Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

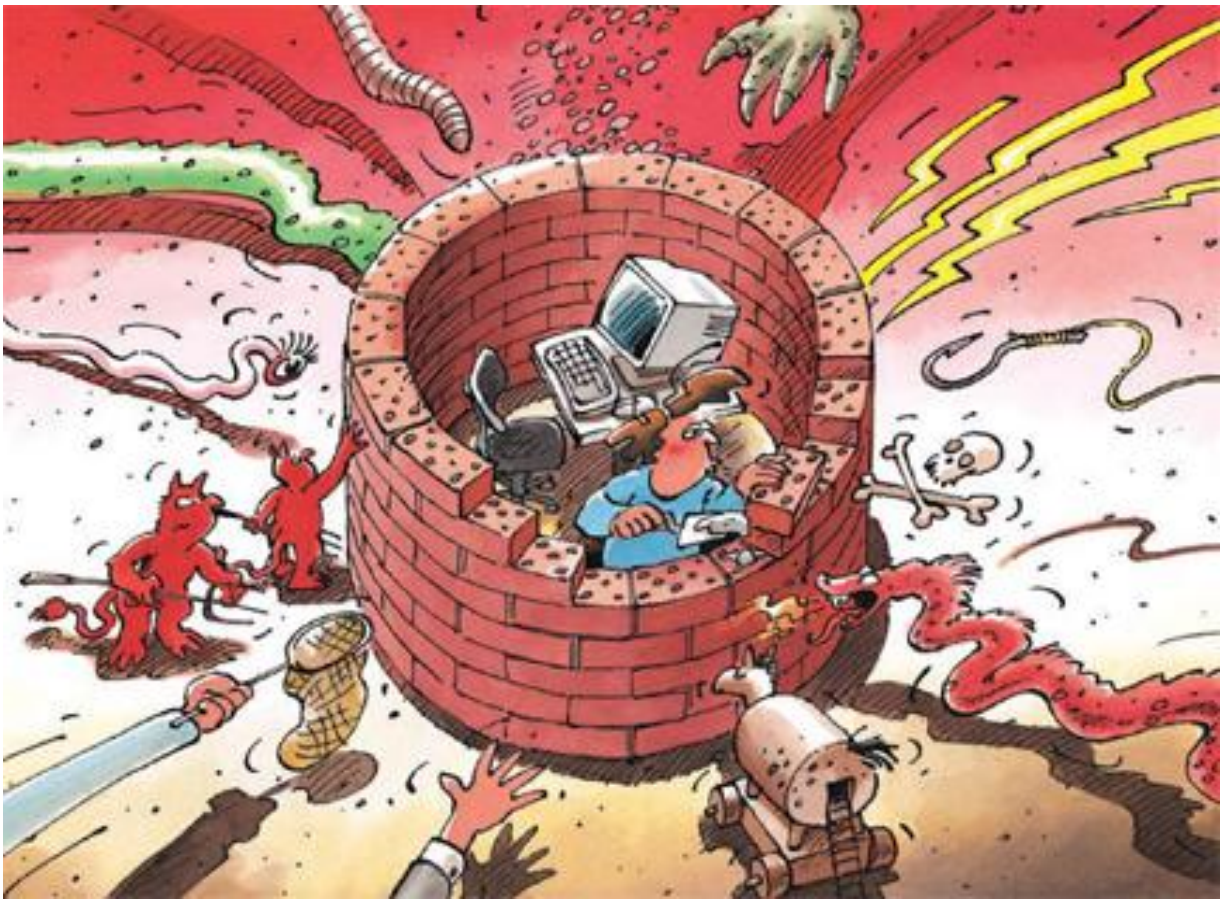
Unité de pilotage informatique de la Confédération UPIC
Service de renseignement de la Confédération SRC

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

# Sûreté de l'information

## Situation en Suisse et sur le plan international

Rapport semestriel 2013/I (janvier – juin)



# Table des matières

# 1 Temps forts de l'édition 2013/I

**DDoS – attaques massives en Suisse aussi**
Le premier semestre 2013 a été marqué par la plus grave attaque DDoS de l'histoire d'Internet. La cible était Spamhaus, organisation à but non lucratif basée en Suisse. Des serveurs DNS suisses ont été détournés pour des attaques DDoS. En janvier 2013, l'infrastructure DNS de la fondation SWITCH a notamment servi à lancer une attaque contre des tiers. MELANI rappelle les mesures à prendre pour protéger sa propre infrastructure DNS contre les attaques par amplification DNS.
► **Situation en Suisse:** chapitre 3.1

- **Surveillance des communications sur Internet**
  Les médias ont abondamment parlé au semestre écoulé des méthodes d'écoute potentiellement utilisées par quelques services de renseignement et rendues publiques par l'informateur Edward Snowden. Les premières révélations concernaient Prism, programme de surveillance de la NSA, avant la découverte des possibilités dont dispose en Grande-Bretagne le Government Communications Headquarters (GCHQ) de se brancher sur les câbles sous-marins transatlantiques, et la publication d'une présentation du programme d'analyse XKeyscore.
  ► **Situation sur le plan international:** chapitre 4.1
  ► **Tendances / Perspectives:** chapitre 5.1
- **Advanced Persistent Threats – publication de nombreux cas**
  Au premier semestre 2013, de nombreuses cyberattaques raffinées, visant des entreprises ou des services étatiques, ont été rendues publiques. Comme les soupçons portaient généralement sur des acteurs étatiques, ces attaques ont été suivies de nombreuses déclarations politiques.
  ► **Situation sur le plan international:** chapitre 4.2
- **Les systèmes de gestion de contenu, nouveau talon d'Achille**
  Le nombre de sites Web a explosé ces dernières années. Grâce aux outils simples proposés, même les non-spécialistes peuvent publier leur propre site Internet. Des systèmes de gestion de contenu (content management system, CMS) sont souvent utilisés à cet effet. Leur popularité croissante les rend intéressants pour les cybercriminels. Et les escrocs à l'affût des vulnérabilités de tels systèmes finissent toujours par en trouver.
  ► **Tendances / Perspectives:** chapitre 5.4
- **Essor des chevaux de Troie dans la téléphonie mobile**
  La tendance des maliciels à se reporter sur les téléphones mobiles s'est poursuivie au semestre écoulé et a fortement augmenté ces derniers mois. Le système d'exploitation Android est leur cible préférée.
  ► **Situation en Suisse:** chapitre 3.3
  ► **Tendances / Perspectives:** chapitre 5.6
  ► **Annexe:** chapitre 7.1
- **Systèmes SCADA et SCI: aspects problématiques, failles de sécurité, cyberattaques et protection**
  En principe, on parle de «système de contrôle industriel (SCI)» à propos de tout système servant à régler ou surveiller un processus physique. Alors que les systèmes informatiques classiques mettent l'accent, outre la disponibilité, sur la confidentialité et l'intégrité, la disponibilité est jugée absolument prioritaire dans les SCI.
  ► **Situation sur le plan international:** chapitre 4.5

# 2 Introduction

Le dix-septième rapport semestriel (janvier à juin 2013) de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI) commente les grandes tendances et les risques liés aux technologies de l’information et de la communication (TIC), livre un aperçu des événements survenus en Suisse et à l’étranger, signale divers thèmes de la prévention et résume les activités des acteurs étatiques ou privés. Les termes techniques ou spécialisés (écrits en italique) sont expliqués dans un **glossaire (chapitre 6)** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleur.

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

**Les chapitres 3 et 4** passent en revue les pannes et les incidents, les attaques, la criminalité et le terrorisme visant les infrastructures TIC. Des exemples choisis illustrent les principaux événements des six premiers mois de l’année 2013. La situation nationale est analysée au chapitre 3 et la situation internationale au chapitre 4.

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

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

# 3 Situation en Suisse de l'infrastructure TIC

## 3.1 Intensification des attaques DDoS

Ces derniers mois, les *attaques par déni de service distribué (DDoS*) sont restées au cœur de l'activité des cybercriminels. On peut distinguer ici entre de nombreuses sortes d'attaques DDoS. Les unes recourent à un *réseau de zombies*, formé de machines infectées ou de serveurs capturés dans Internet. D'autres formes d'attaques DDoS tirent parti des systèmes mal ou trop peu sécurisés dans Internet et/ou des failles inhérentes aux protocoles Internet. De telles attaques DDoS ont beau ne pas être nouvelles, leur nombre et leur intensité ont augmenté ces derniers mois. Et si les banques américaines restent la cible favorite des attaques DDoS, plusieurs entreprises suisses ont subi le même sort (voir plus loin le paragraphe sur les infections par Brobot). Des informations plus détaillées figurent aux chapitres suivants.

**Plus grave attaque DDoS de l'histoire, contre Spamhaus**

Une gigantesque cyberattaque, la plus grave attaque DDoS lancée à ce jour par Internet, est survenue au premier semestre 2013. La cible était Spamhaus[1], organisation à but non lucratif suisse active dans la lutte contre les pourriels et autres menaces du cyberespace.

En mars 2013, des inconnus ont lancé une attaque DDoS massive contre le site Web de Spamhaus. L'attaque a duré plusieurs jours, avec un débit maximal en données transmises de 300 gigabits par seconde (Gbit/s), soit la capacité de plus de 50 CD. Spamhaus s'est adressé à son hébergeur CloudFlare, qui a tenté de déjouer l'attaque. Les agresseurs ont répliqué aux mesures défensives de CloudFlare en attaquant le nœud d'échanges Internet LINX à Londres (London Internet Exchange), ce qui a provisoirement perturbé tout le trafic de données effectué par ce nœud Internet[2].

Ce genre d'attaque DDoS est appelé par les experts *DNS amplification attack*. Des requêtes *DNS* truquées ont été adressées à des serveurs DNS publics (*open DNS resolver*[3]). Comme l'adresse IP source indiquée était celle de Spamhaus, ces serveurs ont envoyé leur réponse à Spamhaus et non à l'expéditeur réel du *paquet de données*. Et comme une réponse à une demande DNS est parfois bien plus longue que la requête, les pirates sont parvenus à causer avec une largeur de bande relativement faible une très forte charge du réseau, culminant à 300Gbit/s.

---

1 The Spamhaus Project: http://www.spamhaus.org/ (état: 31 août 2013).

2 The Verge - Spam war caused failure at critical internet exchange center: http://www.theverge.com/2013/3/28/4156570/Dutch-spamhaus-DDoS-took-down-london-internet-exchange (état: 31 août 2013).

3 Pour plus d'information sur la quantité de Open DNS resolver dans les AS suisses, veuillez consulter: http://securityblog.switch.ch/2013/05/02/ddos-and-open-resolvers-the-swiss-view/ (état: 31 août 2013).

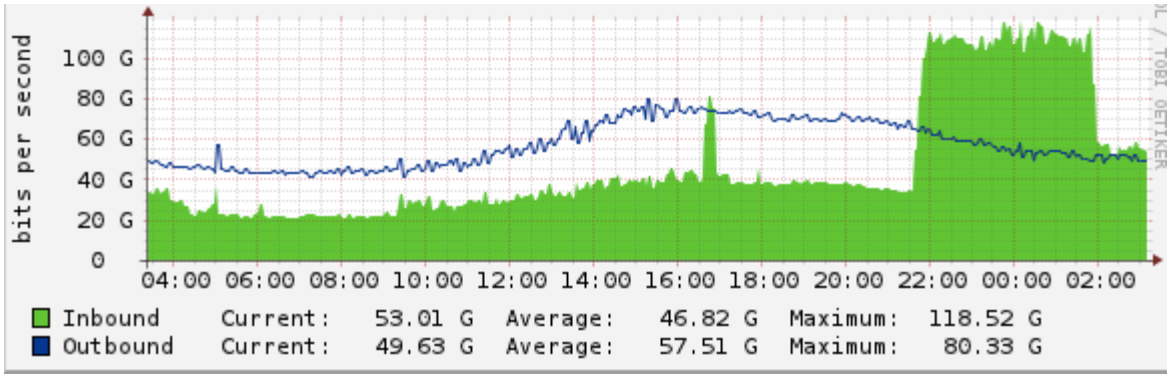



Fig. 1: Trafic réseau avant, pendant et après l'attaque DDoS (source: CloudFlare).

Selon certaines sources, une attaque d'une telle ampleur aurait temporairement paralysé Internet. MELANI n'est pas en mesure d'étayer ces suppositions: en Suisse tout au moins, il a fonctionné de manière irréprochable.

Les mesures suivantes permettent de protéger toute infrastructure DNS des attaques malveillantes commises par rebond DNS (*DNS amplification attack*):

*Prévention de toute usurpation d'adresse IP (IP address spoofing):*

Il faut s'assurer que les appareils en ligne ne puissent pas envoyer des paquets de données en remplaçant leur identité par celle d'autrui (*IP address spoofing*). A cet effet, le standard BCP38 (BCP = best current practice) a été conçu en 2000 et publié sous le titre RFC2827. Or cette norme a beau exister depuis plus de dix ans, une grande partie des fournisseurs de services Internet (*Internet Service Providers, ISP)* ne l'ont que partiellement reprise, voire l'ignorent jusqu'ici.

Afin d'éviter autant que possible que l'infrastructure TIC suisse ne puisse servir à lancer ce genre d'attaques DDoS, MELANI recommande à tous les fournisseurs de services Internet suisses d'introduire à grande échelle la norme (BCP38) décrite dans le document RFC2827, afin de déjouer toute usurpation d'adresse IP.

*Protection des serveurs DNS:*

Une autre mesure pour réduire à l'avenir l'impact des *attaques par réflexion* consiste à protéger les serveurs DNS. De nombreux serveurs (DNS), et quantité de périphériques réseau, sont raccordés à Internet par une configuration standard (généralement les paramètres d'usine de l'appareil). Or de telles configurations sont souvent peu sûres et trop peu restrictives. Ainsi, les appareils acceptent les requêtes provenant de la totalité d'Internet. D'où l'importance de configurer les appareils ou logiciels pour qu'ils ne traitent que les requêtes provenant du domaine d'adresses IP local ou d'autres domaines spécifiés. Une telle précaution permet d'éviter que des escrocs ne se servent de serveurs DNS pour lancer des attaques dans Internet.

MELANI recommande aux exploitants de serveurs DNS ou d'appareils proposant un service DNS de respecter ou de mettre en œuvre les normes et pratiques d'excellence suivantes:

1. RFC 5358 (BCP140) Preventing Use of Recursive Nameservers in Reflector Attacks: http://tools.ietf.org/html/bcp140

2. Windows 2003 Server – Securing DNS:
   http://technet.microsoft.com/en-us/library/cc785404%28v=ws.10%29.aspx
3. Secure BIND Configuration Template:
   http://www.cymru.com/Documents/secure-bind-template.html
4. Désactivation de la récursivité DNS (si elle n'est pas nécessaire):
   http://www.team-cymru.org/Services/Resolvers/instructions.html
5. Mise en place de la technologie RRL (Response Rate Limiting):
   http://www.redbarn.org/dns/ratelimits

## Détournement d'un serveur DNS suisse pour une attaque DDoS

Des serveurs DNS suisses sont aussi détournés pour des attaques DDoS. En janvier 2013, l'infrastructure de la fondation SWITCH, qui gère les domaines de premier niveau (TLD) «.ch» et «.li», a servi à lancer contre des tiers une *DNS amplification attack*[4]. Les pirates ont généré via l'infrastructure DNS, à partir d'une faible bande passante, un flux sortant qui a inondé la cible visée, au plus fort de l'attaque, à un débit de 500 Mbit/s.

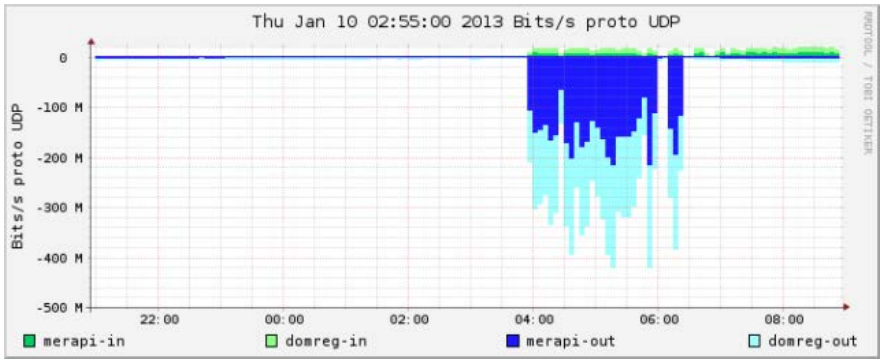



Fig. 2: Trafic réseau avant, pendant et après l'attaque DDoS (source: SWITCH Security Blog).

Comme l'infrastructure DNS de SWITCH est conçue pour un important trafic de données, cette sollicitation abusive n'a pas affecté les domaines de premier niveau «.ch» et «.li». Selon SWITCH, cette attaque par amplification DNS a permis d'obtenir, avec une bande passante de 3 MB/s seulement, des réponses de l'ordre de 225MB/s. Il a donc suffi pour mener à bien une telle attaque, outre certaines compétences techniques, d'un raccordement par câble ou DSL standard. Cet exemple montre que de nos jours, une attaque DDoS est possible à très peu de frais. SWITCH a toutefois bien réagi et très vite neutralisé l'agresseur.

## Attaques DDoS basées sur Brobot en Suisse aussi

Le dernier rapport semestriel MELANI s'est fait l'écho d'attaques DDoS lancées contre plusieurs banques américaines[5]. Le volume de données mobilisées, atteignant parfois

---

4 SWITCH Security Blog - CH-Zone Opfer eines DNS-Amplifikations-Angriffes: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff/ (état: 31 août 2013).

5 MELANI rapport semestriel 2012/2, chapitre 4.2.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: 31 août 2013).

60 Gbit/s, a ralenti l'accès à leurs sites Web, voire l'a rendu impossible par moments. L'Iran serait à l'origine de l'agression.

Les attaques sont réalisées à l'aide de serveurs Web compromis. Les pirates passent au crible Internet, à la recherche d'installations vulnérables utilisant Joomla![6]. Quand ils en découvrent une, ils tirent parti d'une faille de sécurité bien connue de Joomla! afin de placer un *maliciel* sur le site Web de la victime. Ce maliciel est un *script PHP* malveillant du nom de Brobot[7], qui aménage dans le système une porte dérobée et possède une fonctionnalité DDoS. Les serveurs piratés comportent un réel avantage pour les agresseurs: comme les serveurs Web disposent souvent d'une bande passante plus large que les raccordements usuels à Internet, il suffit de quelques zombies pour mener des attaques DDoS efficaces.

Des sites Web suisses ont également fait les frais de Brobot. MELANI a prévenu au premier semestre 2013 des dizaines d'exploitants de sites infectés:

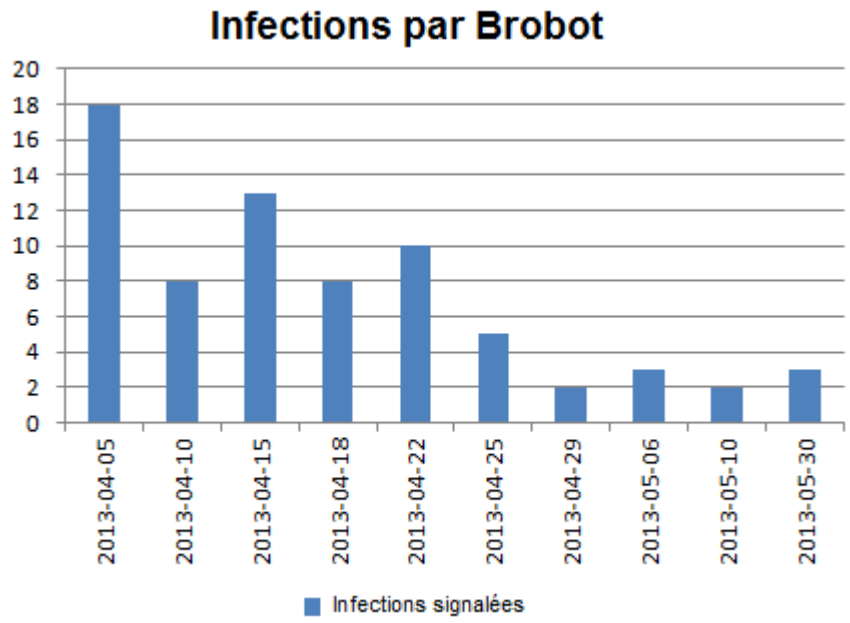



Fig. 3: Infections Brobot signalées par MELANI.

MELANI a informé des infections les propriétaires des sites concernés et leurs hébergeurs. Les exploitants n'ont cependant pas tous réagi – si bien que certains sites Web sont restés infectés pendant plusieurs mois et ont régulièrement servi à lancer des attaques DDoS contre des banques américaines.

---

6 Joomla! est un système de gestion de contenu très répandu.

7 Symantec - PHP.Brobot: http://www.symantec.com/security_response/writeup.jsp?docid=2013-011012-0840-99&tabid=2 (état: 31 août 2013).

## 3.2 Tendances en matière de phishing

De nombreuses tentatives de phishing ont à nouveau été signalées au premier semestre 2013. La tendance des pirates à s'en prendre aussi à la clientèle e-banking des petits établissements bancaires s'est poursuivie. Apparemment, il vaut la peine de configurer et d'adapter les systèmes spécialement pour de telles cibles, même si statistiquement parlant les escrocs ne découvrent à chaque fois qu'une ou deux victimes potentielles.

### Obstacles à la désactivation

Diverses techniques utilisées par les criminels pour empêcher les administrateurs de désactiver leurs sites de phishing ont déjà été discutées dans un précédent rapport semestriel.[8] Une nouvelle technique a été observée pendant la période sous revue. En l'occurrence, l'affichage du site de phishing dépendait du fuseau horaire paramétré dans le navigateur. Le phishing n'intervenait que si l'heure normale d'Europe centrale était programmée, faute de quoi un message d'erreur s'affichait. Il s'agissait bien entendu de faire croire au fournisseur de services Internet (p. ex. américain) que le site était déjà désactivé et qu'il ne devait plus rien faire. Un site frauduleux reste ainsi plus longtemps en ligne et aura tendance à piéger davantage de victimes.

### Premier site de phishing en *Flash* contre un établissement financier suisse

D'habitude, les escrocs créent leurs pages de phishing à partir du site original de la banque, auquel ils apportent quelques petites modifications, puis l'enregistrent sur un serveur spécialement préparé. Cette façon de procéder est relativement simple et ne nécessite pas de connaissances informatiques spéciales. Curieusement, un premier site de phishing conçu en langage *flash* et visant un établissement financier a été découvert. Seules des hypothèses sont possibles sur les raisons ayant poussé les escrocs à recourir à cette forme de programmation compliquée. Le plan du site suggère que les escrocs pourraient avoir utilisé un kit simple pour la création de formulaires de sites Web, qui générait des versions flash. Une autre explication tient à l'impossibilité d'analyser le texte figurant dans les programmes flash. Les programmes antiphishing sont bien incapables d'identifier un tel site de phishing à l'aide de mots-clés, puis de prévenir la victime.

### La clientèle e-banking des petites banques n'est pas épargnée

On observe depuis quelque temps qu'outre les sociétés émettrices de cartes de crédit et les grandes banques, les plus petites banques font toujours plus souvent l'objet de tentatives de phishing. Les escrocs s'imaginent sans doute que ces établissements financiers n'ont pas encore pris des mesures de sécurité suffisantes, ou que leur clientèle n'a guère été confrontée jusqu'ici à ce phénomène.

Statistiquement parlant, une cyberattaque contre de petites banques n'aurait de sens qu'à condition de disposer d'une excellente base de données et de s'adresser exclusivement, de manière ciblée, aux clients des établissements en question. Or une telle approche ciblée n'a

---

[8] MELANI rapport semestriel 2011/2, chapitre 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2013).

pas été constatée. Apparemment, la diffusion et l'envoi des messages de phishing continuent de se faire au hasard.

## 3.3 Téléphonie mobile: essor des maliciels d'e-banking

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a mis en garde, au premier semestre 2013, contre une nouvelle vague d'attaques visant les sessions suisses d'e-banking avec signature des transactions par SMS. La méthode consiste tout d'abord à installer un logiciel malveillant sur l'ordinateur de la victime. Quand celle-ci s'identifie sur son compte d'e-banking, une annonce apparaît, lui signifiant qu'elle doit installer un nouveau certificat de sécurité. A cet effet, il lui est demandé de donner son numéro de téléphone portable ainsi que le modèle de l'appareil. Elle reçoit alors un SMS lui demandant d'installer son nouveau certificat. En réalité, il s'agit d'un programme malveillant, permettant aux criminels d'intercepter les SMS utilisés pour la signature des transactions et d'effectuer des transactions frauduleuses.


Fig. 4: Fenêtre s'affichant pendant la procédure d'ouverture d'une session d'e-banking et invitant le client à installer un certificat sur son téléphone portable.

Les banques suisses ne demandent jamais à leurs clients, dans une fenêtre apparaissant à l'écran ou par SMS, d'installer de nouveaux éléments de sécurité sur leur appareil. MELANI recommande donc aux utilisateurs d'e-banking invités, pendant une session, à installer sur leur téléphone un certificat (voir photo) ou quelque chose d'analogue, d'interrompre leur transaction, de se déconnecter de la plate-forme d'e-banking (bouton Quitter) et de prévenir aussitôt leur banque. L'annexe 7.1 renferme une description complète de cette cyberattaque.

## 3.4 Attaques d'ingénierie sociale contre des sociétés suisses

Des tentatives d'escroquerie ciblées recourent à diverses méthodes d'ingénierie sociale. Ces attaques visent toujours plus souvent des petites et moyennes entreprises (PME).

Deux cas d'entreprises suisses signalés à MELANI méritent d'être exposés ici. Dans le premier, remontant à mars 2013, le directeur financier d'une PME déployant une activité interna-

tionale a reçu un courriel qui semblait émaner de son CEO. Il ressemblait à s'y méprendre aux courriels internes et invitait le directeur financier à virer une grosse somme sur le compte d'un avocat, en vue d'une prétendue acquisition faite en Chine. Le projet était naturellement inventé: il s'agissait d'une simple ruse pour obtenir de l'argent.

Ce cas est révélateur des efforts de recherche que les escrocs sont disposés à faire avant de passer à l'acte. Pour échafauder leur scénario, il leur a fallu se pencher sur la structure organisationnelle de l'entreprise et bien l'analyser.

En juin 2013, MELANI a appris l'existence d'une autre attaque lancée contre une PME suisse. Un inconnu a cherché à s'introduire dans le réseau Intranet de cette société, implantée dans le canton de Zurich. L'escroc a contacté l'entreprise afin de parler à la comptabilité d'une prétendue facture ouverte. Comme son interlocutrice ne trouvait pas la facture dans le système, il a proposé de la numériser et de la lui envoyer par courriel. La collaboratrice a donné au cyberpirate son adresse électronique et a reçu quelques minutes plus tard un courriel muni d'un *hyperlien*. Or en cliquant sur ce lien, elle a obtenu non pas la facture attendue, mais un fichier Windows exécutable portant l'extension «.exe». Lors de son exécution, le fichier a discrètement installé sur son ordinateur un *RAT (Remote Administration Tool*, outil de télémaintenance). Ce programme permettait aux escrocs de contrôler par Internet la machine infectée, à l'insu de son utilisatrice légitime.

Par chance, la collaboratrice s'est méfiée et a signalé le courriel suspect à l'équipe de support informatique de l'entreprise. Cette dernière a confirmé l'infection de son ordinateur et l'a neutralisée. L'entreprise a porté plainte contre inconnu. Là encore, MELANI pense que les pirates avaient des visées financières.

Ce genre d'attaque ciblée, visant des entreprises suisses, est en augmentation au cours des dernières années. L'exemple montre qu'au-delà des grandes entreprises, les petites et moyennes entreprises sont également concernées. Les agresseurs poursuivent des objectifs variés. Le plus souvent, ils agissent par appât du gain (p. ex. fraude à l'e-banking) ou par intérêt commercial (recherche d'informations sur des concurrents et la structure de leur clientèle, espionnage industriel).

De telles attaques sont souvent menées à l'aide d'un *RAT* (*Remote Administration Tool*, outil de télémaintenance*)*. Il s'agit d'un maliciel pouvant être acheté en ligne pour quelques centaines de dollars et offrant une large palette de fonctions (de l'enregistrement des frappes du clavier au contrôle complet à distance). Les *RAT* sont généralement moins sophistiqués sur le plan technique que les chevaux de Troie servant à l'e-banking ou que d'autres maliciels. Néanmoins, de nombreux antivirus ne les reconnaissent pas, ou alors seulement trop tard.

## 3.5 Envoi de courriels munis d'un lien à des sites infectés

Un peu partout, des courriels invitent le destinataire à cliquer sur un objet. MELANI a déjà signalé, dans son dernier rapport semestriel[9], des courriels se référant à une facture ou une

[9] MELANI rapport semestriel 2012/2, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: 31 août 2013).

transaction fictive pour que le destinataire ouvre l'annexe. Or celle-ci contient toujours un maliciel, généralement placé dans un *fichier zip*, qui infecte l'ordinateur à son ouverture. Une tentative un peu différente a été observée le 22 janvier 2013. Un courriel rédigé en néerlandais émanait soi-disant d'une unité de l'administration cantonale argovienne. Si la victime cliquait sur le lien indiqué, sa machine était analysée à la recherche de failles pour y installer un maliciel. Le canton d'Argovie n'a pas été victime d'un piratage de ses infrastructures – des adresses «ag.ch» falsifiées ont simplement été utilisées pour l'envoi des courriels. Il est fréquent que des pirates indiquent comme expéditeur des noms d'entreprises ou de services étatiques familiers des gens.


**Betreff:** Informatie met betrekking tot uw NAT3799 belastingformulier

Houd er rekening mee dat je hebt fouten gemaakt bij het invullen van de laatste NAT3799 aangifte (ID: ).
Zie aanbevelingen en tips van onze fiscalisten Door hier te klikken
( Wacht 3 minuten tot rapport zal laden)

Alsjeblieft tot wijziging van de fouten en verzenden de herziene aangifte aan uw lokale belastingkantoor zo snel mogelijk.

Kanton Aargau

Fig. 5: Courriel muni d'un lien à une infection par *drive-by-download*.

On ignore pourquoi le courriel a été rédigé en néerlandais. Tout indique qu'il s'agit d'une erreur de l'auteur, qui a sérieusement compromis ainsi ses chances de succès. En outre, on voit mal ce qui a conduit à choisir un expéditeur dans l'administration cantonale argovienne. Il importe toutefois de répéter que la prudence s'impose avec les courriels non sollicités d'entreprises ou de collectivités publiques connues, dont les adresses peuvent être aisément falsifiées. Le fait que dans le cas précis, une lacune de sécurité des ordinateurs ait été exploitée pour propager l'infection montre l'importance d'actualiser régulièrement non seulement son système d'exploitation, mais toutes ses applications.

## 3.6 VoIP: abus en Suisse

VoIP (voice over IP) désigne la technologie permettant de téléphoner sur des réseaux IP à partir d'un réseau privé contrôlé, ou alors d'Internet. Ces dernières années, la téléphonie par VoIP et notamment via le réseau public Internet a connu une forte expansion chez les particuliers et dans les entreprises. Cet engouement tient notamment au prix avantageux des conversations internationales. Or les abus ont tendance à augmenter avec la diffusion croissante de cette technologie.

Au premier semestre 2013, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a été informée d'une escroquerie à grande échelle, où l'infrastructure d'une entreprise suisse, ou plus exactement un serveur virtuel détenu par cette société, avait été détourné pour une fraude consistant à lancer des appels sur des numéros fortement surtaxés (*VoIP Toll Fraud*). Une telle activité s'avère très lucrative pour le pirate, qui touche une commission versée par l'exploitant des services à valeur ajoutée.

Dans le cas d'espèce, le serveur virtuel avait été forcé pour mener à bien la fraude. Selon toute probabilité, les comptes se trouvant sur le serveur avaient aussi été piratés, et au final

les appels effectués depuis ces numéros payants ont été facturés aux propriétaires des comptes téléphoniques en question, soit des particuliers ou des entreprises.

Aujourd'hui, presque toutes les escroqueries faisant intervenir le téléphone utilisent la technologie VoIP. A commencer par le voice phishing (hameçonnage par téléphone), où la victime reçoit un appel destiné à lui soutirer ses données d'accès à l'e-banking. L'auteur de l'appel, qui se fait passer pour un expert en support informatique de Microsoft et allègue un problème de sécurité pour accéder à l'ordinateur de la personne appelée, tire parti de la technologie VoIP. D'où l'enjeu prioritaire d'en améliorer la sécurité. L'utilisation d'une infrastructure piratée comporte divers avantages pour les cybercriminels: ils peuvent non seulement téléphoner aux frais d'autrui, mais aussi mieux dissimuler leur identité. Outre ces escroqueries, d'autres risques d'abus de VoIP sont présentés au chapitre 5.7.

## 3.7 Vague de SMS de fraude à la commission

Tout un chacun s'est habitué aux *pourriels*, et les fournisseurs d'accès Internet cherchent à filtrer et écarter autant que possible les messages indésirables. En toute logique, ce type d'attaque devait tôt ou tard s'étendre au canal *SMS*. Il est vrai que jusqu'ici, l'envoi de SMS était trop compliqué pour les polluposteurs par rapport aux pourriels. Mais les choses semblent changer, comme en témoigne un incident survenu au premier semestre 2013.

En avril 2013, une vague de pourriels par SMS s'est abattue sur la Suisse. L'opération a touché plus de 500'000 clients de Swisscom, et de nombreux abonnés d'Orange et Sunrise. Le message avait apparemment été envoyé, au hasard, aux numéros faisant partie de certaines zones d'appel.

Dans le cas d'espèce, le SMS était un exemple typique de fraude à la commission. Les offres et promesses formulées dans de tels messages – ici un gain à la loterie – sont inventées de toutes pièces et ne visent qu'à planter un décor plus ou moins plausible pour que l'escroquerie aboutisse. Quiconque répond est prié de verser une avance sous un quelconque prétexte. L'argent promis ne lui parviendra toutefois jamais. En outre, les données personnelles communiquées (n° de passeport, photos, etc.) permettent aux bandits d'usurper l'identité de la victime pour commettre de nouvelles infractions.


Fig. 6: SMS envoyé lors d'une fraude à la commission

Les SMS avaient été expédiés par les opérateurs britanniques T-Mobile UK et Orange UK. Comme mesure immédiate, Swisscom a cessé d'acheminer temporairement les SMS de ces deux fournisseurs d'accès, jusqu'à ce qu'ils parviennent à neutraliser les pourriels sur leur réseau.

Le pollupostage est loin d'atteindre, sur le créneau des SMS, l'ampleur qu'il a prise dans la communication par courriel : selon les sources entre 70 %[10] et 85%[11] du trafic email est généré par le spam. Ce phénomène varie en outre fortement d'une région à l'autre. Ainsi, la technologie SMS est peu utilisée aux Etats-Unis. D'où un taux de pourriels inférieur à 1 % des SMS. En Asie, ce taux grimpe jusqu'à 30 %.[12] L'envoi de pourriels est plus compliqué par SMS que par courriel, ce qui a dissuadé jusqu'ici les polluposteurs. Toutefois l'essor des téléphones portables, et les possibilités toujours plus nombreuses de les pirater, auront une incidence sur le taux de pourriels envoyés par SMS.

Les possibilités de filtrer les pourriels transmis par SMS ne sont toutefois pas très avancées et reposent généralement sur des «listes noires», à la différence du filtrage des courriels en fonction de leur indice de pourriel (*spam score*).

## 3.8 Contrôle à distance d'écrans publicitaires

Une action particulière a eu lieu en juin 2013 à un office de poste de Zürich. Lors de cette dernière, des jeunes gens se sont dans un premier temps activés autour d'un écran publicitaire. La poste loue en effet à des sociétés marketing des espaces pour mettre en place des écrans publicitaires. L'exploitation et le support est dans ce cas assuré par la société qui loue l'espace.

Suite au démontage des éléments de sécurité physiques et au redémarrage de l'ordinateur relié à l'écran, un jeune homme de 17 ans a pu rapidement se connecter au système. Il a alors installé un outil lui permettant d'afficher du contenu pornographique sur l'écran à partir d'une source externe. Il souhaitait par cette action inhabituelle attirer l'attention sur une faille de sécurité. De par son écho dans la presse et à la télévision, sa démonstration a bénéficié d'une attention au niveau national.

Au-delà des questions juridiques soulevées par ce cas concret, sachant qu'il est illicite de rendre du matériel pornographique accessible aux mineurs, l'incident amène à s'interroger sur la meilleure façon d'agir lorsqu'on découvre une faille de sécurité. Il s'agit de déterminer dans quelle mesure une telle action sert réellement à sensibiliser les gens ou n'est qu'un moyen pour son auteur de se distinguer, et s'il ne serait pas plus efficace, en pareil cas, d'informer directement le service concerné.

L'argent est un stimulant toujours plus puissant dans la détection des lacunes de sécurité. Le marché de la sécurité (Security Business) est très disputé. D'où la présence d'entreprises qui se sont spécialisées dans la recherche des failles de sécurité pour les revendre aux fabricants concernés. La découverte et la publication de lacunes de sécurité s'avèrent aussi un argument publicitaire pour montrer le professionnalisme de sa propre entreprise.

---

[10] http://www.spamfighter.com/News-18508-Spam-Increases-to-707-of-Total-E-mail-Traffic.htm (état: 31 août 2013).

[11] http://senderbase.org/static/spam#tab=1 (état: 31 août 2013).

[12] http://en.wikipedia.org/wiki/Mobile_phone_spam (état: 31 août 2013).

## 3.9 Swiss Cyber Storm et les «cyber-talents» de demain

Le 13 juin 2013, le KKL de Lucerne a accueilli Swiss Cyber Storm 4. Les orateurs de cette conférence, sommités internationales dans leur domaine d'activité, se sont adressés aux décideurs de l'économie suisse.

Il s'agissait par ailleurs de repérer les meilleurs «cyber-talents» suisses. Dans les semaines précédant la journée du congrès, des étudiants et élèves ont eu l'occasion de participer en ligne à des «challenges». Chacun était invité à résoudre des «cyber» -problèmes ou -énigmes. Or au-delà des simples hackers, les épreuves étaient conçues pour révéler les talents capables d'élaborer une véritable réflexion et une approche globale. Concrètement, il ne suffisait pas de savoir comment accéder à un fichier zip crypté. Les candidats devaient aussi indiquer quelle faille de sécurité leur avait permis d'y parvenir et comment la corriger. Autrement dit, l'intrusion n'était pas une fin en soi. Il était tout aussi important de montrer comment protéger ses propres systèmes.

Les attentes envers les participants étaient nombreuses. Par exemple, il leur fallait résoudre le défi technique soumis dans un délai donné, ce qui créait une pression supplémentaire. A cet effet, il était important de savoir sortir des sentiers battus, de faire preuve de souplesse et d'avoir un esprit d'équipe, axé sur la recherche de solutions concrètes.

Le Swiss Cyber Storm a été enrichissant pour tous les participants, qui ont pu élargir leurs connaissances et nouer d'utiles contacts avec le secteur privé. L'un d'eux a déjà reçu une proposition concrète d'emploi.

Qu'est-ce qui suivra le Swiss Cyber Storm?

Le groupe lauréat ne peut pas se reposer sur ses lauriers. Les organisateurs du Swiss Cyber Storm l'ont en effet invité à disputer, en novembre 2013, la finale contre l'équipe gagnante de la conférence similaire organisée à Linz.[13]

MELANI parraine la manifestation avec Swiss Police ICT, association privée qui, avec le congrès informatique de la police suisse, établit depuis des années des liens entre le monde de l'informatique et les autorités de poursuite. Le but commun est de repérer à chaque fois de nouveaux «cyber-talents» suisses.

# 4 Situation internationale de l'infrastructure TIC

## 4.1 Surveillance des communications sur Internet

Les médias ont abondamment parlé, au semestre écoulé, des méthodes d'écoute utilisées par quelques services de renseignement et rendues publiques par l'informateur Edward Snowden. Les premières révélations concernaient Prism, programme de surveillance de la NSA. Il y a eu ensuite la publication des possibilités dont dispose en Grande-Bretagne le Government Communications Headquarters (GCHQ) de se brancher sur les câbles sous-

[13] http://www.verbotengut.at/ (état: 31 août 2013).

marins transatlantiques, puis la diffusion d'une présentation du programme d'analyse XKeyscore. Snowden était employé de la CIA, avant de passer auprès du prestataire de sécurité Booz Allen Hamilton, qui travaille notamment sur mandat de la NSA.[14] Ces révélations ont abouti à un vaste débat, dans divers autres pays, sur les programmes de surveillance en place.

### Prism

Prism est le nom d'un programme de surveillance conçu par la NSA et rendu public par Edward Snowden. Son nom est dû à sa capacité de séparer au moyen d'un prisme, en les déviant de leur trajectoire, les signaux circulant dans les câbles en fibre optique. On peut toutefois douter que des données soient collectées au passage. Ce programme serait plutôt un projet permettant à la NSA d'accéder aux serveurs de différentes sociétés américaines, comme Microsoft, Google ou Yahoo.

Il n'y a rien d'exceptionnel à ce que des services étatiques accèdent aux infrastructures de télécommunication présentes sur leur territoire. De tels accès font en général l'objet d'une réglementation stricte: ils requièrent typiquement une procédure pénale et une décision judiciaire ou des motifs particuliers, prévus dans une loi spéciale. La nouveauté, c'est que les services de renseignement américains bénéficieraient d'un accès non plus ponctuel, mais systématique à ces données, sur tout leur territoire. Toutes les sociétés concernées ont nié l'existence d'une collaboration aussi étroite, en faisant valoir que les données ne sont livrées qu'après une décision judiciaire portant sur des comptes spécifiques.

Selon la position officielle, maintes fois répétée, toutes les mises en écoute avaient une base légale et avaient obtenu l'aval des trois pouvoirs américains. Le «Foreign Intelligence Surveillance Act (FISA)», loi édictée en 1978, réglemente la surveillance à l'étranger, celle des personnes étrangères sur sol américain ainsi que celle des citoyens américains. La Foreign Intelligence Surveillance Court (FISC) adopte, en tant que cour de justice, les mesures de surveillance correspondantes. Les amendements apportés au FISA par des actes législatifs comme le «Patriot Act» (2001) ou le «Protect America Act» (2007) ont conféré aux autorités des compétences étendues de surveillance des communications, compte tenu de l'évolution de la menace – terroriste notamment – et des progrès techniques, comme l'essor d'Internet ou l'acheminement des communications internationales par câble en fibre optique en lieu et place de satellites.

### Tempora

Un autre rapport communiqué par Snowden au quotidien britannique «The Guardian» concerne un programme du nom de Tempora, mis en place par le service de renseignement britannique. Ce programme d'écoute permettrait au British Governement Communications Headquarter (GCHQ) d'accéder aux liaisons transatlantiques et, à partir de là, de dévier les données souhaitées pour les copier. Le rapport divulgué portait sur la ligne TAT-14, menant d'Allemagne, du Danemark, des Pays-Bas et de France au New Jersey via la Grande-Bretagne. Le GCHQ y aurait accès dans la localité portuaire de Bude, point d'atterrissement du câble. Les données espionnées comprendraient des courriels, des entrées Facebook et

[14] Le présent rapport couvre la période allant de janvier à juin 2013. Les autres informations rendues publiques à propos de l'informateur Edward Snowden figureront dans le prochain rapport semestriel.

des conversations téléphoniques. Le GCHQ espionnerait plus de 200 liaisons par fibre optique et affecterait 500 collaborateurs à l'analyse des données recueillies.[15]

Ces dernières années, le trafic Internet transatlantique s'est progressivement reporté sur les câbles en fibre optique sous-marins. Alors qu'en 1986 jusqu'à 80 % des échanges transatlantiques s'effectuaient par satellite, la majeure partie des données sont aujourd'hui acheminées, au niveau tant continental qu'intercontinental, par le réseau de fibre optique. Il existe généralement plusieurs voies possibles pour la communication entre deux utilisateurs. Ce n'est qu'au stade de l'acheminement concret qu'intervient la décision. A supposer même que le trafic des données empruntant un câble sous-marin soit espionné, cela ne signifie pas pour autant que toute la communication, autrement dit la totalité du contenu d'un courriel, puisse être interceptée, même si c'est souvent le cas dans la pratique.

**XKeyscore**

XKeyscore est un logiciel d'analyse développé par la NSA et qui serait utilisé conjointement par différents services de renseignement. Il permettrait de collecter en temps réel, dans diverses banques de données, quantité de données (courriels, discussions en ligne, etc.) provenant d'une personne mise sous surveillance. Les requêtes feraient appel à toutes sortes de critères, comme l'*adresse IP*, la langue, le navigateur, les réglages et les numéros de téléphone. D'où la possibilité de récolter toutes les données enregistrées dans ce contexte. Selon la présentation confidentielle de 2008 publiée par Snowden, le réseau XKeyscore comprendrait plus de 700 serveurs, déployés sur 150 sites dans le monde entier. Les services de renseignement étrangers du Royaume-Uni, du Canada, d'Australie et de Nouvelle-Zélande participeraient aux opérations de XKeyscore. L'agence de renseignement allemande (BND) se servirait elle aussi activement du programme. [16]

Il n'est guère étonnant que des services de renseignement disposent d'outils adéquats, leur permettant d'analyser efficacement des données déjà collectées. A l'heure actuelle, l'examen d'une telle masse de données requiert des programmes d'analyse adéquats. Tout un chacun en connaît le mode de fonctionnement, grâce aux moteurs de recherche: là aussi, il est crucial d'obtenir en une fraction de seconde les résultats souhaités. Qui a accès à quel moment à quelles données d'un tel système? La vraie question n'est pas tant la manière dont un service de renseignement analyse les données que le genre de données qu'un service de renseignement est autorisé à collecter et à enregistrer, soit les requêtes concrètes admissibles dans la masse de données à disposition.

## 4.2 Advanced Persistent Threats: Red October, Net Traveller, MiniDuke

Plusieurs cyberattaques raffinées visant des entreprises ou des services étatiques ont été signalées au premier semestre 2013. Elles font généralement partie de la catégorie de menace *Advanced Persistent Threat*. Les APT se caractérisent par le fait que les pirates cherchent patiemment, par tous les moyens, à accéder à certains systèmes pour s'y incruster

[15] http://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaeht-daten-aus/8391120.html (état: 31 août 2013).

[16] http://www.zeit.de/politik/deutschland/2013-08/bnd-xkeyscore-nsa (état: 31 août 2013).

durablement et y déployer discrètement leurs activités malveillantes. Bien souvent, l'infection d'origine provient d'attaques de type *Spear Phishing* ou *Watering Hole*. Des portes dérobées (backdoors) sont installées et les droits d'administrateur obtenus frauduleusement. Le but final est d'accéder le plus longtemps possible au réseau sans se faire repérer, d'y espionner les données et, le cas échéant, de les modifier ou de les effacer. Comme de telles attaques mobilisent d'importantes ressources, les soupçons se portent souvent sur des acteurs étatiques. Elles pourraient tout aussi bien provenir d'organisations criminelles ou d'individus ayant beaucoup de temps à disposition, très motivés et pensant pouvoir revendre à des tiers les données ainsi collectées.

L'entreprise de sécurité informatique FireEye estime dans son rapport sur les menaces APT que toutes les trois minutes, des entreprises ou des organisations reçoivent un courriel muni d'un lien ou une annexe susceptibles de les infecter.[17] En Suisse aussi, les systèmes renfermant des informations sensibles sont exposés au quotidien à ce genre d'attaques.

Les annonces concernant ce genre de cyberattaques se sont succédé rapidement au premier semestre 2013. Et comme la plupart du temps les soupçons se portaient sur des acteurs étatiques, elles ont été suivies de nombreuses prises de position politiques.

### Janvier: Operation Red October

Le 14 janvier 2013, la société informatique russe Kaspersky a publié des détails sur une opération d'espionnage visant des missions diplomatiques, des gouvernements et des organisations internationales. Les cibles de l'opération appelée Red October se situaient surtout en Europe orientale, en Asie centrale et dans les républiques de l'ex-URSS. Le rapport de Kaspersky indiquait que l'accès à l'*infrastructure du serveur Command & Control* se faisait à partir de nombreuses adresses IP suisses, ce qui a d'abord fait croire que de nombreuses victimes se trouvaient en Suisse. Or MELANI a constaté, lors d'une première analyse, qu'il s'agissait le plus souvent d'adresses IP dynamiques. Une fois éliminés les cas suspects comptés plusieurs fois, le nombre d'infections effectives a pu être ramené à cinq victimes. En outre, il ne s'agissait pas d'organisations suisses, mais d'infrastructures étrangères exploitées en Suisse.

Les victimes avaient été infectées par des maliciels figurant en annexe de courriels. Ces attaques avaient pour particularité de ne pas dérober seulement les données d'ordinateurs infectés, mais aussi celles d'appareils mobiles. Cette opération d'espionnage aurait débuté en 2007, voire plus tôt. Selon Kaspersky, l'agresseur serait russophone.

### Février: APT1

Les attaques visant des entreprises américaines ont augmenté en début d'année. La vague a conduit de nombreux politiciens en vue aux Etats-Unis à plaider pour un renforcement des activités de défense et à montrer du doigt la Chine, d'où proviendraient les plus grands risques en matière de cyberespionnage.

En dépit de la diversité des attaques et des cibles, le schéma est partout le même. Les victimes étaient principalement de grandes entreprises Internet américaines comme Apple, Fa-

[17] http://www2.fireeye.com/WEB2012ATR2H_advanced-threat-report-2h2012.html (état: 31 août 2013).

cebook, Google, Microsoft ou Twitter. Leurs systèmes ont subi des attaques de type *Watering Hole*, sur un site destiné aux développeurs d'applications mobiles. Les visiteurs de cette page ont été infectés par un *0-day-exploit* du programme *Java*. En parallèle, de nombreux grands médias américains (New York Times, Wall Street Journal, Bloomberg, Washington Post) ont aussi déploré des attaques visant les comptes de messagerie de leurs journalistes. Dans les deux cas, les agressions ont été attribuées à la Chine.

Dans ce contexte est paru en février 2013 un rapport de l'entreprise de sécurité américaine Mandiant, prétendant pouvoir démontrer que l'Etat chinois serait impliqué dans les opérations de cyberespionnage dont les Etats-Unis et plusieurs Etats européens ont fait les frais. Il est le fruit de recherches menées conjointement avec les sociétés piratées. Ce rapport conclut notamment à l'existence d'un lien entre un groupe de cybercriminels appelé APT1 et une unité de l'armée chinoise. Mandiant explique que depuis 2006, ce groupe aurait subtilisé au fil des ans quantité de données aux 146 victimes étudiées.

Là encore, la Suisse n'était qu'indirectement concernée, puisque les systèmes touchés consistaient en infrastructures étrangères exploitées sur son sol.

**Février: Operation Beebus**

Dans le même contexte politique, la société américaine FireEye a publié en février 2013 les résultats de ses recherches sur une autre affaire d'espionnage, une APT du nom de Beebus. Elle visait en apparence surtout des entreprises du secteur défense et aéronautique. L'attaque a recouru aussi bien à l'envoi ciblé de courriels qu'à des infections par *drive-by-download*. Les premières traces remontent selon FireEye à 2011. FireEye pense que l'opération, qui a épargné la Suisse, pourrait être d'origine chinoise.

**Février: MiniDuke**

Toujours en février 2013, Kaspersky a révélé une attaque sophistiquée basée sur le maliciel MiniDuke. Elle s'est apparemment concentrée sur des structures étatiques et sur quelques autres objectifs situés en Europe exclusivement. Les victimes ont été infectées par des documents PDF spécialement préparés et annexés à des courriels qui semblaient émaner de personnes connues d'elles (*Spear Phishing*). L'attaque avait pour particularité d'utiliser des comptes Twitter pour générer les *noms de domaine des serveurs Command & Control*. Selon l'état actuel des connaissances, aucune infrastructure touchée ne se trouve en Suisse.

**Juin: NetTraveler**

Au début de juin 2013, Kaspersky a publié des informations détaillées sur NetTraveler, famille de maliciels utilisés pour des attaques APT. 350 victimes ont été recensées dans 40 pays mais, là non plus, il n'existe aucun lien selon l'état actuel des connaissances avec les infrastructures suisses. Les cibles étaient des sociétés actives dans l'industrie, la production d'énergie, les télécommunications et les nouvelles technologies, ou alors des entités gouvernementales. Toujours selon Kaspersky, six victimes auraient été infectées simultanément par NetTraveler et Red October. On ne peut toutefois en conclure ni que les deux attaques avaient un seul et même auteur, ni qu'elles émanaient d'auteurs différents.

Les nombreux comptes rendus d'entreprises de sécurité, de victimes ou d'autorités ont remis sous les feux de la rampe le cyberespionnage et les attaques APT. Or depuis longtemps, ces agressions ciblées ont cessé d'être des événements isolés ou des opérations ponctuelles d'espionnage. Les données sensibles suscitent un intérêt qui ne se relâche pas et sont soumises à des pressions permanentes. La Suisse est d'autant plus concernée qu'elle

abrite de nombreuses entreprises de pointe, dont le savoir-faire et les connaissances ont une valeur inestimable. Outre les précautions techniques d'usage, des mesures d'organisation s'imposent. Indépendamment des incidents récents, la prévention s'avère en effet toujours prioritaire et passe par la sensibilisation des collaborateurs. D'où la nécessité de les former notamment à une utilisation prudente de la messagerie électronique.

Il est rare de pouvoir remonter jusqu'à l'auteur d'une cyberattaque. Même si une localisation géographique précise est parfois possible, il est rarissime de pouvoir démontrer de manière indubitable que l'Etat d'où provient l'agression en porte la responsabilité.

Notons encore que les infrastructures utilisées pour certaines de ces attaques sont connues pour leurs antécédents criminels. Autrement dit, les infrastructures criminelles ne poursuivent apparemment pas qu'un dessein d'enrichissement, mais sont aussi à la solde d'Etats ayant des visées d'espionnage.

## 4.3 Cyberconflit entre les deux Corées

Le conflit entre les deux Corées s'est envenimé au premier semestre 2013. Des indices d'essais nucléaires nord-coréens[18] ayant abouti à un durcissement des sanctions des Nations Unies, la Corée du Nord a annoncé qu'elle était désormais en guerre contre la Corée du Sud et menacé, pour la première fois, les Etats-Unis d'y mener une frappe nucléaire préventive. Ce foyer de conflit a également eu une composante cybernétique. Le 14 mars 2013, l'agence de presse officielle nord-coréenne KCNA a signalé une panne locale d'Internet, due à une cyberattaque hostile. Les Etats-Unis et la Corée du Sud ont été accusés d'avoir provoqué cette panne. On n'en sait pas davantage, et d'ailleurs seule une faible partie de la population nord-coréenne a accès à Internet. Une semaine plus tard, le 20 mars 2013, la Corée du Sud a subi une cyberattaque massive, qui a touché trois chaînes télévisées et deux établissements financiers. Les victimes n'ont plus pu démarrer leur ordinateur, le maliciel ayant effacé leur disque dur. Alors que les bancomats, les terminaux de points de vente (*points of sale*) et les activités de banque mobile (*Mobile Banking*) des établissements touchés étaient en partie hors service, les chaînes attaquées ont diffusé normalement leurs programmes. En outre, des défigurations de sites ont été commises par un groupe baptisé «Whois Team», qui a signalé au passage qu'il ne s'arrêterait pas là. «Les données sont en nos mains et ont disparu des ordinateurs concernés.» Aussi un groupe nommée «New Romanic Cyber Army» a affirmé être responsable de l'attaque et d'avoir soutiré des informations à partir de banques et groupes médiatiques. McAfee a publié dans un rapport que ces attaques étaient liées à une opération d'espionnage, méconnue mais active depuis 2009, contre l'armée sud-coréenne. Cette opération, nommée "Operation Troy", avait le but de rechercher des informations dans des ordinateurs de l'armée selon des mots clés bien précis.[19] Les actions d'hacktivisme peuvent donc bien cacher des opération d'espionnage.

Une autre opération a été menée le 25 juin 2013, 63$^{e}$ anniversaire du début de la guerre de Corée – cette fois sous forme d'attaque DDoS contre des *serveurs DNS* du gouvernement sud-coréen. Des sites officiels, dont celui de la présidence, ont été paralysés. Des représentants du mouvement Anonymous, mentionné comme auteur sur plusieurs sites, se sont dis-

[18] http://www.seismologie.bgr.de/sdac/erdbeben/kernexplosion/nkorea_20130212_deu.html (état: 31 août 2013).

[19] http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea (état: 31 août 2013).

tanciés de l'agression. La Corée du Sud a accusé son voisin du Nord d'avoir organisé les attaques de mars comme celles de juin. Des adresses IP nord-coréennes et des échantillons de maliciels ont été produits comme pièces à conviction.[20]

Après cette dernière agression, Symantec a aussi publié un rapport[21] rapprochant, sur la base d'indices clairs, une des *attaques DDoS* du 25 juin 2013 des attaques lancées depuis quatre ans contre la Corée du Sud, y c. celles de juillet 2009 et mars 2011[22], pour l'attribuer au groupe «DarkSeoul». Symantec pense à un collectif de 10 à 50 personnes qui, selon son rapport, aurait aussi diffusé le *maliciel* d'e-banking Castov. Le groupe s'en serait déjà aussi pris à des cibles états-uniennes. Mais expérience à l'appui, il est très difficile d'identifier l'origine des attaques pour pouvoir les attribuer, le cas échéant, à un acteur étatique.

## 4.4 Piratage du compte Twitter d'Associated Press

Les pirates informatiques s'en sont davantage pris au réseau social Twitter au premier semestre 2013. Le plus grave incident est survenu le 23 avril 2013, où le compte Twitter d'Associated Press (AP) a été compromis. Des «hackers» s'étaient procuré un accès au compte Twitter de l'agence de presse AP et ont envoyé en son nom un tweet annonçant qu'une explosion avait eu lieu à la Maison Blanche et que le Président Obama était blessé. Près de deux millions d'abonnés ont suivi ce tweet. Les marchés américains ont instantanément plongé. En trois minutes, l'indice américain S&P a perdu l'équivalent de 136,5 milliards de dollars de capitalisation, avant que tout rentre dans l'ordre. De même, des comptes Twitter de la BBC, de CBS, de France 24, d'Al Jazeera et de la National Public Radio (NPR) ont été piratés. Quant au quotidien britannique «The Guardian», il a subi une telle mésaventure le 29 avril 2013, où il a diffusé des slogans anti-israéliens et des textes comme «Long Live Syria» ou «Syrian Electronic Army was here». On trouve encore sur la liste des victimes la FIFA et son président. Son compte a envoyé un faux message, annonçant que Joseph Blatter démissionnait de son poste suite à des reproches de corruption, selon lesquels il aurait accepté de l'argent de l'émir du Qatar dans la course à l'attribution de la CM 2022.

Ces attaques seraient dues au groupe «Syrian Electronic Army (SEA)», qui vise à créer «chaos et confusion». Il va de soi que la SEA a cherché ainsi à se faire mieux connaître. Elle a accusé de son côté les médias occidentaux de répandre «mensonges et calomnie sur la Syrie».

La méthode est toujours la même: les pirates envoient aux détenteurs d'un compte Twitter des courriels plausibles, munis d'un lien à un site infecté. Aussitôt installé, le maliciel subtilise le nom d'utilisateur et le mot de passe, grâce auxquels l'agresseur pourra se connecter et diffuser ses propres messages.

---

[20] http://www.csoonline.com/article/736531/south-korea-blames-north-korea-for-cyberattacks (état: 31 août 2013).

[21] http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war (état: 31 août 2013).

[22] MELANI rapport semestriel 2009/2, chapitre 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=fr (état: 31 août 2013).

Les médias sociaux exercent une influence grandissante sur la diffusion de l'information. La concurrence entre médias fait en outre qu'il reste toujours moins de temps pour vérifier une nouvelle, a fortiori lorsqu'elle paraît émaner d'une source renommée. On a trop tendance à oublier que les comptes Twitter ne sont protégés que par un nom d'utilisateur et un mot de passe. Or il suffit d'une attaque ciblée, menée par les méthodes usuelles de *phishing* ou à l'aide de *maliciels*, pour accéder aux mots de passe. Twitter a donc prévenu la branche des médias que de tels incidents pourraient se reproduire, aux dépens notamment de médias en vue et populaires. Afin de limiter le risque d'infection par maliciel, Twitter recommande de ne pas se limiter aux mesures d'usage mais d'utiliser un ordinateur séparé pour composer des tweets. En outre, Twitter songe à des mesures techniques et préparerait l'introduction d'une *authentification à deux facteurs*, comme on en trouve déjà p. ex. dans l'e-banking.[23]

Des fausses nouvelles peuvent aussi être envoyées par Twitter même sans qu'un compte ait été compromis, comme l'a montré en novembre 2011 la mésaventure d'Andrea Caroni. Alors même que le conseiller national Caroni n'avait pas de compte Twitter, un compte truqué créé à son nom a confirmé la réélection de la conseillère fédérale Eveline Widmer-Schlumpf avant même l'annonce du résultat officiel.[24]

Outre toutes ces mesures techniques, il faudrait aussi étudier et préciser en amont comment et par quels canaux on pourrait démentir ou rectifier une fausse rumeur de la manière la plus rationnelle, afin d'éviter que la confusion ne s'installe avec son cortège de désagréments.

## 4.5 Systèmes SCADA et SCI: accès non protégés, failles de sécurité, attaques et protection

Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. L'expression «systèmes de contrôle industriels» (en angl. Industrial Control Systems, ICS) est entrée dans le langage courant. Or depuis quelque temps, les systèmes de contrôle-commande industriels trouvent de nouveaux débouchés en dehors de l'industrie productive, p. ex. dans la domotique ou la gestion du trafic. On peut dès lors parler de SCI à propos de tout système de contrôle qui règle et/ou surveille un processus physique. De même, la plupart des règles de base destinées à protéger de tels systèmes s'appliquent aussi en dehors de la production industrielle.

### Serveurs de port série non protégés dans Internet

Les *serveurs de port série* relient les *interfaces* série des appareils à un réseau de télécommunication. Il est possible d'y accéder sans grande difficulté via Internet dans 10 % des cas, selon des recherches effectuées par l'expert en sécurité HD Moore[25] sur plus de 100 000 serveurs de ce type. Il a ainsi identifié diverses installations dont les accès ouverts

[23] http://www.zdnet.de/88155870/twitter-fuhrt-zwei-faktor-authentifizierung-ein/?ModPagespeed=noscript (état: 31 août 2013).

[24] MELANI rapport semestriel 2011/2, chapitre 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=fr (état: 31 août 2013).

[25] https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers (état: 31 août 2013).

offraient un réel potentiel d'abus – des SCI des chaudières d'une brasserie aux compteurs intelligents (*Smart Meter*) et aux systèmes de gestion des feux de circulation, en passant par les serveurs *VPN* d'entreprises.

Bien des appareils pouvant être commandés par une interface série ne prévoient pas d'authentification supplémentaire. Lorsqu'une liaison physique est établie par l'interface série (ce qui dans le passé se faisait toujours au niveau local), ils considèrent que la personne connectée bénéficie de droits d'accès comme de configuration. D'où la nécessité d'en tenir compte lors de l'installation ultérieure d'accès à distance. Ainsi, de tels accès seront toujours protégés contre les abus. A cet effet, il est possible d'utiliser des tunnels VPN et/ou de restreindre l'accès à quelques adresses IP connues. En outre, il faut s'assurer que l'accès soit crypté et prévoir des mots de passe robustes ou une *authentification à 2 facteurs*.

### Faille de sécurité dans des modules de pilotage: mots de passe déchiffrables

La chaudière à gaz compacte «ecoPower 1.0» est un système de couplage chaleur-force doté d'une technologie de moteur à gaz à usage privé, mis au point par l'entreprise Valliant. Elle produit simultanément de la chaleur et de l'électricité, que le propriétaire peut soit utiliser lui-même, soit réinjecter dans le réseau public. Le pilotage de l'installation s'effectue par un écran tactile intégré, par une *app* iPad ou encore par une *interface Web*. Or certains mécanismes de sécurité n'ont pas été conçus de manière optimale, voire ont été négligés lors de l'introduction du réglage à distance par Internet. C'est ainsi qu'une faille de sécurité permet d'obtenir tous les mots de passe. Outre le mot de passe de configuration du propriétaire, le système livrait en toutes lettres les mots de passe servant à la maintenance à distance et même ceux du développeur du système. Ce qui a permis à des tiers non autorisés d'accéder à la microcentrale, de déchiffrer les données concernant son propriétaire et de modifier les paramètres d'exploitation. Il a fallu que l'exploitant d'un tel appareil contacte des experts en sécurité[26] et que ceux-ci étudient la question, pour que le fabricant apprenne que son produit laissait à désirer. Il a par la suite recommandé par lettre aux clients concernés de débrancher le câble réseau des chaudières, en attendant que des solutions soient trouvées et qu'un technicien de service règle les problèmes sur place.

Valliant a beau avoir ignoré toutes les recommandations de sécurité en raccordant ses produits directement à Internet – et non via un tunnel *VPN* crypté –, Saia-Burgess devrait aussi s'occuper du problème. Car c'est ce fabricant suisse de modules de pilotage qui est responsable de l'enregistrement en toutes lettres des mots de passe ainsi que de la faille de sécurité qui a permis de les découvrir. Les modules de pilotage en cause ne sont d'ailleurs pas uniquement utilisés par Valliant pour ses chaudières, mais apparaissent aussi dans diverses installations parfois de grande taille et revêtant une grande importance.

Tant Valliant que Saia-Burgess sont en train[27] de combler les lacunes et ont publié les mises à jour correspondantes[28]. Vaillant s'est en outre doté d'un service d'assistance téléphonique pour les clients concernés et a installé chez eux des mises à jour et un routeur *VPN* garan-

---

[26] http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheitslucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/; http://heise.de/-1840919 (état: 31 août 2013).

[27] http://www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.html (état: 31 août 2013).

[28] Mise à jour du logiciel de Saia: http://www.sbc-support.com/de/product-index/firmware-for-pcd-cosinus.html (état: 31 août 2013).

tissant un accès sécurisé. Il faudra toutefois encore un peu de temps jusqu'à ce que les mises à jour et les mesures de sécurité additionnelles soient dûment en place dans tous les systèmes concernés.

Ce cas montre de manière exemplaire la problématique à laquelle est confrontée dans son développement une société toujours plus interconnectée (par un seul et même réseau). L'accès à distance à un appareil a beau offrir de nouvelles possibilités et de réels avantages tant au propriétaire, pour son usage, qu'au technicien de service pour son entretien, il prête également le flanc à des cyberattaques, avec les risques qui s'ensuivent. D'où l'importance qu'en plus de réfléchir à la convivialité des nouveaux appareils, toutes les entreprises faisant partie de la chaîne logistique d'un produit définissent aussi des exigences en matière de sécurité, à prendre en compte dès le processus de développement. Car la sécurité est une tâche commune. Même si le fabricant du module de pilotage recommande (au plus tard depuis l'incident décrit ci-dessus, en termes précis et fermes) de ne pas raccorder ses appareils directement à Internet – cela ne le dispense pas du devoir d'y intégrer des mécanismes de sécurité et, le cas échéant, de livrer en temps utile les mises à jour requises.

Les SCI étaient déjà en partie raccordés au réseau de télécommunications avant l'ère d'Internet – généralement par leur propre ligne téléphonique. En cas de besoin, seul le fabricant/fournisseur pouvait s'y connecter à des fins de diagnostic ou de service, pour éviter de devoir se rendre sur place. Depuis que l'accès se fait par Internet, il faut prendre en compte les spécificités de ce média. Le risque qu'un inconnu apprenne le numéro de téléphone d'une installation, qu'il découvre son éventuel mot de passe et, enfin, qu'il en comprenne le protocole propriétaire est sans doute moindre que le risque de voir quelqu'un découvrir dans Internet une installation à l'aide d'un moteur de recherche spécialisé[29], puis analyser les failles de sécurité de son serveur Web à l'aide d'outils standard. S'il s'avère nécessaire d'administrer à distance de tels systèmes, on pourra le faire p. ex. via des tunnels VPN cryptés, prévoyant une authentification forte.

Le battage autour de la vulnérabilité des systèmes de commande a eu un effet positif: la branche s'intéresse désormais davantage aux questions de sécurité.

### Attaque de systèmes de contrôle industriels (SCI)

Kyle Wilhoit, chercheur de la société Trendmicro, a examiné sur une longue période les attaques lancées contre les SCI à l'aide de pots de miel (*honeypot*)[30]. Il a ainsi constaté que les SCI font en permanence l'objet de cyberattaques automatisées ou semi-automatiques.

Les recherches ont abouti aux résultats suivants:

- En cinq mois, plus de 16 000 attaques automatisées ont été lancées à partir de 605 *adresses IP* différentes. Et encore ce chiffre ne tenait pas compte des cyberattaques visant d'autres cibles que les SCI.

- Les attaques suivantes ont notamment été constatées:

---

[29] Voir p. ex. le moteur de recherche Shodan: http://www.shodanhq.com (état: 31 août 2013).

[30] Trendmicro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf et Blackhat: https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf (état: 31 août 2013).

- tentative d'accès aux pages de diagnostic des systèmes simulés;
- tentative d'accès et de modification des protocoles *Modbus* / *DNP3*;
- tentatives de modifier le système (factice) de pompage;
- tentatives d'accès aux domaines protégés;
- accès non autorisés en lecture et en écriture aux *API* (PLC).[31]

- Des attaques ciblées, par maliciel, ont été constatées contre une adresse électronique publiée par le pot de miel. L'agresseur a cherché de cette manière à s'emparer de données utiles à de futures attaques (informations sur les configurations *VPN*, paramètres du réseau et banque de données des mots de passe Windows).

Il ressort de l'analyse de Kyle Wilhoit que les SCI raccordés à Internet subissent souvent des cyberattaques, qu'ils fassent ou non partie d'une installation connue et particulièrement exposée. Les SCI ne devraient donc en aucun cas être directement reliés au réseau, sans mécanismes de protection supplémentaires.

## Comment protéger les systèmes de contrôle industriels (SCI)?

SANS[32], institut américain spécialisé dans la sécurité, a publié 20 éléments-clés[33] indiquant comment protéger son infrastructure informatique. Ces éléments valent en partie aussi pour les SCI. D'autres recommandations ont été émises par l'US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[34]), ainsi que par le National Institute of Standards and Technology (NIST[35]).

Les onze recommandations de sécurité suivantes se basent sur ces documents. Des explications plus détaillées figurent sur le site MELANI[36].

1. Créer et actualiser une banque de données des actifs pour tous les appareils ;
2. Etablir le cycle de vie des logiciels, avec la gestion des correctifs;
3. Définir et utiliser des configurations sûres;
4. Planifier et réaliser des architectures réseau robustes;
5. Mettre en place une protection à plusieurs niveaux contre les maliciels;
6. Authentification et autorisation;
7. Procéder à une analyse centrale des fichiers journaux (logs);
8. Garantir la protection physique;
9. Effectuer et tester régulièrement les sauvegardes et possibilités de récupération;

---

31 API signifie automate programmable industriel et désigne un dispositif destiné à la commande d'installations. Le terme anglais équivalent est PLC (programmable logic controller).

32 SANS, http://www.sans.org (état: 31 août 2013).

33 SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/ (état: 31 août 2013).

34 ICS CERT: http://ics-cert.us-cert.gov/ (état: 31 août 2013).

35 NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (état: 31 août 2013).

36 Listes de contrôle et instructions: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=fr (état: 31 août 2013).

10. Etablir et exercer des processus de gestion des incidents de sécurité;
11. Instaurer une culture de la sécurité.

Il est important de comprendre que dans la plupart des cas, la sécurité ne saurait être garantie du jour au lendemain par une action unique, et que les améliorations constituent un processus continu, qui ne s'arrête jamais. Il est par conséquent judicieux de se fixer des objectifs réalistes et atteignables, et de régler d'abord les points permettant d'améliorer sensiblement la sécurité à peu de frais, p. ex. en changeant tous les mots de passe par défaut et en protégeant les interfaces de commande accessibles de l'extérieur.

Alors que les systèmes informatiques classiques mettent l'accent, outre la disponibilité, sur la confidentialité et l'intégrité, la disponibilité est jugée absolument prioritaire dans les SCI. Or la protection de la confidentialité et de l'intégrité est également un gage de disponibilité. En effet, un système communiquant par un protocole qui préserve la confidentialité et l'intégrité des données sera mieux protégé contre les attaques menées par le réseau et affichera une disponibilité plus élevée.

## 4.6 Pannes logicielles et conséquences

### Erreurs du système de réservation – annulation de nombreux vols d'American Airlines

Le 16 avril 2013 au matin, une erreur informatique apparue dans le système de réservation d'American Airlines a provoqué une panne géante. Aucun passager n'a pu être enregistré sur un vol pendant plusieurs heures. Ce n'est que l'après-midi que les systèmes ont refonctionné. Au total, 700 vols ont été annulés, et davantage encore retardés. La compagnie aérienne américaine organise chaque jour 3400 vols[37]. En l'occurrence, la cause de la panne n'a pas été rendue publique.

Cet exemple montre que lorsqu'une infrastructure vitale tombe en panne, les systèmes SCADA et les systèmes de contrôle industriels ne sont pas toujours en cause. De graves problèmes sont aussi susceptibles d'apparaître si les processus physiques requièrent la disponibilité de (banques de) données.

### Rappel de centaines de milliers de 4x4 par Chrysler à cause d'une panne informatique

Les actions de rappel ne sont pas rares dans la branche automobile. Ce genre d'opération est toujours plus souvent lié à des logiciels défectueux. En mai 2013, Chrysler a ainsi rappelé plus de 400 000 4x4 à cause d'un problème informatique. Sur certains véhicules, le logiciel avait involontairement déréglé le passage des vitesses, ce qui dans le pire des cas aurait pu aurait pu aboutir à un accident.

Comme les voitures modernes comportent toujours plus de fonctions commandées par logiciel, les défaillances informatiques se répandront tôt ou tard dans le secteur automobile.

[37] http://www.handelszeitung.ch/news/peinlicher-computerfehler-american-airlines-kann-nicht-fliegen (état: 31 août 2013).

## 4.7 Opérations policières, mises en accusation et arrestations

Le premier semestre 2013 a été marqué par diverses opérations policières, par des arrestations et des condamnations de cybercriminels.

### DDoS: opération Payback

En janvier 2013, la justice britannique a condamné Christopher Weatherhead, membre du mouvement Anonymous, à 18 mois de réclusion pour son rôle dans l'opération Payback[38] lancée contre Paypal, Mastercard et Visa. D'autres activistes d'Anonymous ont subi des peines moins élevées. Aux yeux du tribunal, Christopher Weatherhead avait été le cerveau de l'opération.

### Maliciel d'e-banking Gozi

Toujours en janvier 2013, la justice américaine a accusé trois personnes d'avoir créé et diffusé le *maliciel* d'e-banking Gozi. Gozi aurait infecté au niveau mondial plus d'un million d'ordinateurs, provoquant des dégâts se chiffrant en millions de francs.

### Ransomware Reveton

En février 2013, la police espagnole a arrêté plusieurs individus ayant créé ou propagé Reveton, dont le chef de bande. Ce maliciel utilisé comme moyen de chantage (*ransomware*) bloque les machines infectées et affiche à l'écran un faux avis de police reprochant à la victime diverses infractions. Reveton promet toutefois, moyennant le paiement d'une certaine somme, d'abandonner les poursuites pénales et de débloquer l'ordinateur. Dûment adapté aux spécificités nationales, il a infecté de nombreux ordinateurs dans quasiment 30 pays dont la Suisse, comme annoncé dans le rapport semestriel MELANI 2012/I[39]. Les arrestations ont abouti grâce à l'étroite collaboration de la police espagnole, d'Europol, d'Interpol et de la société de cybersécurité Trend Micro. Or même après ces arrestations, Reveton et ses diverses variantes continuent de sévir, y c. en Suisse.

### Réseau de zombies Citadel

L'agence de police judiciaire américaine FBI (Federal Bureau of Investigation) et le fabricant de logiciels Microsoft ont désactivé quasiment 1400 serveurs utilisés par Citadel, lors d'une action commune dévoilée le 6 juin 2013. Ce *maliciel* très répandu, apparu en 2011, sert à des escroqueries à l'e-banking, y c. en Suisse. Selon Microsoft, Citadel aurait infligé des pertes de l'ordre de 500 millions de dollars à la clientèle de nombreux établissements financiers. Citadel est un maliciel d'e-banking personnalisable, vendu au noir par Internet et utilisé par de nombreux groupes criminels.

Le FBI et Microsoft ont mené l'action «b54» avec le concours d'établissements financiers et des autorités de poursuite pénale de divers pays. Les *serveurs Command & Control* désacti-

---

[38] MELANI rapport semestriel 2010/2, chapitre 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=fr (état: 31 août 2013).

[39] MELANI rapport semestriel 2012/1, chapitre 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (état: 31 août 2013).

vés servaient au pilotage et à l'administration de réseaux de zombies. Le FBI recherche en particulier un développeur nommé Aquabox, qui serait le créateur du maliciel.

L'opération "b54" perturbera indiscutablement la marche des affaires des groupes criminels utilisant Citadel. Mais il est peu probable qu'elle ait des effets durables ou qu'elle menace l'existence du maliciel. Les maliciels et les réseaux de zombies ont déjà prouvé dans le passé leur aptitude à se régénérer. Et comme ils ont tendance à s'enrichir de nouvelles fonctions, leur détection et leur neutralisation s'avèrent toujours plus difficiles.

## 4.8 Quatrième exercice international Cyberstorm

Le quatrième exercice international Cyberstorm s'est déroulé les 20 et 21 mars 2013. Les pays membres de l'International Watch and Warning Network (IWWN), dont fait partie la Suisse, y testent leur collaboration et leur capacité de réaction à une cyberattaque. L'exercice de cette année visait surtout à contrôler les procédures standard de gestion des incidents cybernétiques.

Cyberstrom est le nom d'un cyberexercice international lancé par les Etats-Unis, soit le Département de la sécurité intérieure, pour évaluer la capacité de réaction aux incidents cybernétiques. Bien qu'il soit principalement axé sur les Etats-Unis et leurs organisations de sécurité, l'exercice a toujours intégré une composante internationale. Le premier exercice remonte à 2006. A l'instar de l'exercice européen Cyber Europe 2012, Cyberstorm IV a contrôlé l'efficacité des procédures opérationnelles (SOP, Standard Operating Procedures) en place. Ces SOP règlent les modalités de la prise de contact, des échanges d'information et de la collaboration en cas de cyberincident international.

Dans le scénario de cette année, de grands portails d'information et des centres de gestion avaient été infectés et des données étaient détournées vers des serveurs étrangers. La complexité de l'exercice, d'une durée totale de plus de 32 heures, a permis de tester la coopération entre les participants. Au total quelque 300 incidents ont été simulés.

Les incidents dans le cyberespace revêtent presque toujours une dimension transfrontière. D'où la nécessité d'une approche internationale commune pour bien gérer les cybercrises. L'exercice a montré le bon fonctionnement des échanges d'informations entre pays, au niveau tant technique qu'opérationnel. Un enjeu essentiel consiste toutefois à bien interpréter la masse de données à disposition afin que si la situation devient critique, une analyse globale donne aussitôt une base de décision aux autorités compétentes.

# 5 Tendances / Perspectives

## 5.1 Risque d’ingérence étatique et rôle de la législation

Toute entreprise, qu’elle soit active sur le marché local ou à l’échelle planétaire, est soumise à la législation de l’Etat où elle opère. L’emplacement du siège principal s’avère déterminant. Typiquement, les décisions finales se prennent au lieu où se situent la direction générale et – selon le secteur d’activité – le principal site de production, la logistique et l’administration, ainsi que toutes les informations utiles à l’activité commerciale.

Cette règle de base vaut pour les fabricants de machines ou les chaînes de restauration rapide comme pour les grandes entreprises, dont les produits et services constituent le socle et l’infrastructure de base des réseaux mondiaux interconnectés. Il va de soi que parmi les normes de droit national applicables, on trouve des lois relatives à la sécurité, qui permettent de lever ponctuellement la protection des données, dans le cadre de poursuites pénales ou lors de soupçons d’activités terroristes. Ainsi, il est communément admis que les sociétés à la pointe de la technologie doivent déclarer aux autorités nationales de contrôle certaines activités déployées à l’étranger, pour prévenir toute exportation de biens à double usage dans des pays ne respectant pas les droits de l’homme. Le problème tient moins ici à l’esprit et à la finalité de telles lois, qu’à leurs effets concrets et aux modalités d’application.

Dans le cas des prestataires TIC, un autre élément accentue cette logique: une écrasante majorité d’entre eux – fabricants de logiciels ou de matériel informatique, prestataires de *cloud computing*, services de transmission des données – ont leur siège aux Etats-Unis, et donc relèvent du droit et de la jurisprudence américains. Une aussi forte concentration d’acteurs du marché dans un même pays accroît les possibilités dont dispose l’Etat en question pour intervenir, au nom de sa législation, dans les affaires de ces exploitants d’infrastructures essentielles des réseaux mondiaux. Il paraît clair qu’en pareil cas, l’usage du droit national a forcément des répercussions mondiales. Autrement dit, les Etats-Unis occupent une position hégémonique dans le monde unipolaire des entreprises TIC actives dans la promotion et l’entretien des réseaux planétaires d’échanges. On pourra certes objecter que la Chine domine tout autant le marché des composantes informatiques, soit la chaîne logistique (supply chain). La question exigera sans doute des clarifications à l’avenir. Or bien souvent, l’exploitation finale de ce matériel destiné à l’exportation, le développement des programmes contrôlant ces composantes, etc… ne sont pas en mains chinoises. Et d’ailleurs, la Chine recherche pour les moteurs de recherche, pour la messagerie électronique ou les médias sociaux des solutions locales, qui sont ainsi dépourvues d‘implications planétaires et ne concurrencent pas le rôle prépondérant joué dans ces domaines par les entreprises implantées aux Etats-Unis.

Dans l’histoire, les positions hégémoniques ont régulièrement posé, du point de vue de la politique de sécurité, des questions délicates à d’autres Etats, à leur économie et à leur population. La question récurrente ici est de savoir jusqu’à quel point un acteur en position dominante est disposé à faire des concessions à autrui, ou s’il est réellement conscient de sa suprématie et des implications qui s’ensuivent. En définitive, l’enjeu est la fiabilité d’un tel acteur – en termes de protection contre l’arbitraire et les abus de pouvoir – pour les autres Etats amenés à le côtoyer. Et cette fiabilité (se traduisant par une sécurité dans la planification et par la sécurité du droit) est au bout du compte fondamentale pour les milieux écono-

miques obliger d'entretenir, dans la sphère d'influence juridique de l'acteur en position hégémonique, des contacts avec d'autres partenaires.

Tout Etat bénéficiant d'une telle position dominante ferait bien d'analyser ce genre de questions de bonne heure et de manière approfondie. Sa souveraineté juridique n'est pas remise en cause, il s'agit essentiellement de préciser (sur le plan politique) quels objectifs il poursuit à travers ses lois, et dans quelle mesure il projette d'adopter et d'appliquer des lois servant ses propres intérêts, aux dépens de ceux d'autres pays. Autrement dit, jusqu'à quel point il entend soit poursuivre, à travers son ordre juridique et donc son influence sur l'industrie indigène (ou le cas échéant active dans le monde entier), ses propres intérêts liés à la politique de sécurité (ou év. d'ordre économique), soit y renoncer explicitement. Il incombe toutefois aussi à la communauté internationale d'aborder ces questions dans les enceintes internationales et de s'efforcer de les clarifier dans un sens ou dans l'autre. La Suisse en particulier déploie une grande activité sur ce plan, dans les forums tant multilatéraux que bilatéraux.

Une longue phase de flou et d'imprévisibilité obligerait inévitablement les Etats à adopter de manière indépendante leurs propres solutions informatiques, non pas dans le cadre d'une concurrence sportive et conforme aux règles du marché, mais au titre de leur politique de sécurité et pour se démarquer des produits du pays en position dominante. Or il va de soi que ce serait un pis-aller, source d'inefficacité et de coûts excessifs pour l'économie, à commencer par les infrastructures vitales.

En Suisse, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) préconise depuis toujours, en matière de sûreté de l'information et de protection des infrastructures TIC, une approche basée sur les risques. Cette approche figure désormais dans la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Elle a ainsi reçu l'aval du Conseil fédéral, en lieu et place d'une approche strictement technique, basée sur les possibilités offertes par les TIC. Il existe déjà ici des alternatives aux produits américains ou chinois dans le domaine des routeurs, avec des programmes créés selon les règles du marché et qui sont bien acceptés.[40]

Une fructueuse gestion des cyberrisques implique de cerner et de comprendre les diverses facettes de la menace. A côté des auteurs des agressions, des vulnérabilités techniques et des dernières découvertes sur les incidents, il faut examiner aussi le rôle de facteurs non techniques relevant de l'agencement physique, du personnel et de l'organisation, ainsi que le cadre juridique et les possibilités d'intervention des autorités dans le pays des fabricants de produits, des prestataires de services et des dispositifs de stockage des données. Chaque entreprise doit ici être laissée libre de pondérer plus ou moins fortement les facteurs de risque qui correspondent le mieux à son profil, à ses processus critiques et à son degré d'exposition à l'étranger, de même qu'à son activité commerciale.

Afin que les entreprises, à commencer par les infrastructures vitales, bénéficient à l'avenir d'un soutien accru dans ce domaine, la Stratégie nationale de protection de la Suisse contre les cyberrisques (cyberstratégie nationale, SNPC) prévoit, outre une augmentation du personnel de MELANI jusqu'en 2017, le renforcement des ressources destinées à faire valoir la

[40] http://www.fp7-ofelia.eu/about-ofelia/ (état: 31 août 2013).
http://www.change-project.eu (état: 31 août 2013).
http://www.openflow.org/wk/index.php/MPLS_with_OpenFlow/SDN (état: 31 août 2013).
http://www.heise.de/ix/artikel/Alles-fliesst-1643457.html (état: 31 août 2013).

position de la Suisse et de son économie dans les enceintes internationales s'occupant de la politique de sécurité.

## 5.2 Manuel de Tallinn

Le Manuel de Tallinn (titre original: Tallinn Manual on the International Law Applicable to Cyber Warfare) a été publié en mars 2013.[41] Cette étude porte sur les modalités d'application du droit international – droit régissant le recours à la force (jus ad bellum) et droit public humanitaire (jus in bello) notamment – dans le contexte de cyberopérations.

Dans 95 règles commentées, le Manuel de Tallinn examine notamment les questions liées à la souveraineté étatique, aux compétences juridictionnelles et aux responsabilités, sans oublier le droit de neutralité et ses implications. On y apprend quand un pirate civil peut être assimilé à un combattant et devient ainsi une cible d'attaque légitime, soit dans quelle mesure ses activités sont imputables à un Etat. La protection des infrastructures civiles vitales y est également abordée, de même que les risques encourus par les centrales nucléaires ou les barrages.[42]

Le manuel a été élaboré entre 2009 et 2012 par un groupe international formé d'une vingtaine d'experts dans divers domaines, à l'invitation du Centre de défense de l'OTAN pour la cyberdéfense en coopération basé à Tallinn, la capitale estonienne. Ce n'est pas un document officiel de l'OTAN, mais une publication académique sans valeur juridique contraignante, qui indique des approches possibles et des avis (parfois divergents) sur la manière dont on pourrait adapter le droit international aux cyberconflits. Comme il s'agit de la première publication détaillée dans ce domaine, certains Etats ou organisations s'inspireront vraisemblablement des opinions qu'elle renferme, même si elle n'a pas un caractère officiel, pour formuler leurs positions et élaborer leurs propres manuels d'instructions.

## 5.3 Fin imminente du support de Windows XP SP3 et de MS Office 2003

Le support technique de Microsoft Windows XP SP3 et de Microsoft Office 2003 cessera le 8 avril 2014. Il est donc vivement recommandé aux entreprises employant ces versions de passer au plus vite à des versions plus récentes et régulièrement actualisées du système Windows et des logiciels MS Office.

Après le 8 avril 2014, Windows XP SP3 et Office 2003 ne bénéficieront plus du support technique, des correctifs de sécurité (*patch*) et des solutions aux problèmes gracieusement proposés jusque-là par le fabricant. Et comme les défaillances des systèmes d'exploitation et des applications abandonnés ne seront plus corrigées, les cyberattaques risquent de se multiplier contre les machines continuant de fonctionner avec Windows XP SP 3 et/ou Office 2003. Les chances de succès de telles cyberattaques augmenteront, et donc le risque couru par les utilisateurs d'anciennes versions.

---

41 http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 (état: 31 août 2013).

42 http://ccdcoe.org/249.html (état: 31 août 2013).

Les toutes nouvelles versions des logiciels comportent des améliorations sur le plan de la sécurité, en intégrant les plus récentes technologies en la matière. En outre, le fabricant a éliminé les défaillances connues. L'usage des tout derniers systèmes d'exploitation ou applications, avec leurs mises à jour (gestion des *patchs* ou rustines), s'avère donc l'un des moyens les plus efficaces d'assurer sa propre sécurité.

Les entreprises dans l'incapacité d'achever leur modernisation informatique le 8 avril 2014 ont la possibilité de conclure avec Microsoft un contrat de support, afin de continuer à bénéficier de ses services. Ce service de support est toutefois bien plus onéreux que le support usuel, et renchérira progressivement. En outre, quiconque opte pour ce service devra soumettre, dans le cadre de son contrat avec Microsoft, un calendrier en vue de la migration de Windows XP SP3 et Office 2003 vers des produits plus récents.

De même, le soutien technique pour Microsoft Exchange Server 2003 et pour Microsoft Office SharePoint Server 2003 cessera le 8 avril 2014.[43]

## 5.4 Les systèmes de gestion de contenu (CMS), nouveau talon d'Achille

Ces dernières années, le nombre de sites Web a littéralement explosé. D'autant plus que même les non-spécialistes ont la possibilité de publier leur propre site, grâce à des outils simples à manier et toujours meilleur marché. Les systèmes de gestion de contenu (content management system, CMS) souvent utilisés à cet effet permettent de créer et publier un site en quelques clics, sans maîtriser la conception des sites Web. Il existe aujourd'hui des dizaines de tels CMS, employés par les exploitants de sites par hobby aussi bien que par les PME. Leur popularité croissante les rend intéressants pour les cybercriminels, qui consacreront d'autant plus d'énergie et d'efforts à la recherche de failles de sécurité qu'un logiciel est répandu et donc que le nombre de victimes potentielles augmente. A l'instar des CMS, tout logiciel comporte des lacunes de sécurité potentielles – aucun produit n'offrant des garanties absolues de sécurité. En outre, les développeurs de logiciels introduisent constamment de nouvelles fonctions. Or à chaque ligne de code supplémentaire, le logiciel ne fait pas que recevoir des fonctions supplémentaires, sa complexité s'accroît et avec elle le risque de vulnérabilité.

Les développeurs ne tardent généralement pas à apprendre les failles de sécurité et bien souvent, quelques jours seulement s'écoulent entre la découverte d'une vulnérabilité et la mise à disposition par le fabricant de la mise à jour de sécurité correspondante. Faute d'installation automatique dans le système, l'exploitant du site doit toutefois intervenir. Et comme entre-temps la gestion de nombreux sites Web incombe à des néophytes qui ont certes bénéficié d'aide pour les concevoir, mais qui méconnaissent les mesures nécessaires pour en assurer l'entretien, bien des sites Web reposent sur un CMS n'ayant plus été actua-

[43] Pour en savoir plus sur les services d'accompagnement de MS couvrant le cycle de vie complet des solutions applicatives, voir: http://support.microsoft.com/lifecycle (état: 31 août 2013).
Pour en savoir plus sur la fin du support technique de Windows XP SP3 et d'Office 2003: http://www.microsoft.com/endofsupport (état: 31 août 2013).

lisé depuis des mois voire des années, et comportent déjà le cas échéant des dizaines de failles de sécurité (connues).

Les outils actuels permettent aujourd'hui de détecter automatiquement les sites Web vulnérables pour s'y introduire. Il est par conséquent relativement aisé aux escrocs de manipuler de nombreux sites, de façon à infecter leurs visiteurs par des maliciels.

Il est possible de réduire drastiquement les attaques basées sur le CMS, en procédant par *patch*ing (reprise des mises à jour de sécurité dès leur publication). D'autres mesures encore contribuent à la sécurité des CMS. Le site MELANI fournit, à la rubrique «Listes de contrôle et instructions»[44], des explications sur les sept mesures énumérées ci-dessous.

1. Activation immédiate des mises à jour de sécurité;
2. Authentification à deux facteurs;
3. Accès à l'interface d'administration réservé à des adresses IP spécifiques;
4. Limitation, à l'aide d'un fichier .htaccess, de l'accès à l'interface d'administration;
5. Protection de l'ordinateur de l'administrateur de site;
6. Pare-feu pour applications Web (Web Application Firewall, WAF);
7. Détection précoce des failles de sécurité.

## 5.5 Là où l'on se rencontre (et s'infecte) – le trou d'eau

Dans les régions désertiques, tous les animaux se retrouvent tôt ou tard au point d'eau pour s'abreuver. Ce phénomène a donné son nom à un type de cyberattaque plus fréquemment observé ces derniers temps, l'attaque dite du trou d'eau (en angl. *Watering-Hole Attack*). Dans Internet aussi, on trouve des endroits où les internautes se rendent souvent – pour se procurer non de l'eau ou de la nourriture, mais des informations utiles. Alors que les moteurs de recherche, les portails d'information et les réseaux sociaux attirent quantité de personnes de tous les horizons, d'autres sites gérés par des prestataires spécialisés attirent surtout les internautes intéressés par le thème en question. D'où leur utilité pour les escrocs visant un corps de métier ou un groupe d'intérêt précis. S'ils parviennent à pirater un tel site pour y placer leur *maliciel*, leurs victimes correspondront précisément au public-cible.

Au printemps 2013, des inconnus se sont introduits sur le site du Ministère américain du travail pour y placer une infection par *drive-by download*, à la faveur d'une *faille de sécurité* d'Internet Explorer 8 inconnue jusque-là. La page concernée permettait au personnel de groupes énergétiques de s'informer sur les programmes d'indemnisation prévus en cas de contact avec l'uranium. Les ordinateurs consultant cette page étaient infectés par un logiciel d'espionnage. Cela montre que les pirates s'intéressaient à la main-d'œuvre du secteur énergétique – des centrales nucléaires notamment – et aux fonctionnaires fédéraux actifs dans ce domaine. Les personnes travaillant avec des armes atomiques étaient aussi visées.

[44] Listes de contrôle et instructions http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=fr (état: 31 août 2013).

Les annonces d'attaques dites du trou d'eau ont augmenté durant la période sous revue. A la différence des infections usuelles par *drive-by download*, où les cybercriminels utilisent indistinctement tout site Web mal protégé pour diffuser leurs maliciels sur n'importe quel ordinateur, de telles opérations nécessitent sensiblement plus d'efforts afin de pirater des sites spécifiques, indépendamment de la sécurité qu'ils offrent.

Ces attaques ont beau viser en premier lieu les ordinateurs de bureau, elles permettent selon l'entreprise concernée d'obtenir, outre des secrets d'affaires, d'autres informations dignes de protection (plans de réseaux, adresses et données d'accès de systèmes de contrôle, etc.), à leur tour utiles pour lancer de nouvelles attaques. Et si la segmentation du réseau d'entreprise s'avère insuffisante, les pirates n'auront qu'à passer d'un système à l'autre pour aboutir au système de contrôle pilotant les processus physiques et le manipuler à volonté.

Tôt ou tard, une *faille de sécurité* apparaît dans chaque navigateur. Nous avons indiqué au chapitre 5.1 du rapport semestriel MELANI 2012/2[45] les possibilités de minimiser les risques lorsqu'une lacune d'un navigateur est découverte. Or il n'est jamais exclu que des attaques dites du trou d'eau soient menées en exploitant de telles erreurs (y compris dans les plugiciels ou *plug-in* des navigateurs) avant qu'elles ne soient rendues publiques.

## 5.6 Chevaux de Troie dans la téléphone mobile

La tendance des maliciels à s'en prendre aux téléphones mobiles s'est poursuivie au semestre écoulé et a fortement augmenté au cours des derniers mois. Le système d'exploitation Android constitue la principale cible. Les raisons tiennent à la grande diffusion d'Android, à la structure ouverte dont il a déjà été question dans le dernier rapport semestriel[46], mais aussi au fait que beaucoup de fabricants ne communiquent pas les mises à jour de sécurité, ou alors seulement une fois les lacunes de sécurité connues.

Les buts des agresseurs sont très variés:

- attaques de comptes bancaires: vol de codes *mTAN*;
- envoi de SMS payants;
- accès aux applications mobiles de micro-paiement;
- vol de données d'accès aux réseaux sociaux et aux comptes de messagerie;
- collecte d'adresses: nom, n° de téléphone, adresse électronique et date de naissance des contacts;
- vol d'identité;
- vol de données en général.

[45] MELANI rapport semestriel 2012/2, chapitre 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: 31 août 2013).

[46] MELANI rapport semestriel 2012/2, chapitre 4.8: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=fr (état: 31 août 2013).

Bien souvent, une composante d'ingénierie sociale sert à la diffusion des maliciels. Par exemple, des apps connues sont munies d'un cheval de Troie et diffusées via des boutiques en ligne (App Store) non officielles. A cet effet, des courriels sont envoyés avec les liens correspondants. Par exemple, des courriels falsifiés d'une banque signaleront l'existence d'une nouvelle app, nécessaire au traitement en ligne des opérations bancaires. On a également observé des cas d'infection par *drive-by download*, où il suffisait de visiter un site Web pour infecter son appareil. Le phénomène a pris des proportions plus spectaculaires, avec l'apparition des premiers réseaux de zombies exclusivement formés de téléphones Android. Les appareils compromis serviront p. ex. à l'envoi de pourriels.

Il est intéressant de noter qu'une bonne partie de ces *maliciels* en circulation reposent sur le même code de base. Ainsi, diverses variantes de maliciels comportent une bibliothèque spécifique (libvadgo), servant à la communication avec les *serveurs Command and Control*. Cette bibliothèque parvient en outre à se dissimuler face aux outils d'analyse, en mettant fin à certains processus ou en manipulant diverses commandes.

La plupart des maliciels pour appareils mobiles sont actuellement écrits pour Android. Les autres plates-formes sont néanmoins aussi exposées. Lors d'attaques ciblées visant des entreprises ou des groupes de personnes spécifiques, un iPhone ou un Windows Phone donnent autant prise aux attaques qu'un terminal Android. En outre, les appareils mobiles peuvent servir de *passerelle* – notamment dans les environnements bien protégés sinon – pour accéder aux réseaux internes. Il importe de tenir compte du problème notamment dans les projets permettant à chaque employé d'utiliser son matériel électronique personnel au travail (*Bring Your Own Device, BYOD)*.

MELANI recommande les règles de comportement suivantes, en vue d'une utilisation sûre des appareils mobiles:

1. Paramétrez correctement les mécanismes de sécurité de votre téléphone (p. ex. introduction du PIN et verrouillage automatique de l'écran d'accueil).
2. N'installez que des applications provenant d'AppStores officiels. Comparez entre eux les avis d'utilisateurs. N'installez jamais d'applications à partir de liens de messagerie.
3. Avant toute installation, vérifiez les droits que réclame une application et demandez-vous s'ils sont réellement nécessaires et si vous souhaitez les accorder (p. ex. accès au carnet d'adresses, lecture et envoi de SMS). En cas de doute, mieux vaut renoncer à une installation.
4. N'utilisez qu'avec la prudence requise les points d'accès sans fil (hotspot) inconnus. Configurez votre téléphone afin qu'il ne se connecte pas automatiquement aux nouveaux réseaux sans fil.
5. Appareils Android, dès la version 4.2: assurez-vous que le service de réputation Google soit actif, car il protège votre appareil contre les menaces déjà connues (apps malveillantes). Ce service peut être configuré dans l'app «Paramètres Google», au point du menu «Valider les applications». Le paramètre «Vérifier les applications» doit être activé.
6. Appareils Android: assurez-vous que l'installation d'apps ne soit autorisée qu'à partir du Google Play Store officiel (en désactivant l'option «Sources inconnues» sous Paramètres -> Sécurité -> Administration du périphérique).

L'annexe 7.1 procède à l'analyse du cheval de Troie Android apparu au premier semestre 2013.

## 5.7 Téléphonie par Internet (VoIP): abus et cyberattaques

Les risques liés à la technologie VoIP et à ses possibilités d'utilisation abusive concernent tant les particuliers que les entreprises. Les dommages potentiels sont toutefois bien supérieurs en cas d'usage abusif de l'infrastructure VoIP d'une entreprise. En dernier lieu, il faut toujours comparer les indiscutables avantages économiques de la téléphonie VoIP avec ses inconvénients possibles sur le plan de la sécurité. Car à l'heure actuelle, les fraudes téléphoniques reposent en général sur la technologie VoIP. Un exemple suisse est décrit au chapitre 3.6. D'autres types d'attaques possibles sont décrits ci-après:

### Attaque affectant la disponibilité (Telephony Denial of Service)

Au début de 2013, les autorités américaines ont signalé le risque de *Telephony Denial of Service*, soit d'attaques en disponibilité de services téléphoniques. Concrètement, une centrale est bombardée d'appels au point d'être injoignable. Les appels sont effectués automatiquement, à peu de frais, à partir d'une installation VoIP (compromise). Ce genre d'opération est généralement accompagné d'une demande d'argent. Les exploitants de la ligne sont priés de verser une somme donnée afin que l'attaque cesse. Le phénomène est extrêmement préoccupant lorsqu'il touche des services publics, notamment des services d'urgences médicales.

### Espionnage

VoIP transforme et compresse les conversations en données numériques. Les cyberpirates cherchent à s'en emparer, comme des autres données numériques. Il existe différentes méthodes de mise sous écoute. Certains programmes malveillants sont conçus pour s'installer directement sur les ordinateurs et y enregistrer les signaux des conversations, avant même qu'ils ne soient cryptés et envoyés via le *protocole IP*. D'autres attaques portent sur les serveurs VoIP, afin d'y espionner le trafic de communication. Autre cas d'abus à signaler, il arrive que le transport de données dérobées soit camouflé pour faire croire à du trafic VoIP.

1. Une règle élémentaire pour minimiser les risques liés à l'emploi de ces technologies consiste à remplacer les codes d'accès d'origine par des mots de passe complexes.

2. Comme tout logiciel, il faut actualiser en permanence les programmes VoIP utilisés.

3. Une mesure de sécurité plus concrète consiste à configurer les appareils VoIP afin qu'ils ne puissent appeler que certaines catégories de numéros, de façon à bloquer autant que possible les numéros surtaxés.

# 6 Glossaire

| | |
|---|---|
| 0-day-exploit | Exploit paraissant le jour même où une faille de sécurité est rendue publique. |
| Adresse IP | Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87). |
| Advanced Persistent Threat | Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources. |
| App | Le terme app (abréviation anglaise d'application) recouvre tous les logiciels d'application destinés à l'utilisateur final. Dans le vocabulaire courant, il désigne surtout des applications pour smartphones modernes et tablettes tactiles. |
| Attaque DDoS | Attaque par déni de service distribué (Distributed Denial-of-Service attack) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes. |
| Attaque par réflexion de DNS | Voir DNS Amplification Attack. |
| Authentification à deux facteurs | Au moins deux des trois facteurs d'authentification sont exigés : un élément que l'on connaît (p. ex. mot de passe, code PIN, etc.) un élément que l'on détient (p. ex. certificat, jeton, liste à biffer, etc.) un élément qui nous est propre (p. ex. empreinte digitale, scanner rétinien, reconnaissance vocale, etc.) |
| Automate programmable industriel (API) | Un automate programmable industriel (en angl. programmable logic controller, PLC), est un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. |
| Bring Your Own Device (BYOD) | Bring Your Own Device (BYOD) est une pratique consistant, pour un employé, à utiliser son matériel électronique personnel dans le cadre de son travail. |
| 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 QR | Type de code-barres en deux dimensions, constitué de modules noirs disposé dans un carré à fond blanc. QR veut dire quick response, car le contenu peut être rapidement décodé. |
| 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). |
| DNS | système de noms de domaine (Domain Name System). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch). |
| DNS Amplification Attack | Attaque par déni de service (attaque Denial of Service, DoS), utilisant des serveurs DNS publics comme amplificateurs. |
| Firewall | Un pare-feu (firewall) protège les systèmes informatiques en surveillant et, éventuellement refusant, les connexions entrantes ou sortantes. Un pare-feu personnel (personal firewall ou desktop firewall) est en revanche installé pour protéger un ordinateur unique; il est directement installé sur le système à protéger, c'est-à-dire sur votre ordinateur. |
| Flash | Adobe Flash (s'abrégeant Flash, auparavant Macromedia Flash) est un environnement de développement intégré propriétaire ser-vant 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. |
| Force brute | La recherche par force brute (Brute Force) ou recherche exhaustive consiste, en informatique, en cryptanalyse ou dans la théorie des jeux, à tester toutes les combinaisons possibles (ou du moins un grand nombre) pour résoudre les problèmes. |

| | |
|---|---|
| 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. |
| Géolocalisation | La géolocalisation permet de déterminer la position géographique d'un terminal connecté à Internet en se basant sur son adresse IP. |
| Honeypot | Le terme honeypot (pot de miel) désigne, en jargon informatique, un programme ou un serveur simulant un ordinateur, un réseau complet ou le comportement d'utilisateurs fictifs. Les pots de miel servent à observer le comportement et à enregistrer les méthodes d'attaque des pirates. |
| Hyperlien | Un hyperlien, ou simplement lien, est une référence dans un système hypertexte permettant soit d'atteindre d'un clic un autre endroit du même document, soit de passer automatiquement à un document électronique lié. |
| IDS | Intrusion Detection System Systeme, mit denen man unautorisierte Zugriffe auf Daten oder Rechner erkennen kann. |
| 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. |
| Interface | Une interface est la frontière entre deux systèmes ou parties d'un même système, et par extension leur équipement d'adaptation permettant des échanges et interactions. Voir interface Web. |
| Interface Web | Interface utilisateur graphique permettant d'utiliser le navigateur Web pour activer des applications client-serveur sur son ordinateur et pour naviguer. |
| Internet-Protokoll (IP) | Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es ist die Implementierung der Vermittlungsschicht des TCP/IP-Modells bzw. der Vermittlungsschicht (engl. Network Layer) des OSI-Modells. |
| ISP | Internet Service Provider. Fournisseur de services Internet. Sociétés offrant, généralement contre rémunération, différentes prestations pour l'utilisation |

| | |
|---|---|
| | ou l'exploitation de services Internet. |
| Java | Java est une langue de programmation orientée objet et une marque déposée de l'entreprise Sun Microsystems (rachetée par Oracle en 2010). |
| Lacunes de sécurité | Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système. |
| Malware | Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie). Voir aussi malware |
| Mobile Banking | On entend par mobile banking les opérations bancaires (paiement de factures, transfert de compte à compte, consultation de comptes) effectuées par un téléphone portable ou un autre appareil portable. |
| Modbus/DNP3 | Modbus et DNP3 (Distributed Network Protocol) sont des protocoles de communication utilisés pour les automates programmables industriels. |
| mTAN | Mot de passe à usage unique envoyé par SMS et utilisé principalement dans le e-banking. |
| Open DNS resolver | Serveur DNS accessible à tous les internautes pour la résolution des noms de domaine. |
| Open Source | Open Source est une palette de licences pour des logiciels dont le code source est accessible au public, dans une optique de développement communautaire. |
| Packer | Programme ou algorithme de compression d'un programme. Conçu à l'origine pour optimiser l'espace occupé par un programme sur le disque dur. Les maliciels utilisent souvent en amont des programmes de compression afin, d'une part, de ne pas être identifiés par les antivirus et, d'autre part, de compliquer l'analyse des maliciels (rétro-ingénierie). |
| Paquet de données | Ensemble de données organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout à un destinataire. |
| Passerelle | Une passerelle (gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, n'utilisant pas le même protocole de routage. |

| | |
|---|---|
| Patch | Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi p.ex. à une lacune de sécurité |
| Phishing | Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées. |
| PHP-Script | 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. |
| Plug-In, Plugin | Plugiciel. Logiciel complémentaire qui étend les fonctions de base d'une application. Exemple : les plugiciels Acrobat pour navigateurs Internet permettent un affichage direct des fichiers PDF. |
| Point of sale (POS) | Un terminal EFT/POS est un terminal de point de vente (POS, point of sale) acceptant le paiement sans numéraire (EFT, electronic funds transfer). |
| Pourriel (Spam) | Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de pollupostateur (spammer) et ses envois de pollupostage (spamming). |
| Ransomware | Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon. |
| Remote Administration Tool | Un RAT (Remote Administration Tool, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur. |
| Réseau de zombies | Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis. |

| | |
|---|---|
| Serveur Command & Control | La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C). |
| Serveur de port série | Un serveur de port série (serial-port server) est un équipement de réseau Ethernet délivrant des ports série pour l'échange des données. |
| Serveur Web | Serveur envoyant sur requête des documents HTLM ou d'autres objets aux clients, qui sont normalement des navigateurs Web. |
| sFTP | sFTP est une méthode de chiffrement du protocole de transfert de fichiers FTP, décrite dans la norme RFC 4217. |
| Smart Meter | Un Smart Meter (compteur intelligent en français) est un compteur électrique de nouvelle génération, qui identifie la consommation énergétique de l'utilisateur de manière détaillée et peut transmettre ces données à l'entreprise chargée de la distribution. |
| SMS | Short Message Service Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile. |
| Spam Score | Indice de pourriel; système de points dont se servent les filtres pour déterminer si un message électronique est indésirable ou non. |
| Spear Phishing | Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle. |
| Spoofing (Usurpation d'identité) | Technique consistant à remplacer son identité par celle d'une autre personne, afin d'agir anonymement. |
| Telephony Denial of Service | Attaque en disponibilité de systèmes téléphoniques, essentiellement basée sur VoIP. |
| Virus | Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager. |
| Voice phishing | L'hameçonnage par téléphone est une pratique criminelle d'ingénierie sociale consistant à communiquer avec des gens par téléphone pour leur dérober des informations personnelles. Cette fraude tire habituellement parti des avantages de VoIP. |

| | |
|---|---|
| VoIP | Voice over IP, téléphonie par le protocole Internet (IP). Protocoles souvent utilisés: H.323 et SIP. |
| VoIP Toll Fraud | Escroquerie consistant à lancer, à partir d'une installation VoIP, des appels sur des numéros fortement surtaxés appartenant à l'agresseur. |
| VPN | Virtual Private Network Réseau privé virtuel. Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (p.ex. Internet). |
| Watering Hole attack | Attaque du trou d'eau, attaque ciblée par un maliciel n'infectant que des sites supposés être visités par un groupe spécifique d'utilisateurs. |
| Web Application Firewall (WAF) | Un pare-feu pour applications Web est une solution protégeant les applications Web des attaques utilisant le protocole HTTP. |
| Web Hosting | Service offert par un fournisseur d'accès à Internet ou un hébergeur, qui permet de disposer d'un espace disque sur son serveur pour diffuser un site sur le Web (synonyme de Nethosting). |
| zip | zip est un algorithme et un format de compression des données destiné à réduire l'espace mémoire occupé par les fichiers lors de l'archivage ou du transfert. |

# 7 Annexe

## 7.1 Analyse d'un maliciel pour Android destiné à la clientèle suisse des applications d'e-banking

### Fonctions

- Le maliciel transmet un SMS à un numéro mobile de l'espace russophone.
- L'objectif est de dérober les codes mTAN.
- Lors de son installation, le maliciel demande l'autorisation de lire les SMS et d'en envoyer, ainsi que des droits d'écriture sur la carte SD.
- Il se fait passer pour une application attribuant un certificat Metaforic.
- Beaucoup d'antivirus reconnaissent entre-temps le maliciel (Android/TrojanSMS.Agent.NV ).

### Infection

L'infection s'opère selon les étapes suivantes:

1. Un site Web demande à la victime d'installer une application sur son téléphone portable. Il lui faut indiquer à cet effet son système d'exploitation.
2. Un code QR s'affiche et mène à la page contenant le maliciel. Ce dernier est un paquet d'installation normal, destiné aux applications Android (fichier APK).
3. Le client doit avoir désactivé certains paramètres de sécurité, pour que l'installation puisse se faire.
4. Une fois l'installation effectuée, le maliciel devient actif et surveille l'entrée des SMS. A cet effet, il se fait passer pour un logiciel de sécurité.
5. Le SMS est adressé à un numéro de téléphone mobile en Russie.

L'escroc a pour but d'intercepter les codes mTAN et de les utiliser pour des attaques contre des comptes e-banking.

### Maliciel

Une fois installé, le maliciel se présente comme une application de sécurité de Metaforic. Metaforic est bel et bien un prestataire de services de sécurité spécialisé dans les appareils mobiles. Expérience à l'appui, les maliciels se font souvent passer, et pas seulement dans la téléphonie mobile, pour un produit fiable afin d'inspirer confiance à la victime. Dans le cas

d'espèce, la mauvaise qualité de la traduction est frappante: l'utilisateur est invité à choisir un mot de passe (Wort Dordine) et à le répéter pour confirmation:


Fig. 7: Copie de la fenêtre d'ouverture de session demandant un mot de passe (=Wort Dordine).

Après l'installation du maliciel, l'application prétend avoir réussi à émettre un certificat.

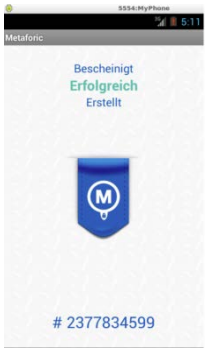



Fig. 8: Confirmation de l'installation du certificat.

Le maliciel sollicite sur le téléphone les autorisations suivantes:

```
In [19]: a.get_permissions()
Out[19]:
['android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.RECEIVE_SMS',
 'android.permission.SEND_SMS']
```

Fig. 9: Octroi d'autorisations au maliciel.

En sollicitant des droits de lecture et d'envoi de SMS, une application montre clairement qu'elle est mal intentionnée. Elle travaille en arrière-plan selon le processus suivant:

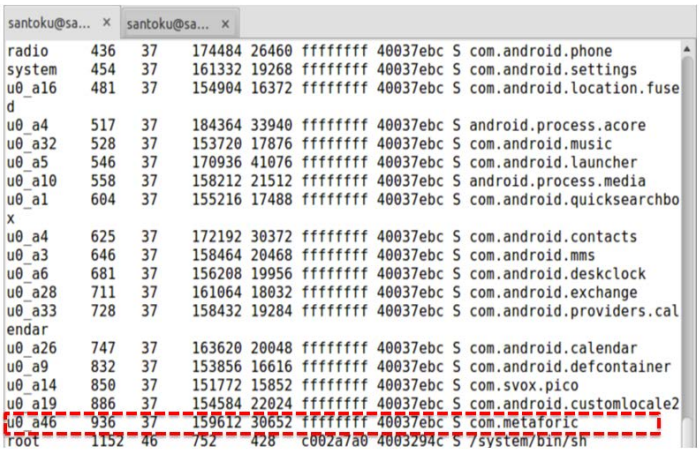



Fig. 10: L'encadré rouge indique le processus du maliciel opérant en arrière-plan.

Le code du programme amène aux conclusions suivantes:

- L'application avait été créée en néerlandais, avant d'être traduite (bien maladroitement) en allemand.

- Le numéro auquel est transmis le SMS volé figure en toutes lettres dans le maliciel. Il a pu être localisé sur le territoire russophone.

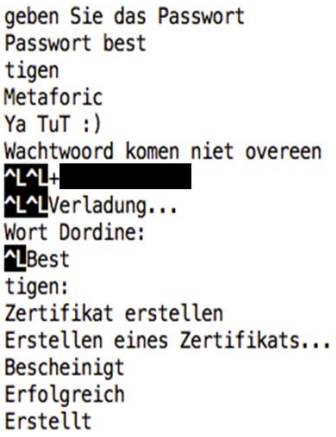



Fig. 11: Texte source muni d'un numéro de téléphone préprogrammé, auquel le SMS sera transmis.

Les applications pour Android portent toujours une signature numérique. Dans le cas précis, l'application était signée par un certificat de débogage (Debug Certificate), qui ne permet pas une distribution dans les Appstores officiels et dont l'usage est exclusivement réservé au développement et aux tests d'applications Android.

En général, les maliciels possèdent une structure très simple, sans fonction de rootkit pour se dissimuler, et ne font l'objet d'aucun cryptage ou obscurcissement pour déjouer les analyses. Ils servent exclusivement à dérober les codes mTANs. Il existe quantité de chevaux de Troie comparables sur la plate-forme Android. Leur taux de reconnaissance par les antivirus, très faible au début, avoisine désormais 50 % (état: début juillet 2013).