeptes, qui voyaient dans Internet l'expression de la démocratie de base et l'invention libératrice par excellence, se montrent critiques. Ils y voient désormais la plateforme idéale pour surveiller les gens, et regrettent d'avoir naïvement cru qu'il en serait autrement.

Internet semble certes rester très vivant et, à court terme du moins, rien ne devrait changer à son statut. Mais il est permis de considérer, au vu des activités de certains services de renseignement dont témoignent les documents divulgués par Snowden, que de nombreux milieux ont définitivement perdu la confiance jusque-là accordée à Internet.

Ces activités montrent encore les problèmes flagrants que pose un outil transnational dont chaque individu ou Etat peut faire l'usage qu'il entend, dans les limites du droit national, sans se préoccuper des conséquences systémiques de ses actes. Si au niveau technique, tel ou tel pays modifie selon son bon plaisir les normes de sécurité internationales ou amène ses propres entreprises, par des mesures de contrainte, à lui livrer secrètement toutes sortes d'informations afin d'accéder commodément et à grande échelle aux données utiles à sa sécurité intérieure, il est susceptible de bafouer les règles de la bonne foi et de nombreux ordres juridiques nationaux. Internet aide sans doute les fonctionnaires du pays en question à réaliser leurs objectifs de surveillance. On oublie alors apparemment que l'avidité et la loi du moindre effort en matière de collecte étatique d'informations et de données personnelles sont discutables d'un point de vue libéral et démocratique.

Ainsi, les entreprises du secteur TIC ont beau être des acteurs globaux, elles restent soumises en fin de compte à des ordres juridiques nationaux différents et pas toujours cohérents. Un tel constat ne vaut pas seulement pour les entreprises actives dans le secteur TIC. D'où l'urgence de rechercher un véritable consensus sur des principes fondamentaux applicables à Internet et aux acteurs concernés.

---

[48] http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying (état: le 20 février 2014).

[49] http://www.tagesanzeiger.ch/digital/internet/GoogleVize-warnt-vor-Untergang-des-Internets/story/12499111 (état: le 20 février 2014).

Dans ce sillage, il s'agit aussi de restaurer la confiance dans la communauté chargée de la sécurité informatique. Soit un climat de confiance entre les organes préposés à la sûreté de l'information, ainsi que des échanges internationaux qui visent en premier lieu à protéger les réseaux, les produits et applications. Or le fait qu'aux Etats-Unis p. ex. l'autorité compétente en la matière (Information Assurance Directorate, IAD) soit subordonnée au chef de la NSA qui, de par son cahier des charges, ne peut s'intéresser uniquement à la sécurité des produits et à la robustesse des normes, rend les choses plus compliquées. De même, le fait que des CERTs responsable de l'échange d'information international pour la protection des réseaux relèvent des unités Signal Intelligence offensive n' aboutit pas nécessairement à rassurer les CERT des autres Etats sur les intentions de ce partenaire. Et pourtant, il incombe principalement à cette communauté technique et à son système supranational d'échange d'information de consolider Internet, soit la sécurité de ses composantes, afin de freiner les tendances isolationnistes et de restaurer la confiance générale nécessaire dans ce domaine.

Les considérations sur la mort d'Internet, qui existe depuis près de 25 ans, semblent certes exagérées. Mais la tâche s'annonce difficile pour restaurer la confiance fondamentale nécessaire au réseau, et pour amener les acteurs de la sécurité informatique à se faire à nouveau confiance les uns aux autres. Il ne sera pas simple non plus d'apporter une solution pratique à un défaut de construction majeur du Web: l'usage du droit national prévaut dans un système transnational comme Internet, alors que son application déploie concrètement des effets extraterritoriaux. Surtout, il faudra mener la discussion à tous les niveaux, des acteurs chargés de la politique de sécurité aux forums plurilatéraux s'occupant des normes et exigences et dont font partie les milieux économiques, directement concernés.

Dans tous les cas, il faudra tirer un bilan et en revenir à l'idée de base d'Internet, conçu comme un système décentralisé et hautement résistant, se prêtant à la transmission de l'information. La sécurité et la confidentialité de ces informations étaient étrangères à cette vision, ou du moins n'y jouaient qu'un rôle secondaire. La sécurité et la confidentialité étaient ainsi au départ, et resteront à l'avenir, du ressort de celles et ceux qui confient des informations et des données à Internet.

5.2 Bitcoin - succès et rançon du succès

Fonctionnement

Bitcoin est une monnaie électronique décentralisée, ce qui signifie que son fonctionnement ne dépend d'aucun émetteur central. Cet aspect la différencie des devises traditionnelles, mais également de nombreuses autres monnaies électroniques.

Deux types d'acteurs principaux cohabitent dans Bitcoin. Les utilisateurs sont représentés par leur porte-monnaie, qui consiste en une paire de clés cryptographiques publique/privée. On peut considérer par analogie la clé publique comme étant le numéro de compte, vers lequel il est possible de transférer de l'argent. La clé privée permet de signer une transaction, c'est-à-dire d'effectuer un paiement.

Pour que le paiement soit effectif, il convient encore de le valider. C'est dans ce processus qu'intervient le réseau des mineurs, qui sont les deuxièmes acteurs majeurs du système. Concrètement, ces derniers participent à la constitution de la «chaîne de blocs», qui est le cœur du fonctionnement de Bitcoin. Il s'agit d'une sorte de livre comptable regroupant toutes les transactions confirmées, consultable par tous les utilisateurs. Ce processus de validation, appelé minage, vise à confirmer les transactions en attente en les incluant dans un bloc. La validation d'un bloc nécessite la résolution par un mineur d'une preuve de travail (proof of work). Cette étape demande une forte puissance de calcul et est rémunérée en Bitcoins, ce

qui engendre une augmentation de la masse monétaire en circulation. L'intégrité de la chaîne de bloc est centrale, puisque pour qu'une nouvelle transaction soit autorisée, il doit être possible de lui faire correspondre une recette antérieure enregistrée par le donneur d'ordre. Sans cette trace, un utilisateur pourrait en effet signer une transaction totalement irréaliste.

Il existe trois manières principales de se procurer des Bitcoins: en participant au minage, en faisant rémunérer une prestation contre des Bitcoins ou en faisant l'acquisition sur une plateforme d'échange, qui permet d'échanger des Bitcoins contre une devise «classique». Les Bitcoins peuvent ensuite être utilisés dans les magasins acceptant ce mode de paiement. Le caractère anonyme des transactions utilisant Bitcoin est souvent évoqué et mérite d'être précisé. L'utilisateur est théoriquement anonyme, puisqu'il n'est identifié que par la détention d'une *clé cryptographique*. En revanche, au contraire de ce qui existe dans le système bancaire classique, les transactions sont publiques.

Enjeux sécuritaires

La popularité croissante de Bitcoin soulève de nombreuses questions, tant au niveau sécuritaire qu'à propos du statut légal et de la réglementation de telles devises.

Plusieurs événements récents démontrent clairement que les Bitcoins et leurs utilisateurs sont devenus des cibles intéressantes pour les criminels et que les méthodes utilisées afin d'acquérir frauduleusement des Bitcoins varient. Différentes attaques et incidents de sécurité ont ainsi été répertoriés ces derniers mois, avec des niveaux de complexité et des cibles variées.

La clé privée, et à travers elle le propriétaire du porte-monnaie, est généralement la cible la plus attrayante. En effet, la confidentialité du porte-monnaie repose exclusivement sur cette clé, et la sécurité de son stockage est donc centrale. De nombreux utilisateurs ont fait l'objet d'attaques visant cet élément. De plus, des services Web proposent également de conserver les clés de leurs clients. Au vu de la centralisation des porte-monnaie et des sommes importantes que cela peut représenter, ces sites sont devenus des cibles de choix. L'un de ces services, input.io, a par exemple été victime en juillet 2013 d'un vol de Bitcoins, pour une valeur de 1,2 million de dollars.

Les plateformes d'échange sont une autre cible potentielle. En décembre, le marché de change Bitcoin Suisse a reconnu avoir été victime d'une attaque. Cette dernière a été couronnée de succès, malgré un modus operandi extrêmement peu perfectionné et relevant principalement de la subversion psychologique (*social engineering*). En l'occurrence, les pirates se sont adressés au fournisseur de compte e-mail de la plateforme, en se faisant passer pour Bitcoin Suisse. Ils ont alors demandé le changement des mots de passe, demande à laquelle le fournisseur a accédé. Le responsable de Bitcoin Suisse a entre-temps changé de fournisseur, sans préciser si les pirates ont utilisé les identifiants pour commettre des activités délictueuses. Des attaques d'autres types visant également des bourses d'échange ont été observées. Une tendance marquée est notamment celle d'attaques par déni de service distribué (DDoS). Dans certains cas, les attaquants ont exigé le paiement d'une rançon contre l'arrêt de l'attaque, selon un modus operandi connu. D'autres attaques de ce type semblent avoir d'autres buts. On a par exemple signalé certaines manœuvres semblant avoir eu comme finalité de déstabiliser le marché, poussant le cours du Bitcoin à la baisse en vue d'acheter par la suite à meilleur prix. La volatilité du cours des Bitcoins et les possibles manœuvres spéculatives inhérentes sont ici au centre des préoccupations.

Un dernier angle d'attaque consiste à viser les gains générés par l'activité de minage. En début d'année 2014, un maliciel transmis à travers des publicités (ads) figurant sur différents sites du groupe Yahoo a été détecté. Ce dernier présente la particularité d'utiliser la

puissance de calcul des ordinateurs victimes, afin de leur faire effectuer un travail de minage à l'insu de leur propriétaire, et de générer ainsi des Bitcoins.

En plus de ces attaques, Bitcoin a régulièrement été évoqué du fait de son utilisation lors de transactions illégales. Bitcoin est notamment largement utilisé pour effectuer des transactions sur des plateformes offrant des produits illégaux, tel le site Silk Road, une plateforme de commerce électronique utilisée pour le marché-noir.

Ces différents enjeux sécuritaires soulignent une nouvelle fois le grand opportunisme dont savent faire preuve les criminels à l'œuvre sur Internet. Au succès d'un service ou comme ici d'un mode de paiement correspondent en règle générale très rapidement des attaques sur mesure. Comme utilisateur, il convient d'être conscient de ce risque, de la valeur des Bitcoins, et donc de la nécessité de les protéger. Cela passe tout d'abord par un stockage sûr. A ce niveau, il est recommandé de conserver la clé cryptographique privée sur un support électronique n'étant pas connecté à Internet ou sur papier (paper wallet). La sécurité générale de la machine, et notamment sa protection contre les infections, reste par ailleurs ici aussi centrale.

L'encadrement et la réglementation de l'usage des Bitcoins sont des aspects qui devraient encore connaître d'importants développements. La popularité de cette monnaie et des préoccupations telles que les possibilités d'abus ou son extrême volatilité, incitent actuellement les Etats à s'y intéresser et plus précisément à envisager des règlementations. L'Allemagne a ainsi accordé le statut officiel de «monnaie privée» au Bitcoin. En Suisse, les deux derniers mois de l'année ont vu trois objets parlementaires s'intéresser au Bitcoin, plus précisément à ses risques et aux possibilités de lui offrir un statut légal.

5.3 Dimension cybernétique des conflits

De nombreux conflits ont désormais un volet cybernétique, à l'instar de l'actuel conflit syrien où est impliquée la Syrian Electronic Army[50]. On y relève surtout de la propagande et de la désinformation, mais également des attaques directes contre des infrastructures. On cite volontiers comme exemples l'attaque DDoS contre l'Estonie, les attaques DDoS contre les banques américaines ou celles survenues dans les deux Corées. L'emploi dans ce contexte des termes cyberguerre ou cyberterreur semble abusif, au vu des dommages effectifs. Car on associe automatiquement un attentat ou une guerre à la panique et à un climat de peur, à des blessés sinon des morts. Or jusqu'ici, le bilan des cyberattaques se limite à des pannes du système, des inconvénients ou des pertes financières.

Alternative à un conflit ouvert

L'histoire montre que les cyberattaques répondent au souci de lancer des opérations ciblées en évitant un conflit ouvert, alors que des opérations analogues aboutiraient à de graves querelles entre Etats, si elles étaient basées sur des armes conventionnelles. Typiquement, le maliciel Stuxnet visait à dérégler les centrifugeuses servant à enrichir l'uranium, dans les installations nucléaires iraniennes. La même intervention, mais menée avec des armes conventionnelles, aurait probablement déclenché un grave conflit dans la région.

[50] Voir plus haut, chapitre 4.8, et aussi rapport semestriel MELANI 2013/1, chapitre 4.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=fr (état: le 20 février 2014).

Des acteurs nombreux, aux mobiles variés

La multiplicité des acteurs et des motifs complique encore l'analyse. Une attaque DDoS contre une banque peut avoir un mobile criminel (chantage) ou alors résulter d'une idéologie, comme l'ont montré les attaques lancées par Anonymous contre des banques au cours des dernières années. On peut toutefois aussi penser à une implication étatique, p. ex. en cas de tentative ciblée d'affaiblir tout un système financier.

La question de l'attribution se posera d'autant plus souvent à l'avenir que divers pays ont reconnu l'énorme potentiel des personnes possédant des cybercompétences – dans les réseaux criminels notamment – et voudront en tirer parti. D'où la possibilité pour un tel Etat de commanditer des actions sans risquer ensuite de se les voir attribuer.

Attaques en perspective

Le risque d'une cyberattaque infligeant d'énormes dommages est-il donc faible? Il serait bien entendu possible de s'en prendre à des systèmes vitaux, dont une panne serait dramatique. Mais de telles attaques requièrent généralement de solides connaissances techniques et des informations privilégiées, et supposent un énorme travail. La sécurité fait en outre partie des priorités des systèmes vitaux. Il importe dès lors de ne pas penser uniquement aux risques de cyberattaques, mais également à la complexité croissante et à l'interconnexion toujours plus étroite des systèmes. Il en devient difficile de comprendre les liaisons et dépendances existantes. Un problème ou un dérangement pourraient ainsi avoir des effets imprévisibles. Il ne doit pas nécessairement s'agir d'une cyberattaque – les pannes peuvent elles aussi être lourdes de conséquences, et dans un système complexe la recherche des erreurs demande souvent un certain temps.

5.4 Détection des virus au 21e siècle – limites des bases de signatures

Histoire de la détection des virus

Le premier *virus* a été détecté en 1971. Il s'agissait de Creeper et il sévissait sur *ARPANET* (Advanced Research Projects Agency Network), l'ancêtre d'Internet. Creeper a été combattu à l'aide d'un programme baptisé «The Reaper». Même si l'on ne parlait pas encore de virus, «The Reaper» peut être considéré comme le premier antivirus de l'histoire. Entre-temps, des antivirus commerciaux existent depuis plus de 20 ans et ont donné naissance à une véritable industrie des antivirus. Où en est aujourd'hui cette industrie, et jusqu'à quel point de tels produits permettent-ils une défense efficace?

Un rapport de test publié en 2012 par le laboratoire «AV-Comparatives.org» indique un pourcentage étonnamment élevé de maliciels bloqués et de sites Web eux aussi bloqués, car porteurs d'une infection. Le taux de reconnaissance y dépasse 90 %:

Whole Product Dynamic "Real-World" Protection Test – (March-June) 2012 www.av-comparatives.org

Summary Results (March-June)

Test period: March – June 2012 (2159 Test cases)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	Cluster[5]
BitDefender	2150	-	9	99,6%	1
G DATA	2147	1	11	99,5%	1
Kaspersky	2146	2	11	99,4%	1
Qihoo	2143	6	10	99,4%	1
BullGuard	2131	21	7	99,2%	1
F-Secure	2135	10	14	99,1%	1
Avast	2110	28	21	98,4%	2
ESET	2117	1	41	98,1%	2
AVIRA	2107	13	39	97,9%	2
Sophos	2112	-	47	97,8%	2
Trend Micro	2108	-	51	97,6%	2
AVG	2103	6	50	97,5%	2
GFI	2102	-	57	97,4%	2
Panda	2097	-	62	97,1%	2
eScan	2094	-	65	97,0%	2
PC Tools	2024	126	9	96,7%	2
Tencent	2052	32	75	95,8%	3
Fortinet	2046	-	113	94,8%	3
McAfee	2041	6	112	94,7%	3
AhnLab	1999	-	160	92,6%	4
Webroot	1963	1	195	90,9%	4

Fig. 3: Rapport de test d'«AV-Comparatives.org»

A en croire cette statistique, les antivirus parviendraient à identifier et éliminer la plupart des virus. Or les conditions du test avaient été spécialement choisies. Tout en simulant un environnement réel, les auteurs avaient prévu que 40 à 50 % des adresses Web soumises pour analyse aboutissent directement à un maliciel, et les 50 à 60 % restants à un kit d'exploit (*exploit pack*). En sachant pertinemment que s'ils sont parfois démunis quand un maliciel s'attaque à l'ordinateur, les antivirus parviennent relativement bien à vérifier et détecter les kits d'exploits. D'où le taux de succès élevé obtenu.

Un test analogue réalisé par le CRDF Threat Center[51], agence Web française à but non lucratif, dans des conditions statiques et avec des analyses portant exclusivement sur la signature numérique des maliciels, a livré un résultat plus différencié. Certains antivirus ont certes identifié plus de 70 % des codes malveillants analysés. Mais d'autres n'en ont repéré que 1 à 3 %. Le taux de reconnaissance moyen avoisinerait 33 % selon cette étude.

[51] https://threatcenter.crdf.fr/?Stats (état: le 20 février 2014).

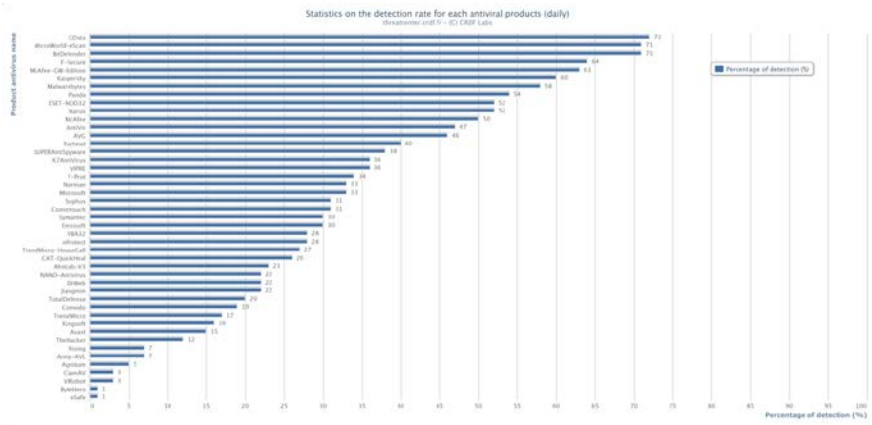


Fig. 4: Rapport de test du CRDF Threat Center

Mode opératoire des pirates, notamment dans le domaine de la criminalité économique

Pour éviter d'être repérés par les antivirus, les criminels modifient souvent plusieurs fois par jour leurs maliciels. Le code malveillant reste identique, mais il est empaqueté de façon inédite pour ne pas être repéré par les antivirus. Les criminels disposent même de plateformes spéciales qui vérifient combien d'antivirus, et lesquels, sont en mesure de détecter la nouvelle mouture d'un maliciel. Or à la différence des offres mises au point par les prestataires de sécurité[52], ces plateformes font très attention à ce qu'aucune information sur les nouveaux virus ne tombe entre les mains des fabricants d'antivirus.

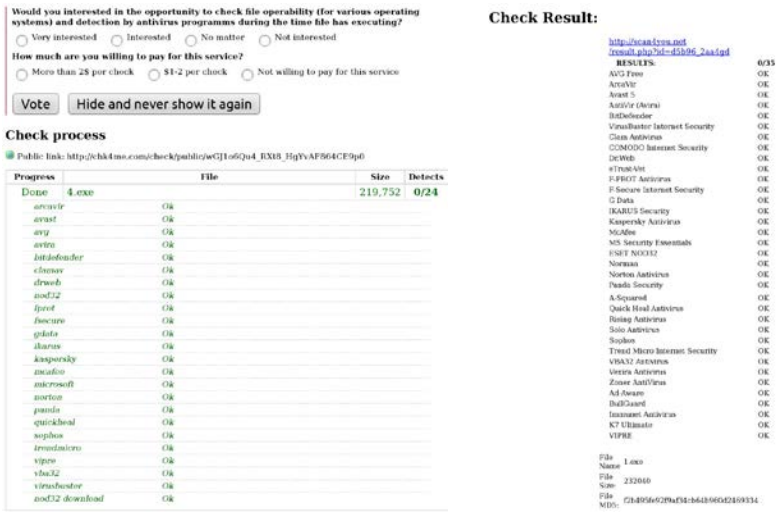


Fig. 5: Exemple d'outil de contrôle utilisé par les criminels. Les antivirus accompagnés d'un «o.k.» n'identifient pas le code malveillant comme virus. A supposer qu'un antivirus l'ait repéré, l'escroc n'aura qu'à l'empaqueter différemment.

La multiplication des variantes et les programmes d'empaquetage font qu'il est toujours plus difficile aux fabricants d'antivirus d'identifier les maliciels sur la base de leur seule signature. Les prescriptions minimales de sécurité (mises à jour du système, *pare-feu* et antivirus) ont beau rester valables, ces mesures ne permettent plus de garantir une protection à 100 %.

52 Par exemple Virustotal: http://www.virustotal.com (état: le 20 février 2014).

Efficacité limitée aux maliciels les plus répandus

Les antivirus ne sont réellement efficaces qu'avec les maliciels courants et largement répandus. En cas d'attaque ciblée ne visant qu'une petite partie de la clientèle, l'identification s'avère problématique et pratiquement impossible. Mikko Hypponen, responsable de la recherche chez F-Secure, a ainsi regretté de ne pas être parvenu à détecter Duqu, Flame, Gauss et leurs pairs: «all of us had missed detecting this malware for two years, or more. That's a failure for our company, and for the antivirus industry in general»[53].

Même si en règle générale les attaques ciblées ne s'en prennent pas aux usagers ordinaires, on a bien vu avec Stuxnet que de telles opérations infectent aussi des machines n'ayant rien à voir avec la cible ou la victime potentielle. On note par ailleurs, y compris sur le terrain de la criminalité économique, une tendance à lancer de plus petites attaques, tirant parti des lacunes de sécurité connues ou basées sur des maliciels empaquetés à dessein pour tromper la vigilance des antivirus.

Nécessité de nouvelles mesures

La question se pose donc des autres mesures requises pour accroître le niveau de sécurité, afin de détecter même les attaques ciblées de moindre envergure. Beaucoup d'entreprises – les plus grandes notamment – recourent déjà à toutes sortes de systèmes supplémentaires pour détecter les anomalies et bloquer le trafic Internet suspect. Ce rôle revient aux systèmes de détection intelligents, qui analysent le trafic sur le réseau des entreprises et repèrent les écarts à la «moyenne». Aux pare-feu et aux antivirus s'ajoutent les systèmes de détection d'intrusion (*intrusion detection system*, IDS), les listes blanches et les *listes noires* de filtrage du trafic réseau, la surveillance (monitorage) du trafic réseau, voire le monitorage du comportement des ordinateurs individuels.

La traçabilité s'avère déterminante dans ce contexte. Au cas où un maliciel (ciblé) se serait introduit dans le réseau d'entreprise, il est essentiel de comprendre comment il est parvenu jusque-là et quels autres ordinateurs ou serveurs sont également impliqués. On n'aura aucune chance sinon de l'éradiquer du réseau. Comme l'ont montré les précédentes attaques, des mois voire des années s'écoulent parfois entre l'intrusion d'un maliciel dans le réseau et sa découverte.[54] La question de la durée de conservation des *fichiers journaux* doit par conséquent aussi être abordée.

Autre leçon tirée des dernières années, les mesures techniques ne sont pas suffisantes. Car au bout du compte, c'est toujours le collaborateur qui peut le plus efficacement identifier une attaque et y réagir de façon adéquate. D'où l'importance d'activités régulières de formation et de sensibilisation du personnel. Il est également utile de créer une adresse à laquelle les collaborateurs pourront signaler tout incident, en sachant qu'ils seront pris au sérieux.

Nécessité d'agir dans les petites entreprises

Les petites entreprises en particulier devraient renforcer leurs mesures de cyberdéfense. A bien des égards, elles ne sont pas suffisamment protégées contre de telles attaques ciblées. Il s'agit fréquemment de sociétés de niche ayant investi un capital considérable dans la

---

53 http://www.f-secure.com/weblog/archives/00002376.html (état: le 20 février 2014).

54 Verizon: Data Breach Investigations Report 2012, fig. 40.
document téléchargeable sous http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf (état: le 20 février 2014).

recherche et le développement, et qui constituent ainsi une cible de choix pour d'éventuelles activités d'espionnage. De telles entreprises en particulier gagneraient à introduire des systèmes de sécurité qui ne reposent pas entièrement sur les antivirus. On a trop tendance à oublier que les coûts de mise en place des mesures de sécurité compensent largement les pertes potentielles, au cas où une cyberattaque aurait abouti.

Mise en œuvre laborieuse chez les particuliers

Les mesures susmentionnées ne sont pas transposables aux particuliers. Des solutions de sécurité étendues et appropriées seraient trop coûteuses en pareil cas. En outre, le temps et les connaissances techniques nécessaires manquent parfois. Comment un utilisateur informatique normal doit-il alors se comporter, et quelles mesures peut-il prendre?

Dorénavant, il faudra que les utilisateurs privés réclament à leur fournisseur d'accès une liaison Internet irréprochable, quitte à payer pour cette prestation. Le fournisseur adopterait de manière centrale, pour tous ses clients, les mesures de sécurité supplémentaires susmentionnées et leur offrirait ainsi une protection accrue. A l'heure actuelle, les clients n'insistent pas suffisamment sur la sécurité, et les fournisseurs d'accès Internet passent cet aspect sous silence dans leur publicité. En dehors des coûts, le principal critère de décision pour un accès Internet reste généralement la vitesse de connexion. Cette situation va (devoir) changer à l'avenir.

5.5 Attaques contre les routeurs domestiques

Les *routeurs domestiques* comportent régulièrement des configurations peu sûres ou des failles de sécurité. Alors que les fournisseurs d'accès proposent pour les appareils récents des mises à jour automatiques, ce n'est pas toujours le cas des anciens modèles.

Configurations par défaut (réglages d'usine) non fiables

Les services des routeurs domestiques susceptibles d'être détournés pour des attaques DDoS constituent un problème majeur à l'heure actuelle. Les services *DNS* et *NTP*, tous deux basés sur le protocole *UDP*, sont principalement concernés. Au cas où un tel service serait mal configuré et accepterait des requêtes du réseau entier, les pirates pourraient en profiter pour lancer des attaques DDoS. Ils exploitent fréquemment la possibilité de générer une volumineuse réponse à partir d'une demande relativement simple (par amplification). Une partie de ces vieux appareils avaient été livrés avec des configurations défectueuses et il n'est pas possible d'y installer, dans le cadre de la télémaintenance, un *firmware* récent et/ou une configuration sûre. Beaucoup d'utilisateurs ignorent que leur appareil est mal configuré et qu'une telle situation comporte des dangers. Or ces routeurs peuvent causer d'énormes dégâts. La correction de ces mauvaises configurations est une opération complexe et de longue haleine. MELANI est en contact avec les principaux opérateurs Télécom, tenus de mettre à jour les appareils vulnérables.

Failles de sécurité

Des lacunes sont régulièrement découvertes dans les versions des firmware incorporés aux terminaux *ADSL*. On ne trouve quasiment aucun fabricant qui n'ait pas déjà dû combler des lacunes de sécurité. Diverses failles majeures révélées en juin et en juillet 2013 concernaient des produits Asus[55], et une autre le service *UPnP* d'appareils D-Link.[56] Selon une lacune

[55] Bugtraq: http://seclists.org/bugtraq/2013/Jul/87 (état: le 20 février 2014).

publiée en octobre 2013, il suffisait de modifier l'agent utilisateur (*user agent, UA*) du navigateur pour accéder au serveur Web interne de certains appareils Netgear.[57] Enfin, d'autres appareils Netgear[58] ou Draytek[59] présentent des vulnérabilités, qui permettaient à un pirate d'accéder au routeur ou d'exécuter des programmes malveillants. De telles lacunes sont exploitées par des vers comme Linux.Darlioz[60], mais permettent également à des pirates de détourner des sessions de e-banking.

MELANI recommande de limiter autant que possible l'accès aux interfaces de maintenance des routeurs. De nombreux appareils prévoient une restriction à une *adresse IP* du réseau interne. Au cas où le fournisseur n'effectuerait pas la maintenance des appareils, il incombe à l'utilisateur de faire des mises à jour régulières. En outre, il ne faudrait activer que les services réellement utilisés. Green a publié des instructions complètes sur la manière de résoudre le problème des résolveurs DNS ouverts, y c. sur les appareils domestiques.[61]

5.6 Objets parlementaires sur des questions touchant à la sûreté de l'information

Sélection des interventions parlementaires déposées au deuxième semestre 2013 sur des questions touchant à la sûreté de l'information.

Objet	N°	Titre	Déposé par	Date de dépôt	Conseil	Dépt	Etat des délibérations et lien
Qst.	13.5284	Contacter Edward Snowden pour obtenir plus d'informations sur les activités d'espionnage menées en Suisse par les Etats-Unis	Glättli Balthasar	09.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135284
Qst.	13.5283	Réaction insuffisante de la part du Conseil fédéral face aux violations du domaine privé subies par des personnes et des entreprises suisses	Glättli Balthasar	09.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135283
Qst.	13.5338	Généralisation du vote électronique	Markwalder Christa	11.09.2013	CN	ChF	hhttp://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135338
Qst.	13.5334	Floutage des photos des zones sensibles dans les documents accessibles au public	van Singer Christian	11.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135334
Qst.	13.5328	Vote électronique	Sommaruga Carlo	11.09.2013	CN	ChF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135328
Qst.	13.5319	Quelles mesures pour empêcher le viol de la protection des données par la NSA?	Schwaab Jean Christophe	11.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135319
Ip.	13.3677	Certains services de renseignement étrangers, tels que la NSA, furètent-il également en Suisse	Groupe socialiste / Tschümperlin Andy	11.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133677
Ip.	13.3692	Marché des télécommunications. La législation et les mesures de régulation en vigueur font-elles encore sens?	Hurter Thomas	12.09.2013	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133692
Qst.	13.5321	La Suisse fait-elle aussi l'objet d'espionnage économique par la NSA?	Leutenegger Oberholzer Susanne / Groupe socialiste	16.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135321
Po.	13.3707	Stratégie cybernétique globale et adaptée aux exigences futures	Groupe BD / Guhl Bernhard	17.09.2013	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133707
Qst.	13.5382	Contrôle de l'exportation de logiciels de surveillance provenant de Suisse	Glättli Balthasar	18.09.2013	CN	DEFR	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135382
Qst.	13.5380	Insuffisance des instruments de lutte contre la cybercriminalité	Reinmann Maximilian	18.09.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20135380
Po.	13.3736	Stratégie WiFi pour la Suisse	Buttet Yannick	18.09.2013	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133736
Ip.	13.3726	Usurpation d'identité. Une lacune du droit pénal à combler?	Schwaab Jean Christophe	18.09.2013	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133726
Qst.	13.1060	Abus en matière de noms de domaine	Fehr Jacqueline	18.09.2013	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20131060
Iv.pa.	13.445	Rendre punissable l'usurpation d'identité dans le dessein de nuire, au moyen des outils de communication informatiques	Golay Roger	18.09.2013	CN		http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20130445
Ip.	13.3773	Pour une loi sur les télécommunications nous permettant d'affronter l'avenir. Elaborer une stratégie globale consacrée au cyberespace	Wasserfallen Christian	24.09.2013	CN	DETEC	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133773

[56] Heise: http://www.heise.de/security/meldung/D-Link-Router-mit-schwerwiegender-UPnP-Luecke-1914510.html (état: le 20 février 2014).

[57] Devttys0.com: http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ (état: le 20 février 2014).

[58] The Shadow File: http://shadow-file.blogspot.ch/2013/10/complete-persistent-compromise-of.html (état: le 20 février 2014).

[59] CERT.org: http://www.kb.cert.org/vuls/id/101462 (état: le 20 février 2014).

[60] Symantec: http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (état: le 20 février 2014).

[61] Green: http://www.green.ch/Portals/0/Support/pdf/Anleitung_OpenResolver_FR.pdf (état: le 20 février 2014).

Mo.	13.3808	Pas de précipitation en matière d'extension du vote électronique	Schwaab Jean Christophe	25.09.2013	CN	ChF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133808
Ip.	13.3799	Sécurité des TI dans l'administration fédérale. Quel est le rapport coût/utilité?	Cassis Ignazio	25.09.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133799
Mo.	13.3812	Garantir la sécurité du vote électronique. N'autoriser que les systèmes vérifiables munis d'un code source libre	Glättli Balthasar	26.09.2013	CN	ChF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133812
Mo.	13.3841	Commission d'experts pour l'avenir du traitement et de la sécurité des données	Rechsteiner Paul	26.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133841
Mo.	13.3930	Exportation de logiciels de surveillance et d'espionnage dans des Etats de non-droit	Glättli Balthasar	27.09.2013	CN	DEFR	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133930
Ip.	13.3927	Protection des données en Suisse	Reimann Lukas	27.09.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133927
Po.	13.3989	Violations de la personnalité dues au progrès des techniques de l'information et de la communication	Recordon Luc	27.09.2013	CE	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20133989
Mo.	13.4009	Mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques	Commission de la politique de sécurité CN	05.11.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134009
Ip.	13.4023	Interrogations sur la politique informatique de la Confédération	Groupe PDC-PEV	27.11.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134023
Po.	13.4069	Scandale de l'espionnage par la NSA et d'autres services secrets étrangers	Schwaab Jean Christophe	04.12.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134069
Ip.	13.4077	Espionnage de données et sécurités sur Internet	Groupe UDC	05.12.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134077
Mo.	13.4086	Programme national de recherche portant sur un système de protection des données applicable au quotidien dans la société de l'information	Groupe des Verts / Glättli Balthasar	05.12.2013	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134086
Mo.	13.4091	Interdire l'utilisation d'installations à des fins d'espionnage politique, militaire ou économique à l'encontre de la Suisse ou d'Etats étrangers	Groupe des Verts / van Singer Christian	05.12.2013	CN	DFJP	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134091
Mo.	13.4165	Affaire Snowden. Accord de non-espionnage avec les Etats-Unis	Allemann Evi	12.12.2013	CN	DDPS	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134165
Po.	13.4308	Améliorer la sécurité et l'indépendance de l'informatique suisse	Graf-Litscher Edith	13.12.2013	CN	DFF	http://www.parlament.ch/f/suche/Pages/geschaefte.aspx?gesch_id=20134308

6 Glossaire

3DES	Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique très répandu.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
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.
ADSL	Asymmetric Digital Subscriber Line Ligne d'abonné numérique à débit asymétrique. Technologie permettant un accès Internet permanent à haut débit par l'intermédiaire de la ligne téléphonique.
Advanced Persistent Threat (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.
Agent utilisateur	Agent utilisateur (user agent) est un terme générique désignant tout programme permettant d'accéder à un site Web (navigateur, robot d'indexation, etc.).
Annexe	Une annexe (attachment) est un fichier envoyé en pièce jointe d'un courriel de texte.
Antivirus Live CD	CD d'un fabricant d'antivirus nettoyant l'ordinateur avant le démarrage du système d'exploitation.
App	Le terme app (abréviation anglaise d'application) recouvre tous les logiciels d'application destinés à l'utilisateur final. Dans le vocabulaire courant, il désigne surtout des applications pour smartphones modernes et tablettes tactiles.
Application	Programme informatique permettant d'effectuer une tâche déterminée. Les traitements de texte et les navigateurs Web sont des exemples d'applications.
ARPANET	Le réseau Arpanet (Advanced Research Projects Agency Network) a été développé dès 1962 par un petit groupe de chercheurs mandaté par les forces aériennes américaines, sous l'égide du Massachusetts Institute of Technology et du Ministère américain de la défense. C'est l'ancêtre d'Internet.
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 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.)
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
Black- / White-List	Black List (liste noire): liste d'adresses ou de noms de domaines pour lesquels des mesures restrictives se justifient. Un blocage du site concerné peut notamment intervenir. White List (liste blanche): Liste d'adresses ou de noms de domaine qui, selon l'auteur de la liste, sont toujours dignes de confiance.
Carte SIM	La carte SIM (de l'anglais: subscriber identity module) est une petite carte à puce que l'on insère dans un appareil de téléphonie mobile et qui contient des données identifiant l'abonné.
Cellule abus	Service d'un fournisseur d'accès auquel peuvent être signalées les activités suspectes constatées dans sa plage du réseau.
Clé (de chiffrement)	Paramètre utilisé en entrée d'une opération cryptographique (déchiffrement, création ou vérification de signature, etc.)
Code source	Le code source (angl. source code) est un ensemble d'instructions écrites dans un langage de programmation informatique évolué, qui se présente sous la forme d'un texte lisible par un utilisateur.
Content Management Systemen (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).
Cross Site Scripting	Le cross-site scripting (abrégé XSS), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web

	visitant la page.
Domaines	Tout nom de domaine (p. ex. www.exemple.com) est associé par l’intermédiaire d’un serveur DNS (Domain Name System) à son adresse IP, laquelle permet d’établir une connexion réseau entre ordinateurs.
Exploit Pack	Un kit d’exploit est un outil qui permet de distribuer des maliciels exploitant les vulnérabilités des programmes.
Fichier journal	Un fichier journal (log file) regroupe de façon chronologique l’ensemble des événements survenus sur un système informatique. Une ligne est consacrée à chaque action.
Firmware	Microprogrammes. Instructions enregistrées dans une puce pour commander un appareil (p.ex. numériseur, carte graphique, etc.). Elles sont en général modifiables par des mises à jour.
Fonction de hachage	L'algorithme génère une série de chiffres, d‘un texte soumis. Les fonctions de hachage s'emploient dans trois domaines: - cryptographie; - systèmes de banques de données. Les fonctions de ha-chage permettent d'effectuer des recherches efficaces dans une grande masse de données. - sommes de contrôle. Chaque fichier reçoit une valeur hachée. Toute modification est un indice de manipulation.
Gestion de cycle de vie	Le cycle de vie des produits est un concept d’économie d’entreprise, comprenant les phases de conception et de lancement, jusqu’au retrait du marché.
Hébergement	Action d’héberger (hosting) un site Web ou une page personnelle sur un serveur afin de les rendre accessibles sur Internet.
HTML	HyperText Markup Language Langage de balisage hypertexte. Le HTML permet de créer des pages Web. Il sert à en définir les caractéristiques (p.ex. la structure des pages, la présentation, les liens sur d'autres pages, etc.). Du fait que le HTML est constitué de caractères ASCII, l'édition d’une page HTML peut s'effectuer avec un traitement de texte usuel.
IFrame	Un IFrame (parfois aussi appelé Inlineframe) est un élément HTML servant à structurer l’espace

	d'affichage d'une page Web. Il permet d'insérer dans son propre site des contenus Web externes.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le server.
Internet Explorer Cache	Une mémoire cache ou antémémoire enregistre temporairement des copies de données provenant d'une autre source afin de diminuer le temps d'accès de l'ordinateur à ces données.
Java	Language de script basé objet pour le développement d'applications.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Lecteur réseau	Espace virtuel disponible en tout temps au même titre que les disques locaux à partir de l'icône Poste de travail, alors que les données sont stockées sur un serveur.
Lettre de lecteur	Les systèmes d'exploitation Microsoft affectent une lettre de l'alphabet aux lecteurs (ou aux partitions système apparaissant comme tels à l'utilisateur).
Mémoire vive (RAM)	Mémoire rapide d'accès, dont le contenu peut être modifié en usage normal (random access memory, RAM).
mTAN	La variante Mobile TAN (mTAN) ou smsTAN utilise comme facteur d'authentification le canal SMS. Le numéro de transaction (TAN) est envoyé sous forme de SMS.
Open Source	Palette de licences pour des logiciels dont le code source est accessible au public, dans une optique de développement communautaire.
Over the air	Technologie permettant d'échanger des données à distance avec les appareils, en utilisant les ondes radio (acronyme: OTA).

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.
PHP Code	PHP est un langage de script principalement utilisé pour la création de pages Web dynamiques ou pour le développement de logiciels d'application destinés au Web.
PIN	Un numéro d'identification personnel (PIN) est un code numérique secret permettant d'obtenir l'accès à une machine et d'y effectuer l'opération désirée.
Point of sale (POS)	Un terminal EFT/POS est un terminal de point de vente (POS, point of sale) acceptant le paiement sans numéraire (EFT, electronic funds transfer).
porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
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).
Propriétaire	S'oppose aux logiciels ou matériels libres.
Protocole NTP	Protocole permettant de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure (Network Time Protocol, NTP).
Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Remote Administration Tool (Remote Access)	Un RAT (Remote Administration Tool, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur

	depuis un autre ordinateur.
Réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis.
Roaming	Synonyme d'itinérance (anglicisme). Fonction initialement reliée au système de téléphonie GSM, permettant à l'abonné d'un réseau d'utiliser son appareil dans une zone autre que celle où il a été enregistré pour recevoir ou passer des appels, pour envoyer ou recevoir des données, ou pour accéder aux autres services des réseaux de téléphonie mobile.
Rootkit	Ensemble de programmes et de techniques permettant d'accéder sans être remarqué à un ordinateur pour en prendre le contrôle.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Scriptcode / Javascript	Language de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Service d'anonymisation	Service permettant, à l'instar de TOR, d'utiliser une adresse IP empruntée afin de cacher sa propre identité.
SMS	Short Message Service. Service de messages courts. Service permettant d'envoyer des messages

	courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
Spear phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
SSH-daemon	Le protocole SSH (Secure Shell) facilite les connexions sécurisées à distance entre deux systèmes, toutes les données transmises étant cryptées. Un démon est un programme constamment actif, exécutant des fonctions en arrière-plan.
Stream	Un flux de données (en anglais: data stream) désigne en informatique une séquence de données qui sont transmises en continu sans que la quantité de données ne soit connue à l'avance.
Système de noms de domaine (Domain Name System).	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).
UPnP	L'Universal Plug and Play (UPnP) est un service permettant aux périphériques de se connecter aisément et donc simplifiant la mise en œuvre de réseaux à la maison (partage de fichiers, communications, divertissements) ou dans les entreprises.
User Datagram Protocol (protocole UDP)	UDP est un protocole réseau simple, sans connexion, faisant partie de la couche de transport de la famille de protocoles Internet. UDP a pour tâche de délivrer à l'application correcte les données échangées par Internet.
Watering Hole attack	Attaque du trou d'eau, attaque ciblée par un maliciel n'infectant que des sites supposés être visités par un groupe spécifique d'utilisateurs.