Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de stratégie informatique de la Confédération (USIC)
Service d'analyse et de prévention (SAP)

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 2009/I (janvier à juin)

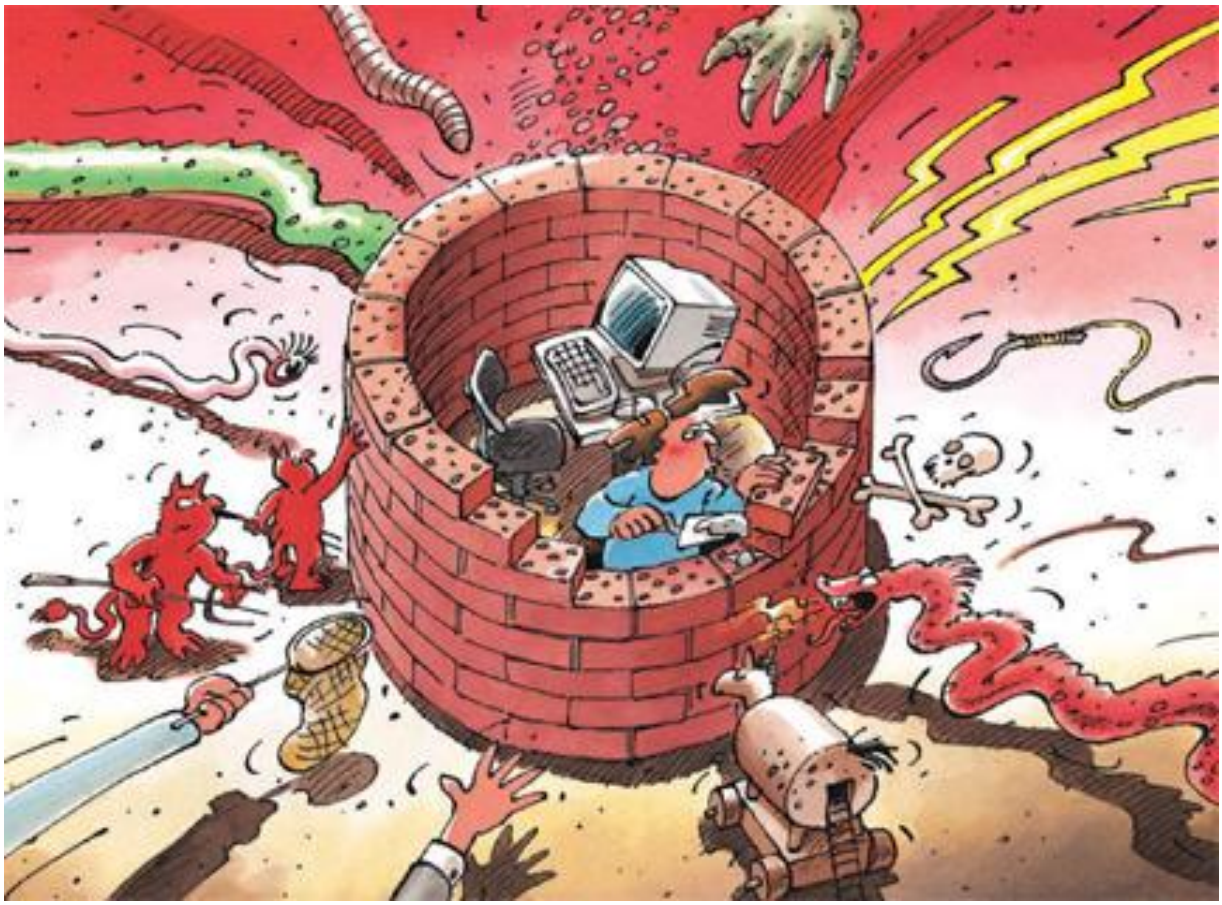


Table des matières

1 Temps forts de l'édition 2009/I 3

2 Introduction 4

3 Situation en Suisse de l'infrastructure TIC 5

3.1 Gozi, nouveau cheval de Troie diffusé par pourriel 5

3.2 Progression des infections par drive-by download 7

3.3 Manipulation de comptes de messagerie suisses 8

3.4 Interruption d'Internet et de téléphonie chez Cablecom 9

3.5 Envois de courriels infectés à de grandes entreprises 9

4 Situation internationale de l'infrastructure TIC 11

4.1 Espionnage informatique visant des ONG tibétaines et le bureau du Dalaï Lama 11

4.2 Conficker 11

4.3 SCADA 13

4.4 Guerre de l'information: mise en place d'unités spéciales dans divers pays 16

4.5 Recrudescence d'attaques DDoS à mobile politique 17

4.6 Panne de réseau chez T-Mobile 18

4.7 Grande-Bretagne: achat d'un réseau de zombies par la BBC pour les besoins d'une émission 18

4.8 Etats-Unis: multiplication des pertes de données en 2008 19

4.9 Les Etats-Unis veulent renforcer la lutte contre les cybermenaces et améliorer la protection existante 20

4.10 La Commission européenne prévoit de mieux protéger ses infrastructures critiques 21

4.11 Volte-face de Facebook sur ses conditions générales 21

5 Tendances / Perspectives 22

5.1 Informatique dans les nuages, externalisation, centralisation et propriété de l'information 22

5.2 SCADA 23

5.3 Evolution générale de la cybercriminalité 23

5.4 Infections par drive-by download 25

6 Glossaire 26

7 Annexe 30

7.1 ICANN et l'OFCOM développent des solutions contre les réseaux Fast Flux 30

7.2 Réglages des navigateurs contre des infections drive-by courantes 36

1 Temps forts de l'édition 2009/I

- **Progression des infections par drive-by download**
  Comme déjà relevé dans les derniers rapports semestriels, la tendance est à l'abandon des vecteurs d'attaque (courriels comportant une annexe ou un lien) au profit d'infections lors de la visite de sites Web (infections par drive-by download). Les modes classiques de diffusion des maliciels ne sont plus aussi efficaces, sans doute parce que les utilisateurs sont devenus plus prudents et ouvrent rarement les annexes suspectes. Selon une analyse de la société de sécurité en ligne Scansafe, 74 % des maliciels diffusés au troisième semestre 2008 l'ont été par des sites Web infectés.
  ► Situation actuelle en Suisse: chapitre 3.2
  ► Tendances 5.4
  ► Mesures de défense: annexe 7.2

- **Discussion à plus large échelle sur la sécurité des systèmes SCADA**
  Les technologies de l'information et de la communication (TIC) s'avèrent depuis longtemps indispensables à la surveillance, au contrôle et au pilotage des installations industrielles, des systèmes de distribution de produits de première nécessité (électricité, eau, combustibles, etc.) ou des transports et du trafic (chemin de fer, systèmes de gestion du trafic, Poste, etc.). Le développement et l'exploitation de tels systèmes de surveillance, de contrôle et de pilotage (en anglais Supervisory Control and Data Acquisition, SCADA) ont une longue tradition. La discussion sur la sécurité des systèmes SCADA est donc menée à toujours plus large échelle. Il est bien clair que de tels systèmes sont essentiels au bon fonctionnement de notre société. Au-delà des cyberattaques (sabotage), ils présentent également des risques de défaillances techniques.
  ► Situation actuelle en Suisse: chapitre 4.3
  ► Tendances 5.2

- **Informatique dans les nuages et propriété de l'information**
  Le 17 mai 2009, la population suisse a approuvé de justesse (par 50,1 % des bulletins) l'introduction des passeports biométriques. Outre les réticences liées à la protection des données, les questions de sûreté de l'information semblent avoir été l'argument décisif dans le camp du non.
  ► Tendances 5.1

- **Fraude à la commission et abonnement forcé**
  MELANI et le SCOCI sont informés chaque jour de divers cas de fraude à la commission, de prétendus gains en loterie et d'offres gratuites. Trop de gens se font apparemment encore piéger par cette forme de cybercriminalité.
  ► Tendances 5.2

- **Conficker**
  Les médias ont abondamment parlé au semestre précédent du ver informatique Conficker. L'intérêt public pour ce maliciel a culminé vers le 1er avril 2009, date à laquelle il était censé s'actualiser. Plus personne ne s'attendait à une propagation aussi fulgurante. Or Conficker a infecté des millions de systèmes un peu partout.
  ► Chapitre 4.2

2 Introduction

Le neuvième rapport semestriel (de janvier à juin 2009) 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 2009. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

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

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

3 Situation en Suisse de l'infrastructure TIC

3.1 Gozi, nouveau cheval de Troie diffusé par pourriel

En décembre 2008 déjà, des cybercriminels avaient tenté de s'implanter en Suisse avec la famille de chevaux de Troie Gozi alias Infostealer.Snifula. Il s'agissait de la troisième famille de chevaux de Troie spécialisés dans le e-banking et prenant pour cible la clientèle des établissements financiers suisses.

Un pourriel au contenu douteux[1] cherchait à attirer les victimes potentielles sur des sites pornographiques spécialement préparés. Le site Internet invitait l'utilisateur à télécharger et installer un *plugiciel Flash*, soi-disant pour accéder aux contenus visuels du site Internet. Or un cheval de Troie spécialisé dans le e-banking s'y dissimulait.

En janvier 2009, plusieurs vagues de pourriels visant à diffuser le même type de cheval de Troie ont été repérées. Les messages comportaient un lien avec une page falsifiée du journal gratuit «20 Minuten». La page avait été intégralement copiée de l'original, si bien que seule l'adresse Web révélait l'escroquerie. Des extraits de l'article du gratuit figuraient aussi dans le pourriel. Le message était dès lors rédigé dans un allemand correct. Les parties modifiées ou ajoutées renfermaient toutefois des erreurs.
Par exemple les titres se référaient soit à l'extension de la libre circulation des personnes à la Bulgarie et à la Roumanie. Comme il s'agit de thèmes spécifiquement suisses, on peut penser à une diffusion ciblée de la part des escrocs.

Von: ZURICH Kontakt [mailto:alarm@20min.ch]
Betreff: ZURICH ALARM:2007 wurden erst 203 Einsteigerinnen aus den osteuropaischen Staaten registriert.

ZÜRICH

50 Prozent mehr Ost-Prostituierte
Die Zahl der Prostituierten aus Osteuropa wächst rasant: Von dort stammt fast die Hälfte der Frauen, die 2008 von der Stapo Zürich neu registriert worden sind.

Bis ins Einzelne>>
Mit den herzlichen Grüßen, Roseann Mansfield.

Pourriel sur le thème de la libre circulation des personnes

[1] http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=fr (état: 21.08.2009).

Page truquée du journal gratuit 20 Minuten. Les internautes sont priés d'installer un plugiciel Flash afin de visionner la vidéo.

L'article du journal 20 Minuten repris par le pourriel avait paru le dimanche soir à 22h18. Le pollupostage a été effectué le lundi à midi déjà. D'autres vagues de pourriels ont suivi le mardi et le mercredi. Le contenu était identique, à ceci près que les noms de domaine changeaient d'une vague à l'autre. En effet, les sites étaient hébergés sur un réseau «*fast flux*», ce qui veut dire que plusieurs serveurs sont utilisés pour sa sauvegarde[2]. Chaque fois que l'un est mis hors service, la requête est automatiquement redirigée vers le suivant. La désactivation est d'autant plus difficile, et donc une attaque peut se poursuivre plus longtemps. Les domaines avaient certes tous été enregistrés auprès d'un registraire DNS chinois. Mais ces circonstances ne disent rien de la provenance des pirates.

Il s'agit à ce jour des dernières grandes vagues de pourriels ayant diffusé des chevaux de Troie spécialisés dans le e-banking. Apparemment, les coûts ont été disproportionnés par rapport aux bénéfices retirés, en raison du maigre butin tiré des ordinateurs compromis. Car globalement, les attaques basées sur des chevaux de Troie spécialisés dans le e-banking se sont raréfiées dès janvier. Les pirates ont préféré d'autres modèles d'affaires, à l'instar des *rogue softwares* ou *roguewares*. Il s'agit de logiciels malveillants qui prétendent avoir découvert des maliciels sur l'ordinateur de la victime, pour l'inciter à acheter un antivirus fictif. En outre, les infections par *drive-by download* gagnent du terrain (voir chapitre 3.2). Des informations plus complètes sur les réseaux Fast Flux figurent au rapport semestriel 2008/1.[2]

[2] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=fr (état: 31.08.2009).

3.2 Progression des infections par drive-by download

Comme déjà relevé dans les deux précédents rapports semestriels, la tendance est à l'abandon des vecteurs d'attaque (courriels comportant une annexe ou un lien) au profit d'infections lors de la visite de sites Web (infections par drive-by download). Les modes classiques de diffusion des maliciels ne sont plus aussi efficaces, sans doute parce que les utilisateurs sont devenus plus prudents: ils ne cliquent plus forcément sur les liens indiqués dans un courriel et ouvrent rarement les annexes suspectes. Selon une analyse de la société de sécurité en ligne Scansafe[3], 74 % des maliciels diffusés au troisième semestre 2008 l'étaient déjà par des sites Web infectés. A ce propos, un rapport de l'entreprise Websense indique que 70 % des 100 sites les plus populaires ont contenu au moins brièvement des maliciels, ou alors que des cybercriminels s'en sont servis pour leurs activités.[4] [5]

Les moteurs de recherche jouent un rôle à ne pas sous-estimer dans les infections par drive-by download. Les escrocs cherchent notamment à compromettre des sites qui soient bien classés, lors de requêtes basées sur des mots-clés populaires, et qui en outre soient mal protégés ou présentent des lacunes de sécurité. Parfois aussi, l'infection par drive-by download met à profit des pages référentes (*referrers*): l'infection n'a alors lieu qu'en cas d'accès au site par le biais d'un moteur de recherche. L'administrateur de site Web qui, le plus souvent, saisit directement son adresse aura du mal à découvrir que celui-ci a été compromis. Dans une attaque par drive-by download connue sous le nom de Gumblar et remontant au mois de mai, le cheval de Troie manipule les résultats des recherches par Google indiquées dans le navigateur. La victime est ainsi amenée à naviguer sur des sites dangereux, ce qui accroît fortement le risque de nouvelle infection.

Les infections par drive-by download ont connu une évolution significative (voir chapitre 5.4 Tendances). De telles attaques ont toutes un point commun, à savoir que leurs auteurs doivent d'abord trouver un site à partir duquel l'infection puisse se propager. Ainsi, les escrocs piratent des serveurs en activité pour y placer leurs codes malveillants. Ils utilisent à cet effet des mots de passe *FTP* dérobés ou exploitent des failles de sécurité des logiciels figurant sur les serveurs. Parmi leurs cibles préférées figurent les systèmes de gestion de contenu (*content management system, CMS*), les forums et les livres d'hôtes avec les banques de données correspondantes. Il importe de préciser qu'en cas d'exploitation d'une lacune de sécurité, la fraude ne concerne généralement pas un seul site mais s'étend de là à d'autres sites hébergés sur le serveur piraté.

L'attaque elle-même s'effectue en plusieurs étapes. Le site piraté comporte un *code* qui redirige à l'arrière-plan le visiteur sur un serveur tiers. La plupart du temps, l'opération se déroule dans un élément *IFrame* généré en *Javascript*. A l'avenir, il faudra aussi s'attendre à une augmentation des cas de redirection automatique par des balises *META Refresh* servant à l'actualisation des métafichiers (voir Tendances, chapitre 5.4). La dissimulation à l'aide de Javascript vise à empêcher la détection de telles infections (p. ex. par des antivirus). Entre-temps, des éléments IFrames sont aussi placés directement sur les sites Web, ce qui est souvent plus discret en raison de la sensibilité accrue à Javascript comme vecteur d'attaques. Une fois la victime redirigée sur le serveur pirate, une série d'examens sont effectués afin de déterminer quels programmes sont installés sur son ordinateur et s'il s'agit d'une ancienne version comportant une faille de sécurité. Le cas échéant, l'ordinateur

[3] http://www.scansafe.com/resources/global_threat_reports2/gtr_2008/Q3_2008_GTR.pdf (état: 31.08.2009).
[4] http://securitywatch.eweek.com/exploits_and_attacks/most_popular_sites_were_hacked_in_08.html (état: 31.08.2009).
[5] http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF (état: 31.08.2009).

recevra la visite d'un maliciel adapté à cette lacune, qui infectera ensuite son système. De telles failles de sécurité concernent non seulement le navigateur lui-même, mais aussi des logiciels comme Flash ou Acrobat Reader lui apportant des fonctions supplémentaires (*Browser plug-in*), ou une lacune critique de l'élément *ActiveX Control*, etc. Enfin, en l'absence de lacune de sécurité adéquate, l'utilisateur est prié avec insistance d'installer manuellement le maliciel.

Les techniques permettant de placer sur un site Internet des infections par drive-by download qui restent le plus longtemps possible indétectables font des progrès fulgurants. Cette évolution est décrite au chapitre 5.4.

La lecture du chapitre consacré aux mesures de prévention (annexe 7.2) vous aidera à protéger votre ordinateur des attaques par drive-by download.

3.3 Manipulation de comptes de messagerie suisses

Le dernier rapport semestriel de MELANI signalait l'intérêt croissant des cybercriminels pour les données d'accès à des services Internet. En l'occurrence, il s'agissait principalement de placer des infections par drive-by download sur des sites Web ou de piller des comptes de vente aux enchères. Il y était aussi question de tentatives de phishing visant des fournisseurs de messagerie comme Bluewin, Hotmail, etc. Rien n'était dit toutefois des possibilités s'offrant aux escrocs ayant dérobé les données d'ouverture d'un compte de messagerie. Bien des gens se diront qu'il leur est égal qu'un tiers ait accès à leurs courriels et que les messages qu'ils reçoivent ne sont pas vraiment confidentiels. Or l'enjeu est bien plus important, sachant que les criminels sont mus par l'appât du gain. Un cas authentique survenu en Suisse montre comment le vol des données d'accès à un compte de messagerie permet de gagner de l'argent.

En juin 2009, des données dérobées ont servi à accéder au compte de messagerie d'un citoyen suisse et à envoyer à ses 350 contacts un courriel faisant état de difficultés au cours d'un prétendu voyage en Afrique. Ainsi, son passeport, tout son argent et ses autres documents lui avaient été dérobés. Pour pouvoir repartir, il avait un besoin urgent de 1000 euros afin de régler sa note d'hôtel et de 100 euros pour la facture téléphonique ouverte. Ce montant serait naturellement intégralement remboursé à son retour en Suisse. L'argent devait être versé via Western Union à Abidjan, à une personne inconnue du destinataire du courriel. Dans ces circonstances, tout contact téléphonique était impossible.

Dans ce cas d'espèce, il n'y a eu aucun dommage. Car dans leur scepticisme, les destinataires ont demandé une confirmation téléphonique à l'ami prétendument en détresse avant d'effectuer le moindre virement, et Western Union les a également mis en garde.

En conclusion, ce n'est pas seulement le compte de messagerie d'une personne qui s'avère intéressant, mais plutôt les contacts qu'elle a établis. A l'avenir, les escrocs ne collecteront donc plus seulement les adresses de messagerie, mais relèveront précisément les contacts avec d'autres personnes. Le but est de personnaliser autant que possible le courriel adressé aux victimes potentielles. En raison des importants efforts requis, cette tactique n'a été observée jusqu'ici que ponctuellement, lors d'attaques bien ciblées. Mais à supposer que ces liens puissent être collectés automatiquement et à grande échelle, la tâche serait plus facile et il faudrait s'attendre à ce que la technique serve aussi à des attaques «non ciblées». Le but restant d'amener la victime à cliquer sur une annexe ou à exécuter une autre action périlleuse. Autrement dit, la prudence ne s'impose plus seulement avec les courriels d'inconnus, mais également avec ceux émanant d'expéditeurs connus. En cas d'incident inhabituel – notamment quand de l'argent est en jeu –, MELANI recommande de procéder à des vérifications téléphoniques, de s'assurer de l'identité de la personne en lui

posant des questions dont elle seule connaît la réponse, ou de discuter de la crédibilité de l'histoire racontée avec des connaissances communes.

3.4 Interruption d'Internet et de téléphonie chez Cablecom

Le 19 janvier 2009, une attaque de DDOS contre un client de Cablecom a causé une forte limitation de traffic sur le réseau de Cablecom qui a durée environ une heure. Le trafic Internet s'est accru à ce moment de plusieurs gigabits par seconde. Les lignes étant saturées, les services Internet et de téléphonie ont été fortement limités, voire interrompus dans la région de Zurich et environs. Cablecom a alors dévié le trafic Internet par le réseau international. Le trafic malveillant a ensuite pu être neutralisé aux points d'entrée du réseau principal de Cablecom ainsi que de la dorsale Internet (*Internet backbone*) internationale. Un tiers des clients dans l'agglomération de Zurich a été touché, soit 90 000 raccordements, lesquels n'ont pas pu ou seulement partiellement téléphoner ou naviguer sur Internet entre 12h50 et 13h50.

Diverses attaques DDoS ont d'ores et déjà été enregistrées en Suisse. Elles prennent très souvent pour cibles des sites à contenu pornographique.[6] Ainsi, le site www.sexy-tipp.ch a été victime d'un *réseau de zombies* en décembre 2007[7]. D'autres sites Internet zurichois liés au milieu de la prostitution ont d'ailleurs connu le même sort. Il est fréquent que de telles attaques touchent aussi d'autres sites hébergés sur le même serveur – la plupart du temps toutefois, elles provoquent un effondrement complet du réseau. Les mobiles de l'attaque lancée contre Cablecom n'ont pas encore été élucidés. Cablecom a déposé plainte auprès de la police.

3.5 Envois de courriels infectés à de grandes entreprises

Une vague d'attaques très ciblées[8], dirigées contre les cadres de grandes entreprises, a été observée au premier semestre 2009. Les courriels, rédigés en anglais, prétendaient qu'un ordre de paiement avait été donné et qu'il fallait en vérifier l'exactitude dans le document annexé «details.rtf». Le maliciel s'installait en cas d'ouverture du fichier.

Un exemple de ce genre de courriel est donné ci-dessous:

Subject: Re: Wire Transfer <Vorname Name des Empfängers>

The wire transfer has been released.

BENEFICIARY : <Vorname Name des Empfängers>
ABA ROUTING# : XXXX92729
ACCOUNT# : XXX-XXX-XXX25
AMMOUNT : $19,438.16

Please check the wire statement attached and let me know if everything is correct. I am waiting for your reply.
Laura

[6] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (état: 31.08.2009)
[7] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état: 31.08.2009)
[8] http://isc.sans.org/diary.html?storyid=6511 (état: 31.08.2009)

Les analyses du maliciel ont montré qu'il enregistrait systématiquement les répertoires consultés via Windows Explorer, les sites visités par le navigateur et les données de formulaires saisies, avant de transmettre ces informations à différents serveurs. Il a été possible d'identifier et de désactiver ces serveurs, qui faisaient l'objet d'une programmation fixe dans le maliciel. Des vagues similaires ont été observées à l'étranger aussi. Le nombre de courriels ainsi envoyés reste inconnu. Or les destinataires étaient presque exclusivement des cadres d'entreprises, ce qui amène à conclure à une attaque très ciblée. Il y avait apparemment déjà eu à la fin de décembre 2008 plusieurs vagues de pourriels conçus dans les mêmes termes[9] [10]. L'annexe était toutefois différente (bank_statement.scr ou bank_statement.zip) et les envois manifestement moins ciblés. On ignore encore qui se cache derrière cette vague et quel était le but visé.

[9] https://tools.cisco.com/security/center/viewAlert.x?alertId=17321 (état: 31.08.2009)
[10] http://fordhamsecureit.blogspot.com/2008/12/wire-transfer-phishing-email-sent-to.html (état: 31.08.2009)

4 Situation internationale de l'infrastructure TIC

4.1 Espionnage informatique visant des ONG tibétaines et le bureau du Dalaï Lama

Le dernier week-end de mars 2009, plusieurs médias ont parlé d'une étude canadienne parue sur l'espionnage informatique chinois et intitulée «Tracking GhostNet – Investigating a Cyber Espionage Network».[11] Il s'agissait des résultats d'une enquête consacrée aux cyberattaques dirigées notamment contre des organisations non gouvernementales tibétaines et contre le bureau du Dalaï Lama, qui avaient compromis au passage d'autres systèmes dans plus de 100 pays. Ni les entreprises ni les services gouvernementaux n'avaient été épargnés.

En 2007 déjà, des rapports confidentiels du chef des services secrets intérieurs britanniques (MI5)[12] mettaient en garde contre des actes d'espionnage ciblés menés à l'aide de chevaux de Troie, selon des méthodes sophistiquées de subversion psychologique (*social-engineering*). Les commanditaires chinois s'intéressaient de près aux *infrastructures vitales nationales* et aux services gouvernementaux. De telles attaques se sont produites entre-temps en Suisse également. Concrètement, les pirates ont envoyé à des personnes-clés d'entreprises stratégiques des documents dont l'expéditeur avait été falsifié. Les informations étaient personnalisées, ce qui donne à penser que les services de renseignement s'étaient d'abord procuré les données correspondantes.

Selon les informations à disposition, ces attaques connues sous le nom de «GhostNet» sont apparentées à celles identifiées contre des institutions étatiques, des infrastructures vitales et des entreprises déjà rendues publiques il y a quelques années. Ces attaques semblent être d'origine chinoise.[13] En Suisse aussi, les recherches liées à Ghostnet ont révélé la présence de systèmes infectés. Mais il s'agissait exclusivement du siège local ou de la représentation en Suisse de groupes économiques ou de gouvernements étrangers. Ni les entreprises helvétiques, ni les organes gouvernementaux n'ont fait partie de Ghostnet.

4.2 Conficker

Le *ver* informatique Conficker (aussi connu sous le nom de Downadup) a beaucoup fait parler de lui durant le semestre écoulé. L'intérêt des médias a culminé autour du 1er avril 2009, date à laquelle il était censé opérer une mutation.

La première version de ce ver Windows est en circulation depuis le 21 novembre 2008. Au début, il était encore peu répandu. Mais les choses ont bien changé en fin d'année. Le ver exploite pour se propager une vulnérabilité du service Serveur de Microsoft Windows (MS08-067), pour laquelle il existe toutefois une mise à jour de sécurité depuis la fin d'octobre 2008. Les principales victimes étaient donc les entreprises ou les particuliers n'ayant pas installé cette mise à jour. Le ver utilise toutefois aussi d'autres possibilités pour se répandre: il teste

[11] http://www.news.utoronto.ca/media-releases/international-affairs/information-warfare-monitor.html (état: 31.08.2009)
[12] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état: 31.08.2009)
[13] http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=fr (état: 31.08.2009)

une liste de mots de passe simples[14] afin de se répliquer au travers de partages réseau ouverts, ou cherche à se copier sur des supports amovibles de stockage comme les *clés USB* ou les appareils photo numériques. Dès qu'une clé USB infectée est branchée sur un ordinateur, une fenêtre s'ouvre et le ver crée une icône standard destinée à l'ouverture de répertoires. L'icône ne se situe toutefois pas dans le domaine «Options», mais sous «Exécuter…». Un clic suffit à installer le ver. Conficker aurait infecté plusieurs millions d'ordinateurs.

Une fois installé, le ver stoppe les mises à jour de Windows et crée un serveur Web local. Il cherche ensuite à se propager et à se dissimuler, pour déjouer les tentatives d'élimination. Il parvient à télécharger et à exécuter toutes sortes de fichiers. Enfin, il bloque l'accès à de nombreux sites spécialisés dans la sécurité et aux services de mise à jour des antivirus.

Le mécanisme de mise à jour et la date magique (1er avril 2009) à laquelle le ver aurait dû s'actualiser ont suscité un vif intérêt de la part des médias. Un algorithme sert ici à générer des noms de domaine avec lesquels le ver tente de prendre contact pour muter. En théorie, Conficker.C est en mesure de composer chaque jour 50 000 noms de domaine à contacter. En cas d'échec, il attend 24 heures avant de générer les 50 000 noms suivants. Comme pour les vers antérieurs, les auteurs ont surtout cherché, pendant les premiers mois, à installer et protéger leur réseau de zombies (consolidation), plutôt qu'à s'en servir pour des actions spectaculaires. La preuve en est que les programmeurs du virus ont utilisé les algorithmes les plus modernes, remontant à quelques semaines parfois. Quant à la technique de cryptage intégrée pour se protéger des autres cyberpirates, elle n'existe que depuis l'automne 2008. Tout laissait donc à prévoir l'absence de grave perturbation d'Internet le 1er avril. Ce n'est que le 7 avril 2009 que l'entreprise de sécurité Trend Micro a remarqué une *activité P2P* accrue de Conficker.C, le ver se transformant dans la variante Conficker.E. Là encore, la principale motivation du ver était de brouiller les pistes. Il a ainsi bloqué les sites proposant des programmes d'élimination des virus. En outre, il se présentait sous un nom aléatoire et effaçait toutes ses traces sur l'ordinateur hôte. Seules des hypothèses sont possibles sur les vrais motifs des auteurs de Conficker. Ils pourraient ainsi chercher à louer un *réseau de zombies* à d'autres escrocs. On sait à ce propos que Conficker.C installe SpywareProtect2009, prétendu logiciel de sécurité (*scareware*)[15].

A l'étranger, ce ver a infecté de nombreux réseaux d'entreprises ainsi que des réseaux gouvernementaux, dont ceux du réseau hospitalier et du gouvernement du Land de Carinthie[16], ou encore des forces armées allemandes[17]. En Suisse aussi, ce ver a paralysé pendant plusieurs heures des réseaux d'entreprise. Près de 1000 *adresses IP* d'ordinateurs infectés y ont été recensées. La plupart des ordinateurs contaminés se trouvaient toutefois en Russie, au Brésil, en Chine et en Inde.

[14] http://blog.namics.com/2009/02/die_aktuelle_li.html (état: 31.08.2009)

[15] http://www.heise.de/security/Deckt-der-Conficker-Wurm-jetzt-seine-Karten-auf--/news/meldung/136083 (état: 31.08.2009)

[16] http://www.heise.de/security/Conficker-in-Kaernten-Nach-der-Landesregierung-nun-die-Spitaeler--/news/meldung/121570 (état: 31.08.2009)

[17] http://www.netzwelt.de/news/79475-conficker-bundeswehr-kaempft-gegen-computerwurm.html (état: 31.08.2009)

Problème des systèmes certifiés

Il est frappant de constater que le ver a fait des ravages surtout dans le domaine de la santé[18]. Il faut dire que ces réseaux comprennent beaucoup de systèmes certifiés (p. ex. instruments de contrôle des appareils d'analyse) dont il est malaisé de corriger les erreurs. Si de surcroît ces systèmes sont reliés à Internet, ils constituent une proie facile pour le ver. Un autre problème tient au branchement d'ordinateurs personnels et d'appareils USB sur les réseaux d'entreprises. En effet, du matériel privé risque d'infecter à son tour le réseau d'entreprise. Le ver tire le meilleur parti possible de cette problématique.

Plus personne ne s'attendait à la propagation aussi fulgurante d'un ver. Suite à l'introduction du Service Pack 2 de WindowsXP, qui contient un pare-feu et télécharge régulièrement les nouvelles mises à jour, tout un chacun aurait dû être protégé contre ce genre de maliciel. La réalité est toutefois bien différente. Il faut bien dire que la plupart des ordinateurs compromis disposaient de versions non officielles de Windows, et que les utilisateurs avaient volontairement renoncé à se connecter au serveur destiné aux mises à jour de Windows.

Une fois de plus, la protection de base d'un ordinateur s'avère cruciale. Il s'agit de mettre à jour le système d'exploitation et ses applications, de disposer d'un pare-feu et d'un antivirus à jour. Sachant que de nombreuses entreprises n'activent pas toujours sur-le-champ les mises à jour, dont elles testent d'abord la compatibilité avec les autres programmes, l'installation s'effectue avec un certain retard, qu'il importe de réduire autant que possible. En outre, les infections par le biais de supports amovibles de stockage augmenteront avec le succès croissant des clés USB, des appareils photo numériques, des téléphones intelligents et des *lecteurs MP3*.

4.3 SCADA

Les technologies de l'information et de la communication (TIC) sont depuis longtemps indispensables à la surveillance, au contrôle et au pilotage des installations industrielles, des systèmes de distribution de produits de première nécessité (électricité, eau, combustibles, etc.) ou des transports et du trafic (rail, systèmes de gestion du trafic, Poste, etc.). Le développement et l'exploitation de tels systèmes de surveillance, de contrôle et de pilotage (en anglais *Supervisory Control and Data Acquisition, SCADA*) ont une longue tradition. A l'origine, les systèmes SCADA ne ressemblaient que de loin aux TIC usuelles: ils étaient isolés des réseaux informatiques, utilisaient du matériel et des logiciels propriétaires et possédaient leur propre protocole de communication avec l'ordinateur central. Depuis quelques années, la commercialisation d'appareils relativement avantageux intégrant, comme technologie d'interface, le *protocole Internet (IP)* a changé la donne dans ce domaine. Les capteurs, les machines et les interrupteurs possèdent toujours plus souvent leur propre adresse IP et utilisent TCP/IP pour communiquer avec l'ordinateur central. D'où l'emploi de TIC courantes et peu coûteuses, le revers de la médaille étant que les systèmes SCADA sont exposés aux menaces bien connues présentes sur Internet; les maliciels et les pirates (hackers) n'ont pas tardé à faire leur apparition. La discussion sur la sécurité des systèmes SCADA doit donc être menée à toujours plus large échelle, comme le montrent les exemples qui suivent. Au-delà des cyberattaques (sabotage), ces systèmes essentiels au bon fonctionnement de notre société présentent également des risques de défaillances techniques, comme le rappelle la panne du système *ETCS* des CFF survenue en été 2009.

[18] http://diepresse.com/home/techscience/internet/sicherheit/473436/index.do (état: 31.08.2009)

Une panne dans le système ETCS a causé une perturbation du traffic ferroviaire entre Mattstetten-Rothrist et dans le tunnel du Lötschberg

L'acronyme ETCS[19] signifie European Train Control System. Là encore, il s'agit d'un système SCADA. L'ETCS vise à créer un système de contrôle des trains harmonisé au niveau européen. Cette standardisation concerne notamment la transmission des informations entre la voie de communication et le véhicule. Les informations devant être transmises par les composants du système ETCS peuvent généralement être obtenues ou générées via les installations de sécurité existantes.

Le système ETCS Level 2 est utilisé sur le nouveau tronçon Mattstetten-Rothrist, dans le tunnel de base du Lötschberg ainsi qu'au tunnel de base en construction du Saint-Gothard. En cas de vitesse supérieure à 160 km/h, le mécanicien de locomotive ne parvient plus à identifier visuellement les signaux. L'autorisation de circuler et le signal de marche sont par conséquent affichés dans la cabine du mécanicien. Les installations de signalisation extérieure deviennent ainsi superflues, à l'exception de quelques indicateurs. Les dispositifs de contrôle de l'état libre des voies et de vérification de l'intégrité du train restent cependant déployés au sol. Tous les trains signalent automatiquement, à intervalles réguliers, leur position précise et leur sens de marche au poste central, qui contrôle en tout temps les mouvements des trains. L'autorisation de circuler est transmise en permanence au véhicule via *GSM-R*, avec les données concernant la vitesse et le parcours. Le 29 juillet 2009, ce système a subi une panne lourde de conséquences pour le réseau CFF. Alors que sur le tronçon Mattstetten-Rothrist, encore équipé de signaux conventionnels, les convois pouvaient circuler jusqu'à une vitesse de 160km/h, dans le tunnel de base du Lötschberg les signaux étaient absents, ce qui a imposé une déviation des trains sur le tronçon des montagnes.

Intrusion dans le système de contrôle du réseau électrique américain

Les pirates ont visiblement réussi à installer dans les systèmes de contrôle des logiciels capables de saboter, sur sol américain, des installations stratégiques destinées notamment à l'approvisionnement en électricité et en eau potable. Ils auraient exploité une faille de sécurité. Selon un rapport du Wall Street Journal[20] se référant aux autorités de sécurité américaines, les pirates se seraient introduits dans le réseau électrique américain et auraient laissé dans le système des programmes malveillants pouvant déployer des effets dans tout le pays. Selon ce rapport, les autorités américaines soupçonnent les pirates de chercher à prendre le contrôle du réseau électrique national. Ils ont beau ne pas avoir tenté jusqu'ici d'endommager les infrastructures, les choses pourraient changer très vite en cas de crise ou de guerre.

Projet *Smart Grid* vulnérable au sabotage

Les réseaux de distribution d'électricité intelligents (en anglais *smart grids*) remplaceront à l'avenir les réseaux conventionnels. Ainsi, la société californienne Pacific Gas and Electric prévoit de remettre à ses clients, d'ici 2011, des compteurs de gaz et d'électricité intelligents. Les compteurs installés chez les consommateurs finaux transmettront directement au nœud de réseau les données collectées sur leur consommation d'électricité ou de gaz. Cette densification des données permettra de mieux gérer la distribution et l'ajustement aux flux. De même, les pannes partielles du réseau seront plus rapidement détectées. Or selon une étude tenue secrète, ces appareils semblent comporter plusieurs lacunes de sécurité. Par

[19] http://mct.sbb.ch/mct/fr/etcs-technologie-funktionsprinzip.htm?= (état: 31.08.2009)
[20] http://online.wsj.com/article/SB123914805204099085.html (état: 31.08.2009)

exemple, ils seraient vulnérables aux dépassements de mémoire tampon (*buffer overflow*) et aux programmes furtifs (*rootkits*). Les protocoles utilisés seraient en outre dépourvus de mécanisme de sécurité. En mettant à profit de telles lacunes, un pirate potentiel pourrait causer une panne de courant. Par exemple, il signalerait une charge particulièrement élevée. Si le producteur d'électricité réagissait à cette annonce, il pourrait en résulter une surtension du réseau. Le mode de transmission des données adopté est la modulation à spectre étalé à sauts de fréquence (*frequency hopping spread spectrum, FHSS)* entre 902 et 928 MHz, de même que les technologies *WLAN* et *GPRS*. Pour le moment, les compteurs d'électricité intelligents ne sont utilisés que dans des projets pilotes. Mais les choses sont sur le point de changer. Dès 2011, les Etats-Unis et l'Europe miseront davantage sur les réseaux de distribution d'électricité intelligents.

Des experts britanniques mettent en garde contre l'utilisation de composantes chinoises dans le secteur des télécommunications

Aux dires d'experts britanniques[21], des composantes fournies par le groupe chinois Huawei permettraient de saboter des infrastructures vitales pour la Grande-Bretagne dans le secteur des télécommunications ou dans l'approvisionnement en électricité et en eau potable. Huawei a livré des pièces maîtresses du nouveau réseau de télécommunications de British Telecom. Fort de ses 87 000 employés, Huawei compte parmi les principaux équipementiers de télécommunications au monde. Il s'agit d'une entreprise privée non cotée en bourse. Son activité de base consiste à développer et fabriquer des appareils pour l'industrie des technologies de la communication (communication mobile, xDSL, réseaux optiques, appareils terminaux, etc.). Les doutes relevées par les experts britanniques n'ont pas pu être jusqu'à présent ni complètement ni partiellement confirmées. Les doutes mentionnées par des experts britanniques n'ont pu été justifiées complètement ou partiellement.

Alors que dans le passé, le pilotage des infrastructures reposait sur des techniques traditionnelles et donc contrôlables, il n'est plus aussi simple de vérifier le fonctionnement des appareils de haute technologie. Ainsi, lors du choix d'appareils ou de la passation de marchés en rapport avec les infrastructures vitales, il faut faire toujours plus attention non seulement au prix d'achat, mais également au niveau de sécurité offert (à long terme). A ce propos, il s'agit d'examiner en détail si une séparation logique suffit ou si l'exploitation des systèmes SCADA doit aussi être séparée physiquement des autres réseaux d'entreprise. Enfin, il est recommandé de recourir à des systèmes redondants afin de pouvoir maintenir l'exploitation de l'infrastructure même en cas de dérangement ou d'accident. Car les pannes de télécommunication (liaisons Internet notamment), d'électricité ou de moyens de transport peuvent entraîner des coûts énormes pour les entreprises comme pour les particuliers.

[21] http://www.telegraph.co.uk/news/worldnews/asia/china/5072204/Britain-could-be-shut-down-by-hackers-from-China-intelligence-experts-warn.html (état: 31.08.2009)

4.4 Guerre de l'information: mise en place d'unités spéciales dans divers pays

La guerre de l'information (information warfare) est une préoccupation majeure des unités chargées de la défense territoriale et de la conduite de la guerre à travers le monde – et pas seulement depuis les attaques massives par déni de service (*denial of service, DoS*) dont les réseaux du gouvernement et du secteur privés estoniens ont fait l'objet en 2007. En Allemagne par exemple, une troupe a été constituée au sein des forces armées en vue de la guerre en réseau (*network centric operations, NCO)*.

La tendance générale à la convergence technique et à la mise en réseau (voir chapitre 5.1) fait que les systèmes militaires de guidage, de communication et de contrôle font toujours plus partie de réseaux intégrés et donc deviennent une cible pour les attaques électroniques. Il s'ensuit qu'en cas d'affrontement guerrier, les moyens militaires conventionnels ne seront plus seuls engagés et qu'une attaque directe des réseaux de l'adversaire entrera aussi en ligne de compte. A contrario, toute armée ayant mis en réseau ses systèmes devra s'assurer de leur inviolabilité.
D'où la tendance depuis quelques années, notamment parmi les grandes puissances militaires comme les Etats-Unis et la Chine, à redoubler d'efforts dans le domaine des TIC. Les capacités mises en place n'ont d'ailleurs vraisemblablement pas qu'une vocation défensive de protection des réseaux nationaux.
En Suisse aussi, le concept d'opérations d'information («information operations») a été examiné de près depuis 2001. L'étude réalisée à ce sujet a débouché sur la mise en place d'un organisme de sécurité informatique pour les infrastructures militaires, le MilCERT.

De telles initiatives soulèvent un certain nombre de questions touchant à l'organisation politique et à l'Etat de droit. Il va de soi que les unités militaires d'un Etat devraient être en mesure de protéger leurs systèmes contre les attaques informatiques venant de l'étranger. Quitte à recourir à des moyens offensifs pour paralyser ou détruire les systèmes de l'adversaire avant d'avoir subi une attaque informatique. De tels moyens peuvent d'ailleurs aussi compléter des opérations militaires. Mais à une époque comme la nôtre où les guerres classiques entre Etats restent l'exception et où les conflits sont principalement réglés en dessous du seuil des hostilités, l'utilisation offensive des systèmes électroniques militaires a beau être tentante, elle serait très périlleuse du point de vue du droit international public.

L'expression de guerre de l'information («cyberwar») a été très souvent utilisée à propos des opérations lancées contre les systèmes d'information du gouvernement géorgien. Or il s'agissait d'attaques à caractère essentiellement criminel, déclenchées contre les systèmes et réseaux informatiques d'un autre Etat. Les agresseurs s'en étant pris, suite au conflit militaire, à la société civile auraient donc logiquement dû être dénoncés pour des activités illégales et poursuivis par la police criminelle de l'Etat des victimes. Il en va de même pour l'action menée par un groupe d'activistes israéliens pendant la guerre de Gaza[22]. Il est vrai que ces deux cas peuvent en partie être jugés sous l'angle du droit militaire, car il s'agissait d'actions menées entre deux Etats – ou parties assimilables à un Etat – lors d'un conflit armé.

Or un brusque assouplissement de ces frontières et la classification de telles actions collatérales comme actes de guerre, justifiant par là une riposte des systèmes électroniques militaires, reviendraient à renforcer la légitimité des mesures militaires dirigées contre des civils, dont la participation au conflit militaire n'est qu'indirecte.

[22] http://www.heise.de/newsticker/Gaza-Konflikt-Der-Krieg-im-Internet--/meldung/121389 (état: 31.08.2009)

Lors de la mise en place et de l'usage de capacités informatiques civiles et/ou militaires il importe de fixer précisément à quelles fins, dans quels cas et surtout contre qui elles pourront servir le cas échéant. En effet, toutes les attaques lancées contre des réseaux militaires ou gouvernementaux ne constituent pas des actes de guerre. Même si l'Etat d'où elles émanent devait se trouver dans un conflit à caractère belliqueux. Même la nature de ces attaques est difficile à déterminer. Souvent, un vrai agresseur ne peut pas être identifié et des mesures de rétorsion peuvent causer des dégâts collateraux dans le pays de déstination.

Les exemples estoniens et géorgiens montrent que de telles agressions peuvent n'être que de nature criminelle, et donc qu'il y a lieu de les poursuivre et de les réprimer avec les moyens dont disposent les autorités de poursuite pénale. Tout brouillage de cette ligne de démarcation risque d'aboutir à des empiétements inutiles du pouvoir militaire dans les domaines d'activité des autorités civiles chargées en premier lieu du maintien de la sûreté intérieure. Au bout du compte, l'Etat affaiblirait sans nécessité les règles ordinaires applicables à la poursuite pénale, à commencer par la protection des droits fondamentaux des accusés.

4.5 Recrudescence d'attaques DDoS à mobile politique

Selon l'entreprise de sécurité Arbor Networks[23], les attaques politiques électroniques se multiplient. Tant leur fréquence que le nombre de cibles sont en constant essor. Parmi les facteurs d'explication, même les non spécialistes peuvent se procurer et utiliser des outils DDoS comme «Black Energy» ou «NetBotAttacker». De tels outils comportent en effet une interface conviviale. L'essai tenté par la BBC en apporte la preuve (voir chapitre 4.7). Alors que les attaques DDoS antérieures visaient surtout les sites pornographiques, celle lancée contre l'Estonie a rappelé que cette technique peut également servir d'arme politique. Outre l'agression dont la Géorgie a été victime[24], des cyberpirates russes ont notamment réussi en janvier 2009 à priver le Kirghizistan de l'usage d'Internet[25]. Leur attaque avait pris pour cible les deux principaux fournisseurs d'accès Internet. Bien qu'ils n'aient pu être élucidés, les mobiles des agresseurs étaient vraisemblablement aussi d'ordre politique.

Il importe de relever que la qualité des attaques DDoS observées ne cesse de s'améliorer. En particulier, elles nécessitent toujours moins d'ordinateurs. Par exemple, les attaques par amplification via un serveur DNS permettent d'obtenir un effet important même avec un petit réseau de zombies. Dans un cas d'espèce[26], un transfert de données de 5 gigabits/seconde a été obtenu à l'aide de 2000 ordinateurs seulement.

[23] http://www.arbornetworks.com (état: 31.08.2009)
[24] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (état: 31.08.2009)
[25] http://www.pcwelt.de/start/sicherheit/firewall/news/192009/russische_cyber_miliz_attackiert_kirgisistan/ (état: 31.08.2009)
[26] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (état: 31.08.2009)

4.6 Panne de réseau chez T-Mobile

Mardi 21 avril 2009 vers 16 heures, toute communication est devenue impossible sur le réseau de T-Mobile. Il s'agit à ce jour de la plus grande panne d'un réseau de téléphonie mobile allemand[27]. Tous les services vocaux ou SMS sont devenus inaccessibles. La défaillance provenait d'une erreur logique de l'enregistreur de localisation nominal (*home location register, HLR)*, qui établit la liaison entre la station de téléphonie mobile et le numéro d'abonné correspondant. En cas de panne du HLR, il n'est plus possible d'établir de liaison et le réseau cesse d'être accessible. Une fois le dérangement réparé, le réseau est redevenu progressivement accessible vers 19 heures.

Le 25 juin 2009, le réseau téléphonique d'E-Plus est à son tour resté muet dans toute l'Allemagne pendant près de deux heures. Cette fois, la panne semble être due à une erreur du serveur central de transmission[28].

Dans les deux cas, une composante centrale aurait été à l'origine de la panne. Ces systèmes sont généralement conçus de manière redondante pour éviter toute défaillance. Cette solution protège très bien des pannes de matériel (p. ex. au niveau du serveur). Or dans le cas de T-Online au moins, il semble s'être agi d'une panne de logiciel. Et comme les systèmes redondants comportent plus ou moins le même logiciel et la même configuration, il n'est guère étonnant que lors de la commutation sur le système de secours, des problèmes de logiciel identiques à ceux du système principal soient apparus et que ce système se soit lui aussi bloqué.

Il importe de souligner que dans le cas de T-Mobile, la mobilisation du service de piquet a été difficile. En effet, comme les techniciens compétents sont généralement alertés par le propre réseau de téléphonie mobile de l'opérateur, il peut être problématique de les joindre. Or suite à l'essor de la téléphonie mobile, toujours plus de services de piquet et d'urgence sont joignables par le réseau mobile. D'où la nécessité de toujours prendre en compte les conséquences qu'une panne de réseau aurait pour le dispositif de secours.

4.7 Grande-Bretagne: achat d'un réseau de zombies par la BBC pour les besoins d'une émission

La société de diffusion BBC a acquis le logiciel de contrôle d'un *réseau de zombies* pour préparer une émission sur la cybercriminalité. Selon la BBC, le réseau baptisé «Click», du nom de l'émission, comptait 22 000 *ordinateurs zombies* au moment de l'achat. Il avait été découvert lors de la visite de chatrooms spécialisés. De tels espaces de discussion servent aux criminels à lier connaissance et à proposer leurs services. Un réseau de zombies est formé par le regroupement d'ordinateurs qui sont infectés par un maliciel et peuvent être commandés à distance par un pirate. Ces 22 000 zombies auraient coûté 700 dollars. Ce montant est avantageux, sachant qu'il s'agissait d'un réseau polyvalent dont les ordinateurs étaient disséminés dans le monde entier. Le prix de vente d'un réseau de zombies est proportionnel à sa qualité. BBC parle de prix pouvant grimper à 300 ou 400 dollars par millier de zombies. A des fins de démonstration, deux adresses électroniques test ont été inondées de milliers de pourriels en l'espace de quelques heures. De même, la BBC rapporte avoir

[27] http://www.welt.de/webwelt/article3603796/T-Mobile-schenkt-Gratis-SMS-als-Entschuldigung.html (état: 31.08.2009)

[28] http://www.zdnet.de/news/wirtschaft_telekommunikation_e_plus_netz_gestern_90_minuten_lang_ausgefallen_story-39001023-41005882-1.htm (état: 31.08.2009)

paralysé un site Web, lors d'une attaque par déni de service distribué (DDoS) lancée d'entente avec l'exploitant de ce site. Il s'est avéré à cette occasion que les demandes de 60 ordinateurs du réseau avaient suffi au blocage du site. Entre-temps, la BBC aurait informé de la situation les propriétaires des ordinateurs infectés. A cet effet, un message d'avertissement s'est affiché sur l'écran des systèmes infectés.

Cette façon d'agir amène à se demander si, par exemple, une entreprise de sécurité aurait le droit de se procurer un réseau de zombies et de le manipuler afin qu'il se désinstalle ou, comme dans le cas présent, qu'il affiche un message d'avertissement sur les ordinateurs infectés. Le débat sur cette option pour combattre les réseaux de zombies n'est pas près de finir. L'acquisition de réseaux de zombies semble toutefois contreproductive, car elle rendrait encore plus lucratif pour les cybercriminels de lancer de tels produits sur le marché. Le rapport de la BBC montre toutefois clairement qu'il est possible de diriger un réseau de zombies à l'aide de programmes simples dont peuvent se servir même les non spécialistes. La tendance se poursuit toutefois dans ce domaine. L'année dernière, des cybercriminels ont mis au point le modèle commercial Crimeware-as-a-Service[29]. Ce genre de plate-forme permet aux pirates de «louer» directement le service désiré, sans avoir à s'embarrasser de considérations techniques. Tout indique que ce nouveau modèle connaîtra une forte expansion au cours de l'année 2009.

4.8 Etats-Unis: multiplication des pertes de données en 2008

Selon l'Identity Theft Resource Center[30], basé à San Diego, pas moins de 35 millions de jeux de données ont été égarés en 2008 aux Etats-Unis. Les pertes signalées par les entreprises ou les autorités sont ainsi en hausse de 47 % par rapport à 2007. La plupart des cas sont survenus dans le secteur privé. Selon ces recherches, le secteur financier et les entreprises de cartes de crédit ont été les plus actifs dans la mise en place de mesures de prévention. L'Identity Theft Resource Center a classé en cinq catégories les événements responsables de pertes de données: perte de supports de données (ordinateurs portables, clés USB, etc.), vol de données tant interne qu'externe, publication ou diffusion involontaire d'informations à caractère personnel, et enfin perte de données par des prestataires externes.

Tout indique d'une part qu'il y a eu une recrudescence des vols de données, d'autre part que les pressions se sont accrues pour que les pertes de données soient rendues publiques. La Suisse ne tient toutefois pas de statistique officielle de ce genre d'incidents. La législation fédérale sur la protection des données ne contient d'ailleurs aucune norme explicite qui obligerait les propriétaires de fichiers à signaler ce genre de mésaventure. On sait néanmoins que de tels incidents n'épargnent pas la Suisse, à l'instar de la publication en mai 2008 de données confidentielles concernant l'Accord de Schengen sur le site Internet du Département fédéral de justice et police (DFJP).[31]

Un concept de sécurité intégrale doit impérativement se concentrer, en raison des multiples possibilités de perte de données, sur la protection des informations elles-mêmes. Ainsi les canaux de distribution, les droits d'accès et les lieux de stockage des données seront adaptés à la valeur effective de l'information. Car tout canal de diffusion ou lieu de stockage

[29] MELANI, rapport semestriel 2008/II, point 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=fr (état: 31.08.2009)
[30] http://www.idtheftcenter.org/ (état: 31.08.2009)
[31] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=fr (état: 31.08.2009)

n'offre pas le même degré de sécurité, de même que les documents ne présentent pas tous le même degré de sensibilité. D'où la nécessité d'affiner la gestion des risques inhérents à l'utilisation qui est faite des données et de l'information. La sensibilisation du personnel revêt ici une grande importance. En effet, les mesures techniques de sécurité ont beau faire partie de la protection élémentaire des données, elles sont vaines en cas de traitement trop laxiste de l'information. Or le maillon le plus faible et le plus vulnérable de la chaîne de sécurité reste le plus souvent l'être humain.

4.9 Les Etats-Unis veulent renforcer la lutte contre les cybermenaces et améliorer la protection existante

En début d'année, le nouveau gouvernement de Barack Obama a publié son agenda concernant la sécurité aux Etats-Unis. Les réseaux électroniques du pays y étaient promus au rang de «biens stratégiques» et la protection de l'infrastructure TIC nationale constituait une priorité. Il s'agissait également de désigner un cyber coordinateur – ou «Cyber Tsar» – directement subordonné au Président, chargé de superviser les services actifs dans ce domaine. Par ailleurs, un effort de recherche et de développement était annoncé, afin de mettre au point une nouvelle génération de matériels et logiciels plus sûrs destinés aux réseaux du secteur public.

La «Cyberspace Policy Review» a été publiée à la fin de mai. Il s'agit d'un état des lieux du cyberespace, assorti de recommandations stratégiques à l'attention des Etats-Unis. Les auteurs concluaient qu'à long terme, Internet fusionnerait avec les technologies traditionnelles de télécommunication et que d'autres exploitants d'infrastructures seraient amenés à faire du réseau Web un canal primaire pour l'interconnexion de divers systèmes (voir aussi SCADA, chapitres 4.3 et 5.2).

A l'instar de nombreuses infrastructures d'approvisionnement de base en biens physiques, Internet est lui aussi exploité dans une large mesure par des acteurs privés. Aussi la Cyberspace Policy Review reconnaît-elle que la sécurité dans ce domaine dépend de la collaboration avec ces acteurs privés. L'Etat ainsi que les exploitants privés d'infrastructures importantes ont un intérêt immédiat au fonctionnement fiable des technologies utilisées et à une transmission en toute sécurité des données dans les infrastructures d'information. D'où la recommandation faite aux Etats-Unis de bâtir un partenariat public-privé au profit de la cybersécurité, dont les partenaires viseraient ensemble, à travers les échanges d'information et la coordination de leurs activités, à renforcer la sécurité, la résilience et la robustesse du monde numérique. Autre constat important, les Etats-Unis ne pourront résoudre seuls les problèmes liés à Internet, qui doivent être envisagés dans leur contexte international. Autrement dit, il s'agit tout à la fois de remanier les bases juridiques et les directives en vigueur, pour qu'une nation numérique résiliente et robuste s'impose sur le sol américain, et de créer un cadre se prêtant à des interventions coordonnées des acteurs impliqués à tous les échelons (local, national, international) en cas d'incidents dans le cyberespace.

4.10 La Commission européenne prévoit de mieux protéger ses infrastructures critiques

L'Union européenne a également reconnu que les TIC sont de plus en plus étroitement liées à notre quotidien et qu'elles constituent une partie essentielle de l'économie et de la société européennes, soit qu'elles fournissent des biens et services d'importance capitale, soit qu'elles servent de base à d'autres infrastructures critiques.

En raison de la dépendance croissante à l'égard des infrastructures d'information critiques, de l'interconnexion transfrontalière de ces dernières et de leur interdépendance vis-à-vis d'autres infrastructures, ainsi que de leur vulnérabilité et des menaces auxquelles elles sont exposées, une approche systémique s'impose pour améliorer la sécurité et la résilience de ces infrastructures. Il s'agit là d'une première ligne de défense contre les défaillances et les attaques, toute panne des infrastructures d'information critiques pouvant gravement perturber des fonctions essentielles de la société.

Les toutes récentes attaques lancées contre les infrastructures de l'information en Estonie, en Lituanie et en Géorgie ont montré que les services et réseaux de communications électroniques sont soumis à d'incessantes menaces.

La Commission européenne plaide par conséquent, dans sa communication du 30 mars 2009 relative à la protection des infrastructures d'information critiques[32], pour des mesures propres à renforcer la sécurité, la résilience et la robustesse d'Internet et, plus généralement, des infrastructures d'information critiques. A cet effet, la Commission entend encourager les partenariats public-privé. En outre, elle prévoit de définir une base commune de capacités et de services en vue d'une coopération paneuropéenne, d'établir un forum pour le partage d'information entre Etats membres et de déployer un système européen de partage d'information et d'alerte. Elle invite les Etats membres à élaborer des plans nationaux en cas d'urgence et à organiser régulièrement des exercices portant sur la réaction en cas d'incident de grande envergure affectant la sécurité des réseaux. Il s'agira naturellement aussi de renforcer la collaboration entre les CERT et les CSIRT nationales.

L'UE entend ainsi s'engager davantage pour protéger l'Europe des cyberattaques et des perturbations de grande envergure, en améliorant l'état de préparation, la sécurité et la résilience.

4.11 Volte-face de Facebook sur ses conditions générales

Au début de février, le fondateur de Facebook a modifié les conditions générales d'utilisation (CG) de son réseau social. Facebook disposait déjà d'un droit d'utilisation irrévocable de toutes les données publiées. La modification des CG visait à étendre cette licence aux données effacées. Face au tollé de protestations soulevé, Facebook a toutefois décidé d'en revenir à ses anciennes conditions d'utilisation.[33]

[32] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:FR:PDF (état: 31.08.2009)
[33] http://www.heise.de/newsticker/Facebook-nach-dem-AGB-Debakel--/meldung/133094 (état: 31.08.2009)

5 Tendances / Perspectives

5.1 Informatique dans les nuages, externalisation, centralisation et propriété de l'information

Le 17 mai 2009, la population suisse a approuvé par 50,1 % des voix l'introduction des *passeports biométriques*. Outre les réticences liées à la protection des données, il semblerait que ce soit surtout l'argument de la sûreté de l'information qui ait conduit à un résultat aussi serré. L'enjeu était le mode d'enregistrement prévu pour les données biométriques. Les données seront enregistrées de manière centrale, pour tous les cantons, à l'Office fédéral de la police (fedpol). Pendant la campagne de votation, cette solution a été dénoncée à plusieurs reprises comme gros risque inutile. Si l'enregistrement des données s'effectuait dans le canton d'origine, une attaque fructueuse ne livrerait pas accès à la totalité des données, mais seulement à une partie d'entre elles. Autrement dit, il ne suffirait pas d'une attaque fructueuse contre la Confédération pour mettre la main sur tous les enregistrements biométriques et il en faudrait donc, dans le meilleur des cas, 26 lancées contre les centres de données des cantons.

De telles réflexions relatives aux risques font partie du quotidien de la sûreté de l'information. Alors que la sécurité TIC reste un des piliers de tout bon concept de sûreté de l'information, la protection de l'information elle-même joue de plus en plus un rôle de premier plan. Il s'agit ici d'un processus classique d'évaluation et de gestion des risques. A titre d'exemple, le blocage de Facebook dans des entreprises n'est pas seulement dû à un souci d'efficience au travail, mais se justifie aussi sur le plan technique. Toutefois, l'un des principaux risques des sites de réseautage personnel (*social networking*) tient au lien pouvant être établi avec l'employeur et au préjudice qui en résulte quand s'il s'agit de sujets délicats. En pareil cas, seules des règles de conduite définissant, indépendamment des technologies, les limites de l'usage autorisé de l'information, dans la sphère privée comme dans le cadre professionnel, porteront leurs fruits. Il s'agit de fixer clairement si les données peuvent être diffusées ou sont à protéger, et le cas échéant de quelle façon.

A cette évolution vers une propriété stricte de l'information et vers une classification continue de la valeur des informations ou données et de chaque document s'opposent les possibilités attrayantes et moins coûteuses des banques de données, applications ou plates-formes dont la maintenance et l'entretien sont centralisés. Il s'agit ici notamment de développements comme l'informatique dans les nuages (*cloud computing*), du monopole de fait de Facebook dans le domaine du *réseautage personnel*, ou encore des systèmes SCADA visant à la centralisation, au reporting en temps réel à la direction[34] et à l'efficience. Les services proposés par l'informatique dans les nuages vont par exemple des applications à la création et à la gestion documentaire. Elle émane d'un prestataire tiers digne de confiance, qui veille également à la sécurité générale du système. Les différences au niveau des programmes de correction, des versions des applications, etc. dans la même entreprise appartiennent ainsi au passé. Il en résulte toutefois aussi une concentration du risque et, le cas échéant, un point de défaillance unique (single point of failure). En définitive, il appartient à chaque entreprise de fixer ses priorités, dans le traitement de l'information, entre l'efficience et les réductions de coûts ou alors la gestion interne de systèmes (sécurité et entretien).

[34] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état: 31.08.2009)

Il faut savoir qu'il deviendra toujours plus difficile de concilier les pressions sur les coûts, le souci d'efficience et de disponibilité de l'information avec les gros risques, l'externalisation des informations et données critiques ainsi que les vulnérabilités croissantes liées à la mise en réseau de plates-formes standardisées. Ce conflit d'objectifs et d'intérêts devra être résolu de cas en cas, par une pesée des risques opérée sur la base d'un maximum d'informations et qui dépendra en premier lieu de la teneur des informations à protéger appartenant à l'entreprise.

La méfiance inspirée par l'enregistrement central, au niveau de la Confédération, des données biométriques reflète déjà une prise de conscience réjouissante. Toutefois il faudrait faire preuve de la même méfiance face aux solutions privées analogues. Il suffit de penser aux nombreux profils de clients créés et actualisés par beaucoup d'entreprises.

5.2 SCADA

L'évolution des systèmes SCADA se poursuivra et, sous l'effet des pressions économiques, le pilotage à distance et l'exploitation sans personnel s'étendront progressivement des composantes isolées jusqu'aux sous-stations entières. La présence d'une technologie de réseau homogène correspond encore au vœu des dirigeants d'un rapprochement entre les réseaux commerciaux et ceux de contrôle. Un exemple à cet égard vient des compteurs intelligents prévus pour le nouveau réseau électrique américain. Or cette évolution posera de nouveaux défis sur le plan de la sécurité TIC. Car il s'agit d'éviter que des incidents, telle l'intrusion de logiciels malveillants dans le réseau d'entreprise, n'aient d'incidence sur le réseau de contrôle. D'où la nécessité d'étendre aux systèmes de contrôle les principes usuels de la sécurité TIC ou les normes et directives correspondantes, et d'exiger des fabricants d'appareils qu'ils prévoient des mécanismes de sécurité suffisants. Pour être complet, tout train de mesures devra inclure des échanges d'expériences au sein des exploitants de systèmes de contrôle (p. ex. sur les vulnérabilités) ainsi qu'entre ceux-ci et les autorités à même de leur livrer des informations sur l'état actuel des menaces. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI est en étroit contact avec les fournisseurs électriques suisses et participe activement aux échanges internationaux d'informations.

5.3 Evolution générale de la cybercriminalité

MELANI et le SCOCI[35] continuent d'être informés chaque jour de toutes sortes de cas de fraude à la commission, de prétendus gains en loterie ou d'abonnements forcés. Cette forme de cybercriminalité reste apparemment payante. Les rapports établis par les pays où de tels abus sont commis le confirment. Des escrocs sont parvenus à y amasser très rapidement des sommes élevées. Les abonnements forcés s'avèrent également très lucratifs au quotidien. A côté de tous les développements techniques liés à la diffusion et à l'utilisation des maliciels, la ténacité, la patience et la créativité permettent donc aussi de s'enrichir sans grandes connaissances techniques. Car parmi les nombreux internautes, un escroc aux aguets finit presque toujours par trouver la victime idéale. Des compléments d'informations

[35] SCOCI: Service national de coordination de la lutte contre la criminalité sur Internet (http://www.scoci.ch/)

sur les formes de tromperie, avec les mises en garde correspondantes, figurent sous les liens indiqués en bas de page[36] [37].

Fraudes à la commission et prétendus gains en loterie

Dans cette arnaque, des pourriels sont envoyés à large échelle à des victimes potentielles. Les offres et promesses figurant dans ces lettres sont inventées de toutes pièces et visent seulement à planter un décor plausible pour pouvoir mener à bien la tromperie. Des courriels annonçant de prétendus gains en loterie continuent également d'être envoyés. Il s'agit là d'une variété de la fraude à la commission .

Cette combine fonctionne, comme le montrent des rapports consacrés au Ghana où sévissent les «sakawas»[38] [39]. Ce sont le plus souvent des jeunes gens issus de milieux défavorisés et rêvant de réussir. Agissant généralement depuis des cybercafés, ils ont mis en pratique tous les stratagèmes connus dans la région, notamment au Nigeria. L'ampleur prise par le phénomène tient au fait que beaucoup d'escrocs ont rapidement fait fortune et exhibent leur richesse, faisant des émules. Le phénomène des «sakawas», apparu dans le contexte de la cybercriminalité, s'est étendu localement à d'autres agissements criminels (y compris des meurtres et homicides[40]), toujours dans un but d'enrichissement personnel.

Offres gratuites

Des personnes signalent régulièrement à MELANI s'être inscrites sur un site et avoir reçu ensuite une facture d'abonnement, suivie de nombreux rappels. De telles offres encouragent l'internaute à conclure un contrat ou à commander sans tarder des prestations. Les coûts et les éventuelles conditions du contrat sont signalés de façon très discrète. Une fois le «contrat» conclu, des rappels et des menaces de mise aux poursuites sont envoyées pour intimider le client. Les lettres sont parfois envoyées au nom d'avocats ou de sociétés de recouvrement, pour effrayer la victime et l'amener à payer «volontairement» la créance douteuse. Les sites en question sont généralement écrits en allemand, et leurs prestataires se montrent toujours plus créatifs et arrogants. Souvent aussi, des factures et des rappels ont été adressés à des personnes ne s'étant jamais enregistrées sur un tel site.

A ce jour, les escrocs cherchaient surtout à attirer les internautes sur de tels sites par le biais des moteurs de recherche. Ainsi, certaines de leurs offres s'affichent en premier lors de la saisie de mots-clés spécifiques dans Google. Apparemment, ils recherchent désormais aussi leurs victimes par courriel[41]. Les techniques destinées à dissimuler les coûts sont toujours plus sophistiquées. Alors que cette information figurait auparavant en petits caractères ou était dissimulée dans les conditions générales, des images animées sont de plus en plus utilisées. Le prix disparaît au bout de quelques secondes, et donc la victime ne le remarque pas. Ces pratiques semblent être florissantes. On sait que chaque jour, 15 à 20 000 euros aboutissent sur les comptes des auteurs de telles offres[42].

Le Secrétariat d'Etat à l'économie (SECO) recommande de ne pas régler ce genre de facture et de déclarer à l'auteur de l'offre par courrier recommandé, aussitôt après avoir

[36] http://www.den-trick-kenne-ich.ch/4/de/ (état: 31.08.2009)
[37] http://www.fedpol.admin.ch/fedpol/fr/home/aktuell/warnungen.html (état: 31.08.2009)
[38] http://www.ghanaweb.com/GhanaHomePage/features/artikel.php?ID=162565 (état: 31.08.2009)
[39] http://www.modernghana.com/news/192603/1/female-sakawa-hits-accra.html (état: 31.08.2009)
[40] http://www.Ghanavoices.wordpress.com/2009/08/13/girls-killed-for-sakawa/ (état: 31.08.2009)
[41] http://www.melani.admin.ch/dienstleistungen/archiv/01089/index.html?lang=fr (état: 31.08.2009)
[42] http://www.pressebox.de/pressemeldungen/ct/boxid-261364.html (état: 31.08.2009)

constaté l'erreur, que l'on a été trompé par le site en question et que l'on conteste le contrat pour cette raison. Le SECO précise qu'une seule lettre suffit: la correspondance que le prestataire ne manquera pas d'envoyer par la suite peut être ignorée.

Pour tout complément d'information, nous vous recommandons de consulter la brochure suivante:
http://www.seco.admin.ch/dokumentation/publikation/00035/00038/02033/index.html?lang=fr

5.4 Infections par drive-by download

Les infections par drive-by download s'affineront à l'avenir pour être toujours plus difficiles à détecter. Aujourd'hui, elles sont généralement chargées de manière statique sur le site Web. Le pirate possède par exemple une liste de données d'ouverture de session FTP. Ces données lui servent à accéder automatiquement au compte, à télécharger une page (généralement la page d'*index* ou un fichier Javascript .js disponible), à y introduire le code malveillant puis à recharger la page infectée. Le pirate peut naturellement aussi accéder au site par une *faille de sécurité*. Le script chargé est toutefois visible et donc détectable pour n'importe quel visiteur ainsi que pour l'administrateur du site Web.

L'année dernière déjà, de nouvelles techniques ont été mises au point pour éviter que les exploitants de sites Web en particulier ne s'aperçoivent de la tromperie. En juin 2008, de nombreux sites suisses ont été piratés en vue du placement d'un *JavaScript* malveillant. L'attaque était perfide, car le code malveillant ne s'exécutait pas lors du chargement normal du site. Il ne s'activait qu'en cas de consultation à partir d'un moteur de recherche comme Google ou Yahoo. En effet, les propriétaires consultent fréquemment leurs sites, mais généralement en saisissant directement l'adresse ou à partir de leur liste de liens favoris. Une telle tactique visait à dissimuler l'infection le plus longtemps possible.

Alors que l'exemple susmentionné était encore conçu à l'aide d'un Javascript statique et qu'une analyse du code source permettait de détecter l'infection, de nouvelles tendances attestent déjà d'une évolution. Ainsi, le code ne figure plus directement sur le site Web, mais c'est le serveur qui l'exécute. Concrètement, le serveur décide à chaque visite s'il y a lieu d'insérer le code malveillant, et le cas échéant sur quelle page. Il devient donc quasiment impossible à l'administrateur du site de reproduire l'infection. Dans un cas récent et concernant aussi un hébergeur suisse, l'attaque semble s'être faite par un compte FTP compromis. Un *script PHP* avait été chargé sur le serveur. Il n'y avait toutefois pas eu de manipulation du site Web mais du serveur, afin qu'il rédige de temps à autre un visiteur sur un site infecté. Un *cookie* chargé d'installer le maliciel aide le pirate à identifier l'ordinateur infecté. En l'occurrence, les redirections ne sont pas seulement dissimulées derrière les pages d'index, mais également derrière des photos et des *favicons*.

Au lieu de IFrames, les redirections étaient logées dans la commande d'actualisation des métafichiers (META Refresh). Or les navigateurs désactivent encore moins de telles redirections que les commandes IFrame. Comme de surcroît elles n'apparaissent qu'à la première visite, elles sont quasiment aussi difficiles à distinguer que les exploits IFrame.

Afin de protéger votre ordinateur contre les attaques par drive-by download, lisez le chapitre consacré aux mesures de prévention (annexe 7.2).

6 Glossaire

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

ActiveX	Technologie développée par Microsoft pour charger de petits programmes – les composants ActiveX – lors de l'affichage de pages Web sur l'ordinateur de l'internaute, d'où ils seront ensuite exécutés. Ils permettent de réaliser divers effets ou fonctions. Cette technologie est malheureusement souvent sujette à un emploi abusif et représente un risque au niveau de la sécurité. Par exemple, de nombreux "numéroteurs" (dialer) sont chargés et exécutés sur l'ordinateur par ActiveX. Le caractère problématique d'ActiveX ne concerne que Internet Explorer, car cette technologie n'est pas compatible avec les autres navigateurs.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Attaque DoS	attaque par déni de service (denial of service). Vise à rendre impossible l'accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs.
Bot / Malicious Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (malicious bots) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
Browser plug-in	Logiciel s'installant sur un navigateur pour lui apporter des fonctions supplémentaires, comme la visualisation de contenus multimédia.
Buffer Overflow	Les dépassements de mémoire tampon (buffer overflow) comptent parmi les lacunes de sécurité les plus fréquentes des logiciels actuels. Un cyberpirate peut en tirer parti à distance, notamment via Internet. Lors d'un tel incident dû à une erreur du programme, la mémoire du système cible reçoit plus de données qu'elle ne peut en contenir, ce qui permet d'y glisser des codes malveillants.
Cloud Computing	L'informatique dans les nuages (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les TIC ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises d'un ou plusieurs prestataires. Les applications et les données ne se trouvent plus sur l'ordinateur local ou au centre de calcul de l'entreprise, mais dans le nuage (cloud). L'accès à ces systèmes à distance s'effectue par un réseau.
Code	Instructions donnant à l'ordinateur les ordres à exécuter.
Computer Emergency Response Team (CERT)	Le terme CERT (ou CSIRT, Computer Security Incident Response Team) désigne un organisme chargé de la coordination et de l'adoption de mesures liées aux incidents relevant de la sécurité informatique.

Content Management System (CMS)	Un système de gestion du contenu (CMS, acronyme de content management system) est une solution flexible et dynamique permettant aux entreprises ou organisations de corriger et ajouter sur des sites Web des textes, des photos et des fonctions multimédias. Un auteur peut actualiser un tel système sans connaissances préalables en programmation ou en langage HTML. Les informations gérées dans ce contexte sont appelées contenu (content).
Cookie	Témoin de connexion. Petit fichier texte enregistré sur l'ordinateur de l'internaute à l'occasion de sa visite sur une page Web. Les témoins permettent par exemple de mémoriser les réglages personnels pour un site Internet. Il est cependant aussi possible de les utiliser abusivement, notamment pour établir un profil détaillé des habitudes de l'internaute.
Domain Name System	Système de noms de domaine. 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).
European Train Control System (ETCS)	L'European Train Control System (qui s'abrège ETCS) est une composante d'un vaste système interopérable de régulation de l'exploitation ferroviaire. L'ETCS vise à remplacer les nombreux systèmes de signalisation et d'arrêt automatique des trains en place dans les pays européens. Il sera instauré à moyen terme sur les tronçons à grande vitesse et sera étendu à long terme à l'ensemble du réseau ferroviaire européen.
Fast Flux	Fast Flux est une technique basée sur le protocole DNS dont les réseaux de zombies se servent pour répartir entre diverses machines hôtes, et donc dissimuler, des sites de phishing ou renfermant des maliciels. Si un ordinateur cesse de fonctionner, le suivant prend le relais.
Flash	Adobe Flash (s'abrégeant Flash, auparavant Macromedia Flash) est un environnement de développement intégré propriétaire servant à créer des contenus multimédia. Flash s'emploie aujourd'hui sur de nombreux sites Web, dans des bannières publicitaires ou comme fonction d'un site, p. ex. comme menu système. Des sites sont entièrement développés à l'aide de Flash.
Frequency Hopping Spread Spectrum (FHSS)	La modulation à spectre étalé à sauts de fréquence (frequency hopping spread spectrum, FHSS) est une technique de modulation du signal radio où, grâce à l'utilisation d'un spectre de fréquences plus grand, les signaux transportant les données ont la possibilité de changer constamment de fréquences, à intervalles rapprochés, selon une séquence connue seulement par l'émetteur et le récepteur.
FTP	File Transfer Protocol (FTP) est un protocole de transfert de fichiers sur un réseau TCP/IP. Il s?utilise par exemple pour charger des pages Web sur un serveur Web.
General Packet Radio Service (GPRS)	Le general packet radio service (service général de radiocommunication par paquets) est un service de transmission numérique des données par ondes radioélectriques, offert sur un

	réseau mobile de type GSM et utilisant la commutation de paquets.
Global System for Mobile Communications Railway (GSM-R)	Global System for Mobile Communications - Rail(way) (GSM-R ou GSM-Rail) est un système privé de téléphonie mobile basé sur la norme GSM, utilisé par les entreprises ferroviaires.
Home Location Register (HLR)	Le home location register (HLR) (enregistreur de localisation nominal) constitue, dans un système de téléphonie mobile, la base de données servant à la gestion des abonnés. On retrouve dans cette base la description de l'identité de l'abonné, la liste des services auxquels il a droit ainsi que les données relatives à sa localisation dans le réseau.
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.
JavaScript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Lecteur MP3	Logiciel ou appareil permettant d'écouter des morceaux de musique comprimés au format MP3.
META Refresh	Les éléments Meta refresh (actualisation des métafichiers), servant à rafraîchir une page Web, peuvent spécifier une URL alternative pour rediriger automatiquement l'utilisateur vers un site différent. Le temps de consultation jusqu'au changement de page peut être défini dans les paramètres de contenu. Exemple: <meta http-equiv="refresh" content="5; URL=http://www.melani.admin.ch" /> L'utilisateur est redirigé ici après cinq secondes vers le site http://www.melani.admin.ch.
Network Centric Warfare (NCW) / Network Centric Operations (NCO)	Network Centric Warfare (NCW, guerre de l'information ou cyberguerre) est un concept militaire servant à désigner la guerre à l'âge de l'information. L'arme de cette lutte est non seulement l'information, mais aussi le contrôle des systèmes d'information.

	Network Centric Operations (NCO) désigne les opérations électroniques menées dans le cadre de la guerre de l'information.
P2P	Peer to Peer Architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux échanges de données.
Page d'index	Fichier d'un serveur/site Web généralement utilisé comme page d'accueil.
Passeport biométrique	Passeport muni de données biométriques lisibles électroniquement. Une puce RFID renferme les données personnelles comme le nom, le sexe, la date de naissance, etc.
PHP	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.
Protocole Internet (IP)	Le terme protocole Internet (Internet Protocol, IP) désigne un protocole de la couche réseau, tel que normalisé dans le modèle OSI. Ce protocole de la suite TCP-IP régit la circulation des informations à travers les réseaux hétérogènes.
Referrer	Le terme referrer (référent) désigne l'adresse URL de la page Web affichant le lien qui a conduit l'utilisateur au site actuel. Cette information fait partie de la requête HTTP transmise au serveur Web.
Réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis.
Réseautage personnel	Traduction du concept américain de «social networking». Un profil ou page de membre permet aux utilisateurs d'une plateforme d'échanger et d'établir des relations entre eux. Des données personnelles y sont souvent publiées (nom, date d'anniversaire, photos, intérêts professionnels, loisirs, etc.).
Rogue Software, Rogueware	Les rogue softwares, ou roguewares, sont des faux utilitaires qui prétendent avoir découvert un logiciel malveillant (généralement un logiciel espion) sur l'ordinateur de la victime pour l'inciter à acheter une solution de sécurité.
Rootkit	Ensemble de programmes et de techniques permettant d'accéder sans être remarqué à un ordinateur pour en prendre le contrôle.
Scareware	Le terme scareware désigne des logiciels vendus par des sociétés éditrices ayant su provoquer chez les clients potentiels du stress ou de la peur. Il s'agit d'une forme automatisée de subversion psychologique. Si la victime tombe dans le panneau et se croit menacée, il lui est suggéré de télécharger un logiciel payant pour éliminer le virus fictif. Parfois la personne se croyant victime de cyberpirates est elle-même amenée à effectuer des manœuvres rendant possible une telle attaque.

Smart Grid	L'expression «smart grid» désigne un réseau de distribution (d'électricité) intelligent, où les donnée de différents appareils (compteurs des consommateurs, etc.) parviennent au producteur grâce aux technologies informatiques. Des ordres peuvent aussi être donnés à ces appareils, selon le réglage du réseau.
Systèmes SCADA	Supervisory Control And Data Acquisition Systèmes servant à la surveillance et à la gestion de processus techniques (p. ex. approvisionnement en énergie et en eau).
Time to live (TTL)	Dans le protocole utilisé par les serveurs DNS, une donnée Time-to-live est présente et indique le temps pendant lequel l'information donnée par le serveur (le plus souvent un nom de domaine ou un autre serveur DNS) doit être conservée en cache. Passé ce délai, l'information doit être considérée comme obsolète et être mise à jour.
USB Memory Stick	Clé mémoire USB. Petit dispositif de stockage des données connecté à l'interface USB d'un ordinateur.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
Ver	A la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur.
Zombie	Traduction de bot / malicious bot.

7 Annexe

7.1 ICANN et l'OFCOM développent des solutions contre les réseaux Fast Flux

Dans son rapport semestriel 2007/II[43], MELANI avait examiné sous l'angle technique les réseaux Fast Flux. Le problème a pris des proportions alarmantes ces deux dernières années. L'ICANN[44], l'organisation s'occupant de la gestion des noms de domaine, s'est vue contrainte d'analyser en détail la situation. Le Comité consultatif pour la sécurité et la stabilité de l'ICANN (Security and Stability Advisory Committee, SSAC)[45] a publié en mars 2008 un premier rapport sur la question. Ce problème confronte l'ICANN à des défis particuliers, car les réseaux Fast Flux exploitent le DNS via les techniques IP «Fast Flux» (enregistrement à durée de vie brève), en changeant de serveurs de noms (Double Fast Flux).

[43] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état: 01.09.2009)
[44] http://www.icann.org (état: 01.02.2009)
[45] http://www.icann.org/en/committees/security/sac025.pdf , voir aussi http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-initial-report-summary26jan09-fr.pdf (état: 01.09.2009)

Dans son premier rapport, le SSAC a déjà proposé une première série de solutions destinées à endiguer ce phénomène. Il convient notamment de mentionner la désactivation des réseaux de zombies hébergeant l'infrastructure Fast Flux, la désactivation des noms de domaine impliqués et la limitation des possibilités de changer de serveur de noms.

La Generic Names Supporting Organization (GNSO) de l'ICANN[46] a publié en janvier 2009, sur la base de ce rapport, un premier rapport du Working Group on Fast Flux hosting (FFWG[47]), dont la version définitive est parue le 6 août 2009[48].

La partie 1 analyse le rapport récemment paru et la partie 2 passe en revue les interventions d'autres organisations cherchant à combattre les réseaux Fast Flux illégaux (surtout dans le domaine du phishing). La partie 3 enfin explique les démarches entreprises en Suisse pour adapter la législation en la matière.

Partie 1

Pour commencer, la GNSO pose le problème de la définition des réseaux Fast Flux utilisés à des fins illégales (Fast Flux attack networks) par rapport aux réseaux volatiles (volatile networking) utilisés en toute légalité. Suite à son rapport intermédiaire de janvier 2009, l'ICANN a donné aux utilisateurs la possibilité de réagir aux études menées jusque-là. Les avis exprimés, qui émanent le plus souvent des principaux acteurs de ce domaine, mais aussi de citoyens privés, sont riches en enseignements. On sait ainsi que divers exploitants Internet utilisent pour leurs activités des techniques similaires aux réseaux Fast Flux. Ce sont, par exemple:

- les organisations qui gèrent des réseaux constituant des cibles potentielles (réseaux gouvernementaux, installations militaires, mais aussi multinationales ou acteurs Internet importants): leur accessibilité doit être garantie en permanence, ce qui a conduit à utiliser une valeur *TTL* basse permettant les transferts de ressources nécessaires;

- les réseaux partagés (comme Akamai): dans ce cas, les réseaux volatiles peuvent répartir entre plusieurs serveurs les données générées ou réduire les temps d'attente au moyen de plusieurs serveurs situés dans des zones géographiques différentes;

- le support de la mobilité: là encore, une durée de vie brève permet de créer des réseaux ad hoc pour soutenir une certaine forme de mobilité;

- la liberté d'opinion / les groupes d'intérêt: il s'agit ici de vaincre la censure avec du matériel qui ne serait pas publiable sinon (en dehors des réseaux Fast Flux, il existe d'autres techniques, comme le réseau Tor servant à héberger des contenus sur différents sites, afin notamment d'empêcher l'identification des ordinateurs).

Il a d'abord fallu réfléchir aux instruments convenant le mieux pour maîtriser les réseaux Fast Flux utilisés à des fins criminelles. Par exemple, l'interdiction des valeurs *TTL* basses nuirait tout autant aux réseaux Fast Flux légaux. La GNSO a donc cherché à définir les propriétés principales des réseaux Fast Flux criminels:

- les nœuds de réseau peuvent être situés sur des ordinateurs infectés; ce n'est toutefois pas une nécessité;

---

[46] http://gnso.icann.org (état: 01.09.2009)
[47] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf (état: 01.09.2009)
[48] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf (état: 01.09.2009)

- ils sont volatiles, en ce sens qu'ils utilisent un groupe d'ordinateurs zombies pour parvenir à cet effet;
- les ordinateurs zombies sont répartis entre des systèmes indépendants les uns des autres (autonomous systems);
- les changements de serveur de noms (name server, NS) sont fréquents;
- les IP des ordinateurs se trouvent surtout dans le segment des clients finaux bénéficiant d'un haut débit (ADSL, câble TV);
- la qualité des entrées Whois est médiocre; les informations concernant le détenteur sont pauvres (fausses déclarations);
- le logiciel de serveur nginx[49] est souvent installé sur les réseaux de zombies. D'où une configuration de proxy inverse, avec plusieurs connexions gérées en même temps entre la victime, le réseau de zombies et le serveur de contrôle (mothership), en vue de la publication de contenu (p. ex. site Web);
- le nom de domaine est enregistré sur un compte préexistant et donc non suspect;
- les noms de domaine apparaissent dans diverses combinaisons chiffrées (p. ex. as1.com, as2.com, as3.com, etc.);
- l'unique but du réseau Fast Flux est de prolonger l'attaque (p. ex. attaque de phishing visant un établissement financier).

Cette analyse a débouché sur deux opinions différentes concernant la meilleure façon de maîtriser les réseaux Fast Flux illégaux. Certains experts recommandent la voie des échanges d'informations, alors que d'autres préféreraient que l'ICANN et ses membres (registraires et registres[50]) s'engagement activement. Les propositions suivantes ont été formulées à propos des échanges d'informations:

- mise à disposition d'informations supplémentaires sur les noms de domaine générés par DNS (et non via Whois). Ces informations pourraient inclure l'âge du domaine, le nombre de changements de serveur de noms sur une période donnée, etc.;
- publication de résumés des réclamations concernant un domaine, selon un classement par registraire, TLD ou serveur de noms;
- encouragement des fournisseurs d'accès à utiliser Netflow/sFlow pour déterminer s'ils comptent des réseaux de zombies parmi leur clientèle;
- soutien aux initiatives privées visant à faciliter les échanges d'informations (à l'instar de l'Anti-Phishing Working Group pour la lutte contre le phishing).

D'autres experts, favorables à des mesures plus énergiques de la part de l'ICANN et de ses membres, préconisent les solutions suivantes:

---

[49] http://nginx.net (état: 01.09.2009)

[50] Les registres (registry) sont les organisations responsables de l'attribution des ressources relatives aux numéros Internet (numéros IP, systèmes autonomes). Quant aux registraires (registrar), ils s'occupent de gérer les réservations de noms de domaine.

- procédures accélérées visant à effacer des noms de domaine en collaboration avec des organes accrédités;

- mise en place de règles pour l'utilisation de valeurs TTL basses et limitation du nombre de changements autorisés dans une période donnée pour les enregistrements d'adresses ou de serveurs de noms;

- identification des serveurs de noms comme «statiques» ou «dynamiques». Les serveurs statiques devront indiquer l'adresse IP du serveur de noms. Il serait envisageable de percevoir une taxe spéciale sur les serveurs de noms dynamiques;

- prélèvement d'une taxe spéciale en cas de changement de serveur statique, répartie pour moitié entre l'ICANN et le registre. Les recettes serviraient à améliorer la lutte contre les abus;

- amélioration de la procédure d'enregistrement des noms de domaine.

Nous verrons ci-dessous que certaines de ces procédures sont déjà utilisées en Suisse ou qu'elles font l'objet d'une procédure de consultation. D'autres en revanche sont peu goûtées, comme l'idée de percevoir un supplément de taxe en cas de changement de serveur DNS. Une telle mesure serait contreproductive d'un point de vue commercial.

A la fin de son rapport, le groupe de travail recommande d'examiner les idées suivantes, dans l'optique des développements à venir:

- examiner lesquelles des solutions proposées pourraient soit être inscrites dans la loi, soit être reprises par l'industrie ou simplement être retenues comme pratiques d'excellence;

- évaluer la meilleure manière d'impliquer les registraires et les registres dans la politique de désactivation des noms de domaine;

- élaborer un système de signalement de données Fast Flux (Fast Flux Data Reporting System, FFDRS), soit une banque de données collectant des informations sur de tels réseaux;

- charger l'ICANN de définir des pratiques d'excellence visant à mieux réglementer le secteur pour limiter les activités illégales;

- examiner les possibilités d'impliquer d'autres parties prenantes dans la procédure d'élaboration de mesures de lutte contre les réseaux Fast Flux illégaux.

Partie 2

Le rapport final du groupe de travail de la GNSO signalait à plusieurs endroits les interventions d'autres associations visant à endiguer les réseaux Fast Flux illégaux (surtout dans le domaine du phishing). Cette deuxième partie les examine en détail.

Parmi les groupes les plus actifs dans ce domaine figure indiscutablement l'Anti-Phishing Working Group (APWG[51]). Il s'agit d'un collectif d'acteurs économiques spécialisés dans la lutte contre le vol d'identités et les tentatives de phishing par courriel. Dans un rapport

[51] http://www.antiphishing.org (état: 01.09.2009)

d'octobre 2008[52], l'APWG adresse aux registres diverses recommandations visant à prévenir le phishing ou tout au moins à en atténuer les effets.

Différentes solutions sont envisageables selon l'APWG, de la sensibilisation des utilisateurs aux techniques visant à démasquer les tentatives d'escroquerie, en passant par les systèmes complexes d'identification et les méthodes rapides de désactivation des domaines de phishing. Les cinq principales recommandations sont exposées ci-dessous:

- procédure sommaire de désactivation des noms de domaine, prévoyant une collaboration étroite entre les registres et les organes accrédités;

- exploitation active des données collectées pour découvrir et désactiver les noms de domaine utilisés pour lancer des cyberattaques;

- transmission aux autorités de poursuite pénale des noms de domaine utilisés pour les cyberattaques;

- protection des clients contre les tentatives de phishing. En effet, dès qu'ils se sont emparés des données d'accès à la gestion des noms de domaine de clients, les cybercriminels peuvent modifier les DNS de domaines existants ou en enregistrer de nouveaux, en se servant de l'identité non suspecte d'un client normal[53];

- interdiction ou limitation de l'usage des sites Fast Flux. Les restrictions concerneraient les changements de nom des serveurs DNS ou la durée de vie minimale en minutes (TTL).

Le rapport de l'APWG contient encore toute une série de recommandations:

- une fois identifié un nom de domaine à partir duquel une activité illégale est déployée, ne pas se contenter de le bloquer mais vérifier si d'autres noms de domaine ont été enregistrés à partir des mêmes indications (nom, IP, courriel, adresse, carte de crédit);

- installer un système de blocage des enregistrements de domaines suspects (registrar lock), puis collecter un maximum d'informations, des en-tête de requêtes http jusqu'aux données personnelles du détenteur. Chercher ensuite à confirmer les données collectées: vérifier s'il existe des noms de domaine aux propriétés analogues (p. ex. s'ils se relaient grâce à des combinaisons chiffrées, voir plus haut); vérifier si les noms contiennent des fragments de noms de domaine ou de marques connus (eBay, PayPal, établissements financiers divers); analyser les adresses IP utilisées pour l'enregistrement de noms et chercher à les comparer avec les listes noires existantes (comme Spamhaus XBL p. ex.); contrôler l'authenticité des adresses électroniques; rendre obligatoire le nom de domaine complet (fully qualified domain name, FQDN), et donc l'indication de l'adresse IP; contrôler les cartes de crédit utilisées.

- le cas échéant, développer ensuite un système d'attribution de points aux données récoltées, pour parvenir à un filtrage aussi précis que possible.

L'APWG a fait de nombreuses propositions qui exigent des efforts considérables et une réelle volonté de collaboration. L'APWG n'est toutefois pas un cas isolé. Entre autres

---

[52] Anti-Phishing Best Practices Recommendations for Registrars, http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf (état: 01.09.2009)

[53] http://www.icann.org/committees/security/sac028.pdf (état: 01.09.2009)

initiatives visant le même but, il convient de mentionner le Whois Data Problem Reporting Service (WDPRS)[54]. Il s'agit d'une interface Web permettant aux utilisateurs de signaler aux registraires affiliés à l'ICANN des données Whois de noms de domaine incomplètes ou manifestement fausses. En effet, ce peut être un premier indice d'une utilisation abusive de ces noms. Un autre projet a pour nom Phishtank[55]. Ce portail permet à chacun d'annoncer des courriels de phishing (avec les noms de domaine qu'ils contiennent). D'où une banque de données régulièrement alimentée, que n'importe qui peut interroger pour savoir si un site de phishing repéré y figure déjà. Trois organisations encore sont actives dans ce domaine: le Messaging Anti-Abuse Working Group (MAAWG[56]), forum rassemblant l'industrie mondiale de la messagerie électronique; ShadowServer[57], qui s'occupe principalement de la surveillance des activités des réseaux de zombies; StopBadware[58], qui se concentre sur la création d'une banque de données des logiciels malveillants présents sur la toile.

Partie 3

La Suisse n'est pas non plus restée inactive. Plusieurs nouveautés au niveau législatif marquent le début de la répression de ce genre de criminalité. Une première étape a consisté à modifier les conditions générales d'enregistrement des noms de domaine finissant par .ch. Jusqu' à février 2009, il était possible de se servir d'un nom de domaine dès son acquisition, la facture émise étant payable à 30 jours. Les escrocs avaient donc beau jeu d'enregistrer des noms de domaine pour un mois sans rien payer. Le nom de domaine était effacé à l'expiration du délai de paiement et après l'envoi infructueux d'un rappel. Pour mettre fin à ce genre d'abus, SWITCH a modifié les dispositions du contrat d'enregistrement[59]. Celui-ci stipule désormais que «la saisie dans le fichier de zone intervient généralement 24 heures après le traitement de la réception du paiement chez SWITCH». Autrement dit, il faut payer le nom de domaine avant de pouvoir s'en servir. Cette première mesure s'est avérée dissuasive contre l'enregistrement massif de domaines en .ch à des fins de phishing constaté en 2008.

Ce n'est pas tout. L'Office fédéral de la communication (OFCOM) a élaboré un avant-projet de loi qui doit encore être mis en consultation. Il y est question d'ajouter un nouvel article à l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT). Cet article conférerait à SWITCH la possibilité de bloquer et d'effacer tout nom de domaine en .ch soupçonné d'être utilisé pour:

- répandre des codes malveillants;
- accéder à des données sensibles par des méthodes illégales.

La déclaration de soupçon serait faite à un organe accrédité par l'OFCOM.

Le point essentiel et aussi le plus controversé de tous les rapports (p. ex. document de l'APWG ou de la GNSO, voir plus haut) portait sur l'introduction de procédures accélérées permettant, grâce à la collaboration des registraires et des organes accrédités, de bloquer temporairement ou d'effacer complètement un nom de domaine. Un projet de loi dans ce sens ferait faire à la Suisse un grand pas en avant dans la lutte contre la cybercriminalité.

---

[54] http://wdprs.internic.net (état: 01.09.2009)
[55] http://www.phishtank.com (état: 01.09.2009)
[56] http://www.maawg.org (état: 01.09.2009)
[57] http://www.shadowserver.org (état: 01.09.2009)
[58] http://www.stopbadware.org (état: 01.09.2009)
[59] https://www.nic.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQXU234MN6SC2T4PAQGM6TDMI#a8 (état: 01.09.2009)

7.2 Réglages des navigateurs contre des infections drive-by courantes

Introduction

Chaque site comporte une série d'instructions, qui forment le code HTML. Ces instructions signalent au navigateur (p. ex. Internet Explorer) comment doit se présenter le contenu du site consulté. Si certains sites sont formés de documents textuels exclusivement et ne prévoient aucune fonction supplémentaire (pages statiques), d'autres offrent des contenus dynamiques. Tel est le cas des écritures mobiles, des formulaires de commande en ligne, des images animées ou des bannières publicitaires au contenu changeant. De telles fonctions dynamiques sont réalisables à l'aide de contrôles ActiveX et de JavaScript. Elles peuvent hélas aussi servir à provoquer des actions indésirables et préjudiciables à l'ordinateur du visiteur.

Recommandations générales

Actualiser régulièrement le système d'exploitation et les applications
Certains produits disposent d'une fonction de mise à jour automatique qu'il faudrait toujours utiliser. Contrôler régulièrement qu'elle soit activée. Les sites des fabricants renseignent généralement sur les mises à jour actuelles des logiciels.

Limiter les fonctions de JavaScript
Limiter autant que possible l'exécution des JavaScripts (Active scripting) dans les paramètres du navigateur (ou désactiver cette fonction). Il faut savoir qu'en cas de désactivation de JavaScript, de nombreux sites Web ne fonctionneront plus correctement. Si la navigation en pâtit, il convient d'assouplir les restrictions (par étapes) jusqu'à ce que la gêne redevienne supportable.

Limiter les contrôles ActiveX (Internet Explorer uniquement)
Limiter autant que possible l'exécution des contrôles ActiveX dans les paramètres du navigateur.

Régler sur le niveau élevé les paramètres de sécurité d'Internet Explorer. Les pages 5 et 6 des Instructions pour configurer Windows XP en toute sécurité[60] expliquent pas à pas comment procéder (ces explications servant à régler le niveau de sécurité d'Internet Explorer restent valables pour d'autres systèmes d'exploitation Windows).
Important: Comme beaucoup de sites Web font appel à Active scripting, il ne sera plus possible de visionner entièrement certains sites après avoir modifié ces paramètres. D'où la recommandation d'inscrire dans la liste des «Sites de confiance» les sites Web fréquemment consultés (auxquels on fait confiance). Les Instructions pour configurer Windows XP en toute sécurité indiquent là encore comment procéder, en page 6.

Remarque: le réglage sur «haut» du niveau de sécurité d'Internet Explorer désactive automatiquement les fonctions suivantes (Javascript, IFrame et actualisation des métafichiers).

[60] http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=fr (état: 01.09.2009)

Les pages qui suivent passent en revue les principales sources d'infection par drive-by download et les mesures à prendre pour s'en protéger.

Cas 1: Javascript camouflé (tentative de rediriger l'ordinateur à l'aide de Javascript sur un site malveillant).

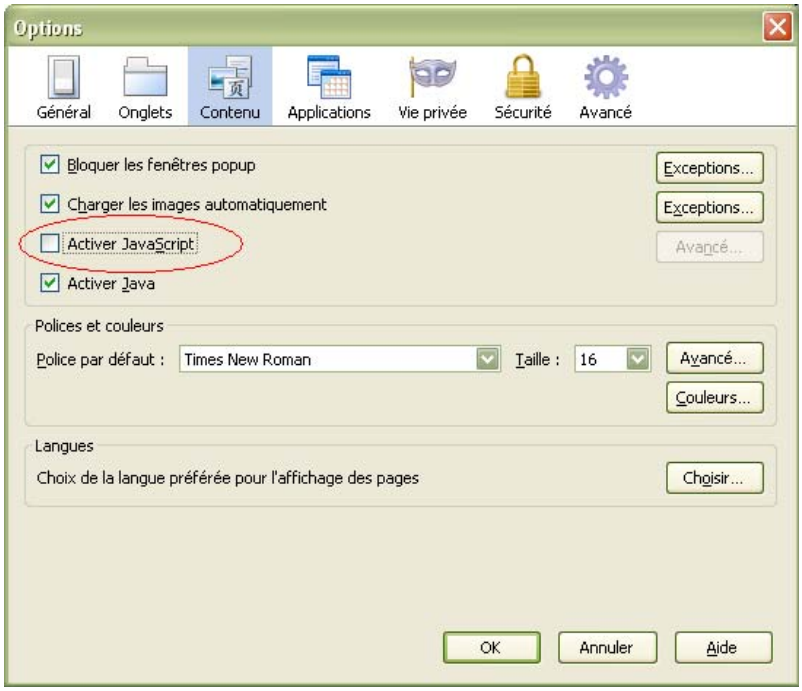
➔ Solution: désactiver Javascript.

➔ Inconvénient: les sites utilisant Javascript ne fonctionnent plus.

Firefox

Première possibilité: utilisation du programme NoScript[61]. Il suffit d'un clic de souris pour activer durablement ou brièvement Javascript en vue de la consultation d'un site.

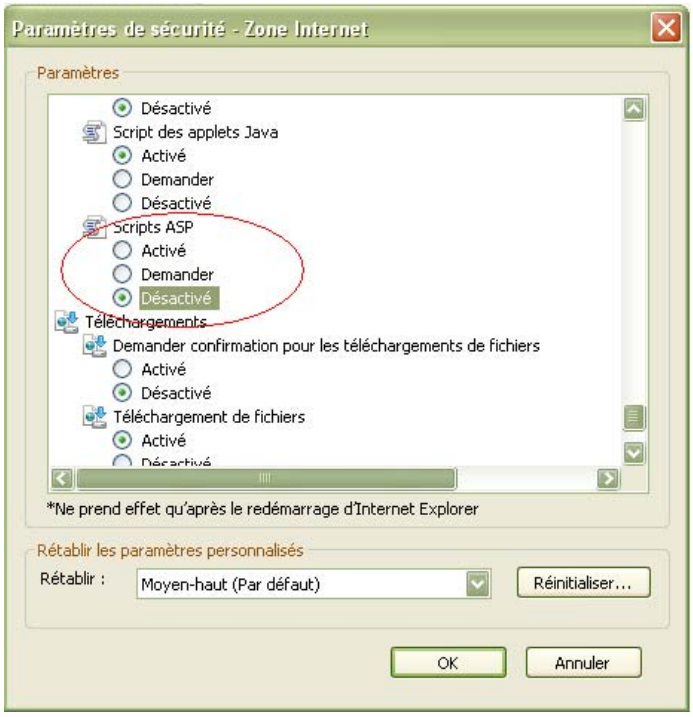
Seconde possibilité: sous Outils ➔ Options ➔ Contenu: ne pas cocher Activer Javascript



Internet Explorer

Sous Outils ➔ Options Internet ➔Sécurité ➔ adapter le niveau autorisé pour la zone Internet. Il est possible soit de désactiver complètement la fonction Scripting, soit alors d'indiquer pour chaque site utilisant Javascript si l'on souhaite l'activer (Invite de commandes).

[61] https://addons.mozilla.org/de/firefox/addon/722 (état: 01.09.2009)



Cas 2: exploit IFrame (un IFrame – nouvelle page insérée dans une page – sert au navigateur à ouvrir un site malveillant en arrière-plan).

➔ Solution: désactiver IFrame.

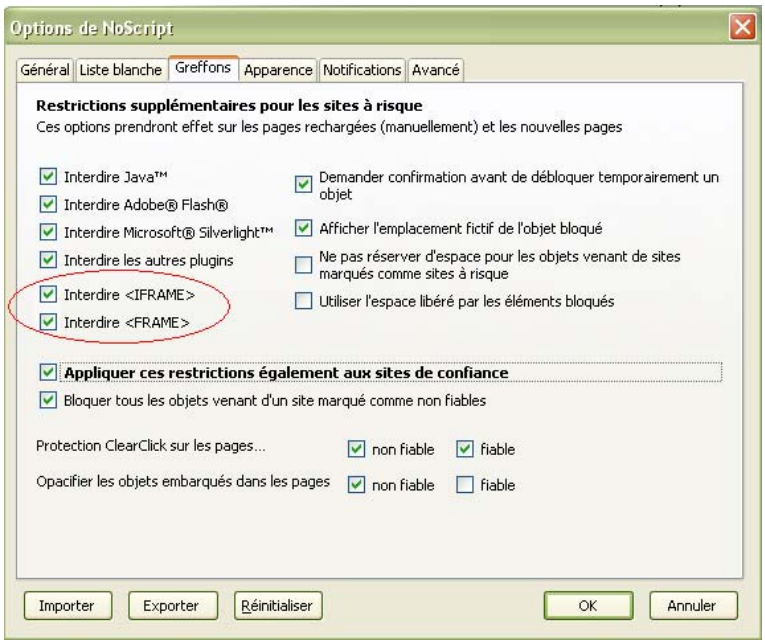
➔ Inconvénient: les sites ayant besoin des IFrames ne fonctionnent qu'imparfaitement.

Firefox

Première possibilité: utiliser le programme NoScript.

Après avoir installé le programme NoScript, cliquer dans le navigateur sur le côté droit de la souris, sélectionner l'entrée NoScript et modifier la rubrique des paramètres.

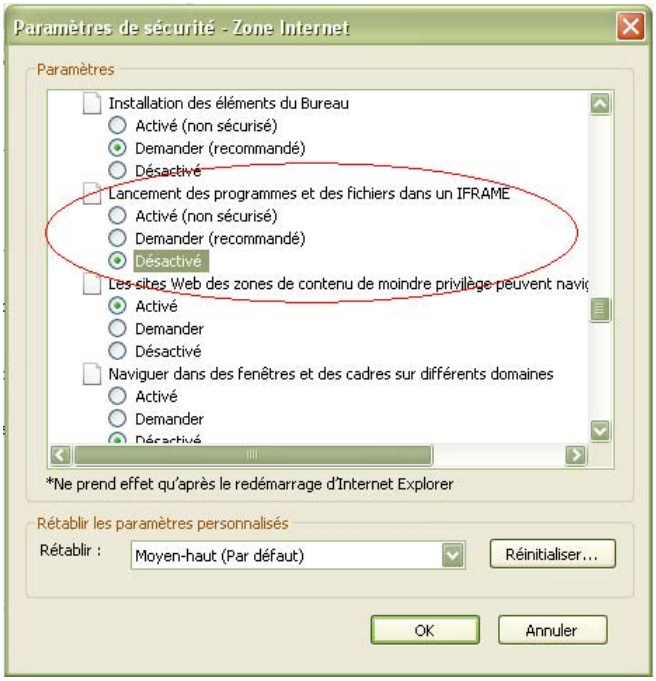
Sélectionner Interdire <IFRAMES> et interdire <IFRAME>.



Seconde possibilité: indiquer la commande: **About:config** dans la ligne d'adressage du navigateur Firefox, puis régler la fonction **Browser.frames.enabled** sur **false**.

Internet Explorer

Sous Outils ➔ Options Internet ➔Sécurité ➔ adapter le niveau autorisé pour la zone Internet. Le lancement des programmes ou des fichiers dans un IFrame doit être complètement désactivé, ou alors il faut régler ce paramètre pour que l'ordinateur demande pour chaque site comportant un IFrame s'il doit être activé (Invite de commandes).



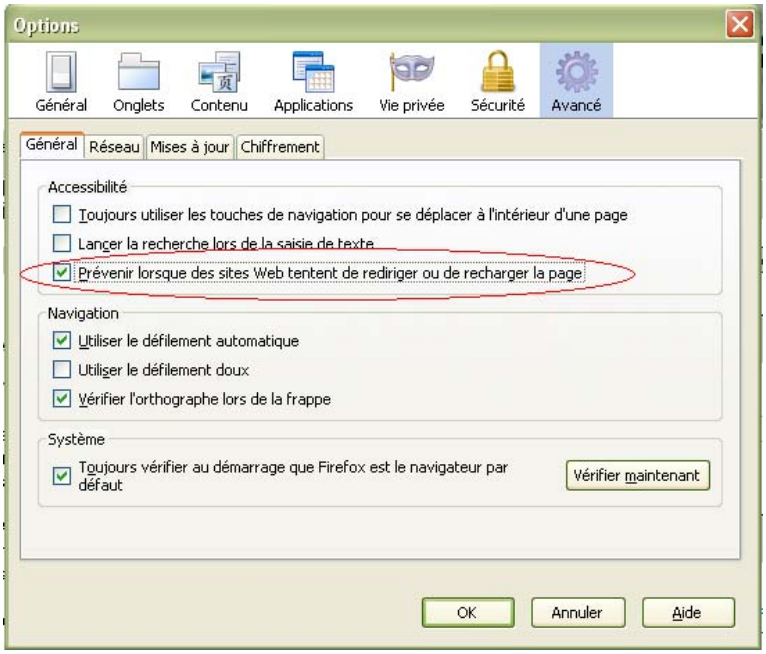
Cas 3: META Refresh (la commande d'actualisation des métafichiers redirige automatiquement le navigateur vers un site infecté).

➔ Solution: restreindre les éléments META Refresh.

➔ Inconvénient: les sites comportant des redirections ne fonctionnent plus qu'en partie.

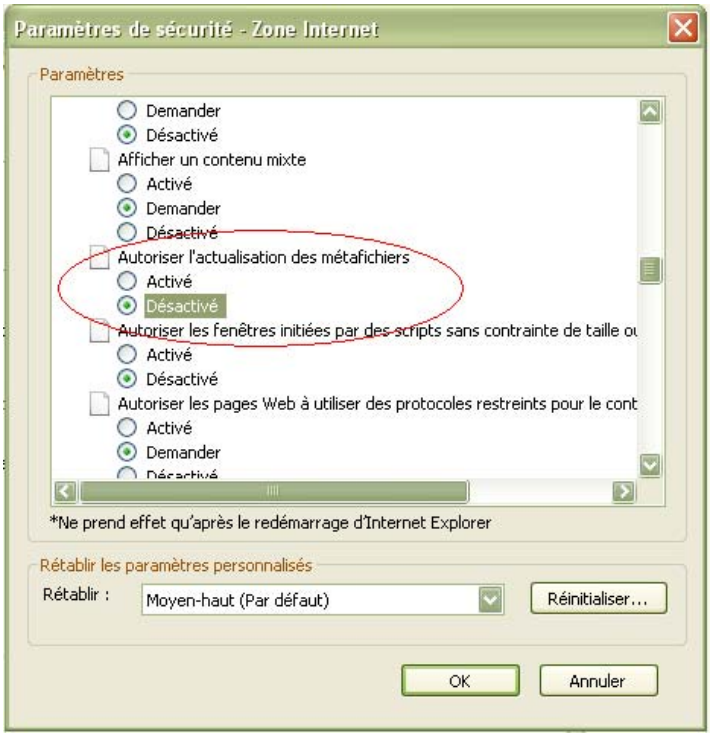
Firefox

Sous Outils ➔ Options «Prévenir lorsque des sites Web tentent de rediriger ou de recharger la page». Chaque fois qu'une tentative est faite pour rediriger le navigateur, il faudra donner une confirmation manuelle.



Internet Explorer

Sous Outils ➔ Options Internet ➔Sécurité ➔ adapter le niveau autorisé pour la zone Internet. Les éléments d'activation des métafichiers (META Refresh) peuvent être complètement désactivés.


Paramètres de sécurité - Zone Internet
Paramètres
Demander
Désactivé
Afficher un contenu mixte
Activé
Demander
Désactivé
Autoriser l'actualisation des métafichiers
Activé
Désactivé
Autoriser les fenêtres initiées par des scripts sans contrainte de taille ou
Activé
Désactivé
Autoriser les pages Web à utiliser des protocoles restreints pour le cont
Activé
Demander
*Ne prend effet qu'après le redémarrage d'Internet Explorer
Rétablir les paramètres personnalisés
Rétablir :
Moyen-haut (Par défaut)
Réinitialiser...
OK
Annuler