Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

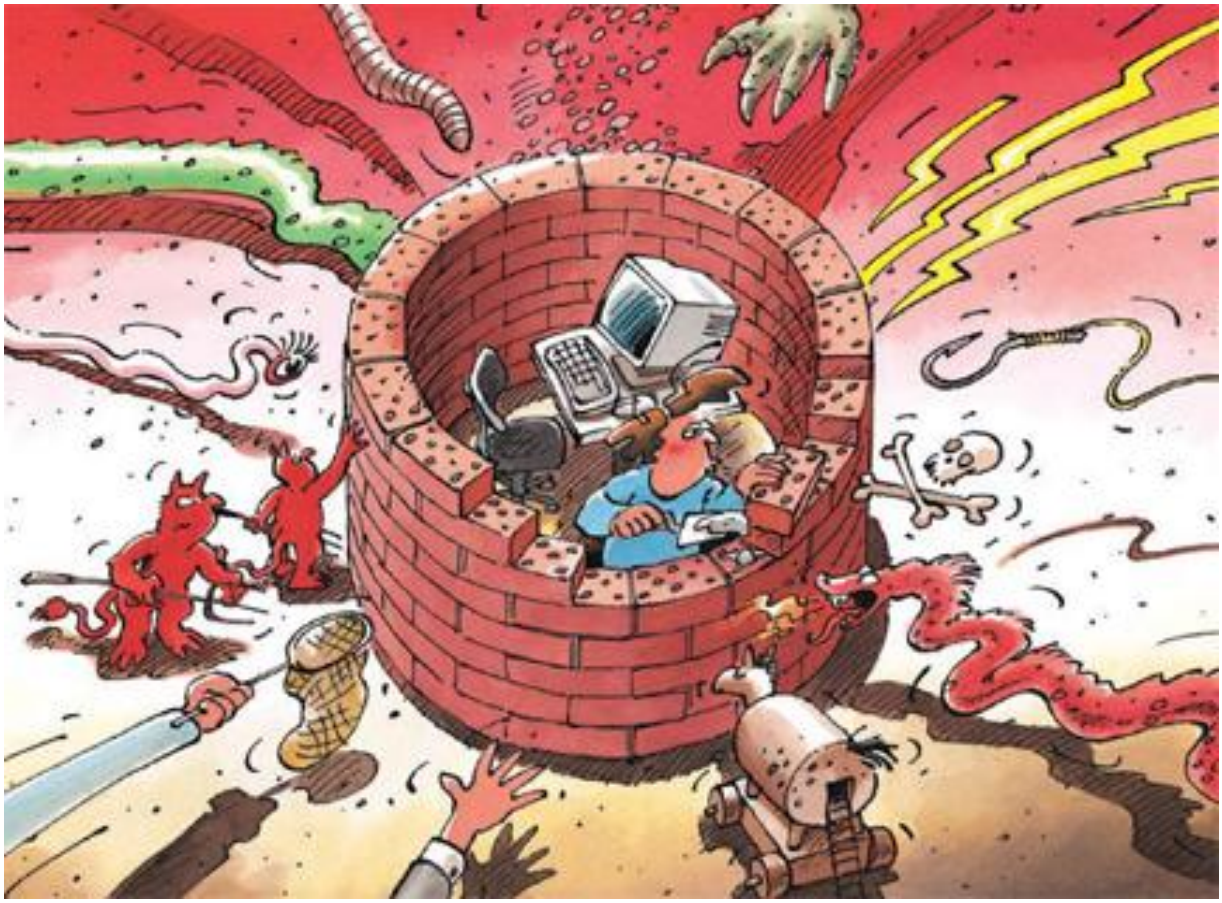
Unité de stratégie informatique de la Confédération (USIC)
Office fédéral de la police fedpol

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2007/I (janvier à juin)



En collaboration avec:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Table des matières

Temps forts de l'édition 2007/I

- **Attaques visant des services financiers suisses**
  Le nombre d'attaques «classiques» de *phishing*, où un courriel invite la victime à communiquer ses mots de passe, a fortement baissé en Suisse. Toutes sont d'ailleurs restées vaines. En revanche on compte toujours plus d'attaques fructueuses lancées à l'aide de *maliciels*. Les *systèmes d'authentification à deux facteurs* (p. ex. listes à biffer, SecurID, etc.) n'offrent plus une protection sûre dès le moment où l'ordinateur du client a été infecté par un maliciel.
  ► Situation actuelle: Chapitre 2.1 (voir aussi 2.4)
  ► Tendances pour le prochain semestre: Chapitre 3.1
  ► Exemples / Incidents: Suisse: Chapitre 4.2; scène internationale: Chapitre 5.2

- **Espionnage industriel et vol de données**
  L'espionnage industriel ciblé reste d'actualité, qu'il soit d'origine étatique ou privée. Il menace tant les exploitants d'*infrastructures vitales* et l'industrie d'armement que les services publics. Les entreprises industrielles de moyenne importance ainsi que les fabricants d'articles de luxe ou le secteur de la mode sont également visés. Les attaques se basent sur des courriels envoyés de façon ciblée à des collaborateurs. Une partie de ces envois contiennent un *maliciel* en annexe, les autres comportant un lien à un site spécialement préparé.
  ► Situation actuelle: Chapitre 2.3
  ► Exemples / Incidents: Suisse: Chapitre 4.1; scène internationale: Chapitre 5.2

- **Attaques visant des serveurs Web: envoi de maliciels, phishing, vol de données**
  Les cas de serveurs Web compromis sont en augmentation. Le but est tantôt d'utiliser les serveurs pour répandre des *maliciels*, p. ex. lors des *infections par « drive-by download »*, tantôt de dérober des données (avant tout sur les serveurs à vocation commerciale), de sauvegarder (à titre intermédiaire) des données (liées notamment au *phishing*) ou encore de diffuser des messages à contenu généralement politique.
  ► Situation actuelle: Chapitre 2.2 (voir aussi 2.4)
  ► Exemples / Incidents: Suisse: Chapitre 4.1; scène internationale: Chap. 5.1 et 5.2
  ► Prévention: Chapitre 6 (thème des infections par «drive-by download»)

- **Maliciels / Vecteurs d'attaque**
  Les *maliciels* restent généralement envoyés à l'aide d'un courriel muni d'une annexe ou d'un lien avec un site Web spécialement préparé. Des techniques astucieuses d'*ingénierie sociale* amènent la victime à ouvrir l'annexe ou à cliquer sur le lien.
  Par ailleurs, toujours plus d'infections proviennent de sites Web qui installent un maliciel sur l'ordinateur des visiteurs de passage, sans aucune intervention de leur part (*drive-by download*). Cette manœuvre tire parti des *lacunes de sécurité* du système d'exploitation, du navigateur ou d'une autre application. Le phénomène ne se limite plus, depuis longtemps, aux sites douteux et touche également des sites sérieux et connus (compromis par les pirates).
  Le taux de reconnaissance des maliciels par les antivirus reste faible.
  ► Situation actuelle: Chapitre 2.4 (voir aussi 2.2)
  ► Exemples / Incidents: Suisse: Chapitre 4.2; scène internationale Chap. 5.1 et 5.2.
  ► Prévention: Chapitre 6 (infections de type *drive-by download*)

1 Introduction

Le cinquième rapport semestriel (de janvier à juin 2007) 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 un enjeu important dans le domaine 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** à la fin du rapport. Quant aux jugements portés par MELANI, ils figurent à chaque fois dans des encadrés en couleurs.

Le **chapitre 2** décrit la situation actuelle, les dangers et les risques du semestre écoulé. Un aperçu des tendances à prévoir est donné au **chapitre 3**.

Les **chapitres 4 et 5** 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 2007. Le lecteur trouvera là des exemples à valeur d'illustration et des compléments d'information sur les observations générales des chapitres 2 et 3, à caractère général.

Le **chapitre 6** traite un thème important de la prévention, étroitement lié aux dangers mentionnés au chapitre 2.

L'accent est mis, au **chapitre 7**, sur les activités des collectivités publiques ou du secteur privé ayant trait à la sûreté de l'information, en Suisse et à l'étranger.

Le **chapitre 8** passe en revue les travaux législatifs menés.

Enfin, le **chapitre 9** résume des études ou statistiques importantes consacrées aux TIC.

2 Situation actuelle, dangers et risques

2.1 Attaques visant des services financiers suisses

Les attaques classiques de *phishing* – menées au moyen d'un courriel dont l'expéditeur est falsifié et d'un lien menant à un site Internet de phishing, dans le but de soutirer les numéros de listes à biffer destinés aux portails de e-banking – ont fortement baissé en Suisse au premier semestre. Les quelques attaques observées ont d'ailleurs échoué. Les groupes criminels s'y prennent désormais autrement pour pirater les systèmes de e-banking, comme annoncé dans le dernier rapport semestriel (chapitre 3.1). Concrètement, ils infectent les ordinateurs de clients de *maliciels* leur permettant de mener des attaques de l'intermédiaire (*man-in-the-middle*). De telles attaques ont également été lancées avec succès contre des portails suisses de e-banking.

Les maliciels distribués par courrier électronique – dans l'annexe infectée ou via un lien à un site spécialement préparé – aboutissent sans être décelés à l'ordinateur de la victime, en tirant parti des *lacunes de sécurité* du système d'exploitation ou des applications. En Suisse, des courriels dont l'expéditeur avait été falsifié (au nom de ricardo.ch et d'une étude d'avocats bernoise) ont été mis en circulation (voir chapitre 4.2). L'infection peut également se produire lors de la visite unique d'un site préparé (voir chapitres 2.2, 2.4 et 5.1), sans même que la victime ait cliqué sur un lien indiqué dans un courriel. Les maliciels deviennent actifs dès qu'un site de e-banking est consulté. Soit ils redirigent le client vers un site bancaire truqué, soit ils manipulent les données indiquées dans le navigateur.

Dans le premier cas, le site falsifié «imite» le vrai site de la banque pour obtenir le nom d'utilisateur et le mot de passe. Une fois ces informations indiquées, les sites bancaires demandent un second élément d'authentification (p. ex. numéro de liste à biffer ou code généré par un *jeton*). Le site falsifié recueille ces indications également. Après quoi il interrompt la liaison et affiche un message d'erreur. Pendant ce temps, le pirate utilise les données d'accès récoltées pour s'annoncer (en temps réel) sur le vrai site et y effectuer des transactions financières illégales.

Dans le second cas, le maliciel se loge dans le navigateur. Le pirate modifie le numéro de compte, le nom du destinataire et le montant avant que ces données de transaction de l'utilisateur ne parviennent cryptées à la banque via Internet. Puis le maliciel intercepte également la confirmation de la banque et la modifie dans le navigateur. La victime pense ainsi avoir effectué le virement souhaité, alors que le paiement est effectué à un autre destinataire et que, le cas échéant, le montant a été modifié.

Ce type de maliciel est d'ailleurs téléchargeable en tout temps sur des ordinateurs déjà infectés – comme ceux faisant partie d'un *réseau de zombies*. Par conséquent, des systèmes infectés que les pirates destinaient auparavant à d'autres usages peuvent servir ultérieurement à des fraudes contre le e-banking.

Les maliciels d'aujourd'hui permettent de lancer des attaques fructueuses contre des clients du e-banking, sans que ceux-ci aient réagi à un courriel de phishing et livré ni numéro de liste à biffer, ni mot de passe. Dès le moment où l'ordinateur du client est infecté par un maliciel, les *systèmes d'authentification à deux facteurs* utilisés par les banques suisses ou

étrangères (listes à biffer, jetons à code aléatoire ou chiffré à l'aide d'une méthode cryptographique, etc.) s'avèrent donc peu sûrs.[1]

Les utilisateurs feraient donc bien d'être prudents avec leur messagerie électronique ou en surfant sur Internet, de mettre à jour leur système d'exploitation et leurs applications, ainsi que d'utiliser des logiciels antivirus et un pare-feu actualisés (voir les recommandations figurant sur le site de MELANI).[2] En cas d'irrégularité ou d'incident inhabituel de e-banking, comme l'interruption soudaine d'une session, il importe de prévenir immédiatement l'institut financier concerné.

Le chapitre 3.1 livre une estimation de l'évolution future. La situation en Suisse est décrite au chapitre 4.2, celle sur le plan international faisant l'objet du chapitre 5.2. L'argent escroqué est souvent transféré à l'étranger par des complices, appelés «money mules» (chapitre 4.3).

2.2 Attaques de serveurs Web, à des fins de distribution de maliciels, de phishing ou de vol de données

Les cas de serveurs Web compromis ont augmenté au premier semestre 2007.[3] Google a par exemple relevé que sur quelque 4,5 millions d'URL, 450 000 tentaient de diffuser des *maliciels*. Pour juin seulement, Sophos a constaté que pratiquement 30 000 sites, généralement à contenu tout à fait sérieux, avaient été infectés chaque jour.[4] Parmi les sites compromis ayant propagé des maliciels on peut citer le site des Dolphins de Miami (vainqueurs de la finale du championnat de football américain), celui du fabricant coréen de composants informatiques Asus, le site des services de santé publique américains, ou encore celui de l'opéra et du musée d'art contemporain de Sidney.[5]

Les compromissions tirent fréquemment parti de *lacunes de sécurité* des applications Web; les banques de données gérées à partir de serveurs Web sont également souvent prises pour cibles. Une attaque menée en Italie a ainsi détourné plusieurs milliers de sites hébergés

[1] Voir: http://www.schneier.com/blog/archives/2005/03/the_failure_of.html; http://www.schneier.com/essay-083.html; http://www.zdnetasia.com/news/security/0,39044215,62010658,00.htm; http://www.darkreading.com/document.asp?doc_id=116456; http://www.itseccity.de/?url=/content/virenwarnung/aktuellemeldungen/070329_vir_akt_trendmicro.html (état au 18.07.2007).

[2] Voir: http://www.melani.admin.ch/themen/00166/index.html?lang=fr (état au 26.07.2007).

[3] Voir p. ex.: http://blogs.iss.net/archive/WebBrowserExploitati.html; http://blog.washingtonpost.com/securityfix/2007/05/cyber_crooks_hijack_activities_1.html; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017261; http://googleonlinesecurity.blogspot.com/ (état au 26.07.2007).

[4] Voir: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-update-2007_wsrus.pdf; http://www.heise.de/newsticker/meldung/93334; http://www.darkreading.com/document.asp?doc_id=120373, http://www.siteadvisor.com/studies/map_malweb_mar2007.html ainsi que le dernier rapport de l'Anti-Phishing Working Group: http://www.antiphishing.org/reports/apwg_report_may_2007.pdf (état au 17.07.2007).

[5] Voir: http://www.smh.com.au/news/security/virus-blight-spreads-to-museum-site/2007/06/13/1181414340831.html; http://www.heise.de/newsticker/meldung/84761; http://www.theregister.co.uk/2007/02/08/cdc_malware/; http://www.heise.de/newsticker/meldung/87965 (état au 26.07.2007).

sur un serveur. Il a suffi d'une lacune de sécurité présente sur un site, combinée à une erreur de configuration commise par l'hébergeur (voir chapitre 5.1, sous MPack).[6]

Les attaques lancées contre les serveurs Web visent plusieurs buts. Premièrement, le serveur compromis peut servir à diffuser des maliciels, en infectant l'ordinateur de ses visiteurs. Deuxièmement, le contrôle d'un serveur Web servant au e-commerce permet souvent de dérober de précieuses données (comme les données de cartes de crédit). Troisièmement, un serveur Web compromis peut être utilisé pour héberger des données illégales, comme un site de *phishing*, ou pour sauvegarder des logiciels piratés ou des données acquises illégalement. Les serveurs compromis sont souvent modifiés pour diffuser des messages politiques (*defacement*).

Il est recommandé aux exploitants de sites Web d'actualiser leurs applications Web et de s'assurer que leur hébergeur effectue les mises à jour nécessaires et qu'il respecte les consignes de sécurité d'usage.[7]

La question des infections par des sites Web est décrite au chapitre 2.4. Des exemples figurent aux chapitres 4.1 et 5.1, tandis que le chapitre 6 porte sur les mesures préventives.

2.3 Espionnage ciblé

La menace due à l'espionnage industriel ciblé, d'origine étatique parfois, constituait déjà une priorité thématique du rapport semestriel 2005/II, et tous les rapports ultérieurs sont revenus sur la question (voir rapport semestriel 2006/II, chapitres 2.3 et 5.2). Le risque est plus que jamais d'actualité.

Aux Etats-Unis, les attaques d'espionnage ont connu une recrudescence contre les systèmes gouvernementaux, notamment les réseaux du Ministère des affaires étrangères et du Ministère de la défense.[8] Le problème se pose également avec toujours plus d'acuité dans l'économie privée. MELANI a mis en garde à plusieurs reprises dans le passé contre des attaques visant le secteur privé helvétique. Dans d'autres pays aussi, la question est à l'ordre du jour. Selon les estimations du magazine Der Spiegel, l'Allemagne aurait déjà subi des dommages se chiffrant en milliards.[9]

La méthode utilisée dans l'espionnage industriel est généralement la même que pour l'espionnage étatique. Des recherches sont d'abord effectuées sur les employés d'une société et sur le contexte (p. ex. via des sites de réseautage personnel comme Xing, Linked-In, etc., des sites officiels d'entreprises, des sites privés de collaborateurs, des rapports annuels ou des articles de presse, etc.). Un envoi ciblé de courriels est ensuite effectué à

---

[6] Les mêmes hébergeurs sont souvent pris pour cibles, voir: http://blogs.stopbadware.org/articles/2007/05/04/stopbadware-identifies-hosting-providers-of-larged-numbers-of-sites-in-badware-website-clearinghouse (état au 26.07.2007).

[7] Des recommandations destinées à la bonne configuration des serveurs Web figurent notamment sous: http://www.cpni.gov.uk/docs/re-20030801-00726.pdf; http://www.cpni.gov.uk/ProtectingYourAssets/applications.aspx ainsi que http://www.stopbadware.org/home/security (état au 19.07.2007).

[8] Voir p. ex.: http://www.fcw.com/article97658-02-13-07-Web&printLayout; http://seclists.org/isn/2007/Jan/0023.html; http://www.heise.de/newsticker/meldung/91571/ (état au 30.07.2007).

[9] Voir: http://www.manager-magazin.de/unternehmen/mittelstand/0,2828,464284,00.html; http://www.ftd.de/unternehmen/industrie/159669.html; http://www.spiegel.de/wirtschaft/0,1518,465041,00.html; http://www.vnunet.com/vnunet/news/2184744/intellectual-property-theft (état au 30.07.2007).

quelques collaborateurs. Il s'agit généralement d'employés occupant des fonctions dirigeantes et ayant accès à des données confidentielles.[10] Les courriels affichent un nom d'expéditeur falsifié, la formulation et le contenu se réfèrent aux activités de la victime et ils contiennent un *maliciel* en annexe ou un lien à un site diffusant des maliciels (voir chapitres 2.2, 2.4 et 5.1). Les documents utilisés à cet effet font souvent partie de la famille MS Office (Word, Excel, Powerpoint), ou alors il s'agit de fichiers PDF.[11] Les attaques se basaient également sur des *0-day-exploits* tirant parti de *lacunes de sécurité* encore inconnues.[12]

Quand le secteur étatique ou des exploitants d'*infrastructures vitales* sont visés, l'espionnage porte principalement sur des données confidentielles importantes pour l'industrie d'armement ou utiles pour des activités terroristes ou militaires (voir l'exemple suisse du chapitre 4.1).

Toujours plus d'entreprises, notamment celles d'importance moyenne et celles du secteur industriel (construction de machines et d'installations surtout), sont confrontées à l'espionnage industriel – d'origine chinoise notamment. Les fabricants d'articles de luxe ou de mode sont également visés.[13] Les entreprises privées sont d'autant plus exposées qu'elles ont une avance technologique sur leurs concurrents ou qu'elles entretiennent des contacts commerciaux avec des régions économiquement arriérées et/ou dont la législation sur la propriété intellectuelle laisse à désirer.

Les auteurs des attaques sont tantôt des cybercriminels organisés ou agissant isolément (à la recherche d'informations monnayables), tantôt des concurrents (désireux d'être à la pointe de la connaissance ou de faire du sabotage), des acteurs financés par l'Etat (pour se procurer des informations sensibles à caractère militaire ou économique), ou encore des terroristes (se renseignant sur les infrastructures pour 'y commettre des attentats).

Comme les attaques ont un caractère ciblé et recourent à des maliciels spécialement créés, les logiciels antivirus et les logiciels anti-spyware ne les reconnaissent généralement pas. La distribution de maliciels par des sites Internet sérieux préalablement compromis devrait jouer un rôle croissant à l'avenir. Les pirates visent à prendre le contrôle des sites utiles à leurs desseins criminels (voir chapitres 2.2, 2.4 et 5.1).

[10] Voir aussi les rapports de MessageLabs concernant des attaques ciblées: http://www.messagelabs.com/mlireport/messagelabs_intelligence_special_report__targeted_attacks_april_2007_5.pdf et http://www.messagelabs.com/mlireport/MessageLabs%20Intelligence%20-%20Jun%20Q2%20Report%20-%20FINAL.pdf (état au 30.07.2007).

[11] Voir note précédente ainsi que: http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm; http://www.heise.de/security/news/meldung/84311; http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=software&articleId=9018519&taxonomyId=18&intsrc=kc_top (état au 30.07.2007).

[12] Voir p. ex.: http://www.theregister.co.uk/2007/04/19/us_state_dept_rooted/. Une description technique concernant une attaque typique figure sous: https://isc.sans.org/diary.html?storyid=2894; des conseils pour se protéger figurent sur le site ISC SANS: http://isc.sans.org/diary.html?storyid=2967 (état au 30.07.2007).

[13] Voir p. ex. l'article suivant du Washington Times (lien aux archives): http://nl.newsbank.com/nl-search/we/Archives?p_product=WT&p_theme=wt&p_action=search&p_maxdocs=200&p_text_search-0=chinese%20AND%20hackers%20AND%20get%20AND%20the%20AND%20drop%20AND%20on%20AND%20fashion%20AND%20houses&s_dispstring=chinese%20hackers%20get%20the%20drop%20on%20fashion%20houses%20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_sort=YMD_date:D&xcal_useweights=no (état au 30.07.2007).

2.4 Maliciels / Vecteurs d'attaque

La situation n'a guère changé par rapport au semestre précédent, sinon que toujours plus de systèmes sont infectés lors de la visite d'un site Web. La plupart du temps, le *maliciel* s'installe sur l'ordinateur de la victime par un courriel muni d'une annexe ou d'un lien à un site infecté. L'adresse du prétendu expéditeur comporte de plus en plus une référence locale visant à en augmenter la crédibilité. Les principaux exemples en Suisse ont été envoyés au nom de ricardo.ch et d'une étude d'avocats bernoise (voir chapitre 4.2).

Ainsi, toujours plus d'infections proviennent de sites Web d'où un maliciel se télécharge sur l'ordinateur de la victime de passage, sans intervention de celle-ci. Ce type d'infection a pour nom «*drive-by download*». Manifestement certains sites n'expédient qu'une seule fois leurs maliciels à la même victime – il ne se passe rien d'anormal en cas de visite ultérieure.[14] Alors que dans le passé des sites peu recommandables étaient utilisés pour la distribution des maliciels, il est toujours plus fréquent d'être infecté lors de la visite d'un site au contenu sérieux. Le site en question ne diffuse pas intentionnellement des maliciels – au contraire, les pirates ont exploité ses failles ou des erreurs de configuration pour y installer des programmes malveillants, ou pour rediriger à partir de là le visiteur vers un site contenant un maliciel (voir chapitre 2.2). L'infection se fait par des *lacunes de sécurité* du navigateur Web ou d'autres applications, comme des antivirus ou des *plugins* (Adobe Reader, Flash, QuickTime, etc.). Le logiciel MPack a beaucoup fait parler de lui dans ce contexte (voir chapitre 5.1). Il s'agit d'un outil de piratage vendu au marché noir et permettant même aux non-spécialistes de compromettre des systèmes (voir chapitre 5.2).

Les taux de reconnaissance des maliciels par les logiciels antivirus ne se sont hélas guère améliorés. C'est ainsi qu'il a fallu plus d'une semaine pour que la majorité des antivirus sur le marché reconnaissent certaines variantes de programmes malveillants.

Les pirates développent constamment de nouvelles versions du même maliciel. Les sites compromis diffusent une version différente à chaque visiteur, ou alors les versions évoluent à distance rapprochée. En outre, les maliciels sont de mieux en mieux dissimulés sur l'ordinateur infecté. Cette tactique fait que les logiciels de sécurité les ne trouvent pas et que les spécialistes ont du mal à les reconnaître et à les analyser. D'où aujourd'hui un faible taux d'identification par les logiciels antivirus.

Des exemples sont donnés aux chapitres 4.2, 5.1 et 5.2.

[14] Voir: http://www.finjan.com/GetObject.aspx?ObjId=443 (état au 26.07.2007).

3 Tendances / Evolution générale

3.1 Cybercriminalité et attaques visant des services financiers suisses

Comme indiqué dans le dernier rapport semestriel (chapitre 3.2), un marché souterrain des services cybercriminels s'est établi et évolue déjà dans une phase de consolidation. C'est notamment le cas pour le *phishing* et les escroqueries à base de *maliciels.* Le «chiffre noir» des méfaits a beau reste difficile à évaluer, la cybercriminalité est déjà considérée comme plus lucrative que le trafic international de la drogue.[15]

Les acteurs évoluant dans ce milieu appliquent le principe de la division du travail et sont organisés de façon toujours plus professionnelle, avec un degré variable d'énergie criminelle (voir chapitre 5.2). En particulier, le nombre de personnes peu qualifiées sur le plan technique mais mues par une énergie criminelle d'autant plus grande et commettant leurs vols avec des maliciels (achetés à des tiers) devrait augmenter. Le commerce des maliciels de qualité professionnelle est en constante expansion, tandis que leur taux d'identification par les logiciels antivirus diminue (voir chapitres 2.4 et 5.2).

Un tournant vient d'être franchi. L'ère des «vagues» ponctuelles de phishing, dont le début et la fin pouvaient être établis avec précision, est révolue. A l'avenir les attaques lancées avec des maliciels contre des solutions de e-banking occasionneront à tout moment des pertes au système bancaire – à l'instar des abus de cartes de crédit.

Il est à prévoir que les maliciels visant les portails suisses de e-banking seront bientôt aussi diffusés par *infection par « drive-by download »*, et non seulement par courriel comme jusqu'ici (voir chapitres 2.1, 2.2, 2.4, 5.1 et 6). C'est ainsi que quiconque surfe sur Internet sans prendre des mesures de sécurité suffisantes (système d'exploitation et applications dûment actualisés) s'expose à être attiré sur un site spécialement préparé et à voir ses comptes bancaires pillés. Il ne sera même plus nécessaire d'avoir réagi à un courriel suspect.

L'expansion des attaques de maliciels contre les services financiers devrait se poursuivre, aussi longtemps que les poursuites pénales ne seront pas mieux coordonnées à l'échelle internationale, que des bases légales harmonisées n'auront pas été mises en œuvre et que des progrès techniques n'auront pas été réalisés dans la sécurité du e-banking. En Suisse, un écueil supplémentaire tient à ce que la Confédération n'a pas la primauté pour les poursuites pénales, alors que de tels cas ont un caractère typiquement supracantonal ou international. La coordination des enquêtes entre les diverses polices cantonales concernées est un frein à l'efficacité et devrait donc absolument se faire à l'échelon de la Confédération. En outre, il serait important d'annoncer systématiquement les incidents à la police.

La situation actuelle est décrite au chapitre 2.1. Le chapitre 4.2 analyse les incidents survenus en Suisse et le chapitre 5.2 fait le point sur la situation internationale.

[15] Voir p. ex.: http://www.vnunet.com/articles/print/2189322; http://www.silicon.com/publicsector/0,3800010403,39166127,00.htm (état au 30.07.2007).

4 Bilan de l'infrastructure TIC nationale

4.1 Attaques

Piratage du site d'une société suisse spécialisée dans la technologie spatiale

En juin 2007, un accès non autorisé a été constaté à la zone protégée par mot de passe d'un site consacré à la recherche sur les moteurs-fusées. Les détecteurs installés ont rapidement reconnu et empêché l'accès illégal, ce qui fait qu'aucune donnée n'a pu être téléchargée. L'accès provenait d'*adresses IP* proche-orientales, de Palestine et de Syrie notamment. On ignore toutefois si l'attaque venait réellement de ces pays, ou si elle avait été lancée à partir d'ordinateurs basés dans ces pays pour dissimuler sa vraie provenance. Mais il est révélateur qu'une semaine avant l'attaque, un courriel muni d'une adresse IP palestinienne avait déjà été envoyé pour inviter l'entreprise en question à collaborer.

Cet exemple montre que même des entreprises de taille moyenne peuvent faire l'objet d'attaques d'espionnage industriel. Dans le cas d'espèce, seule l'application exemplaire de mesures de sécurité a permis d'éviter le transfert non désiré de savoir.

MELANI donne au chapitre 2.2 une appréciation des attaques visant des serveurs Web. Le chapitre 2.3 traite de l'espionnage industriel ciblé contre des entreprises suisses.

4.2 Criminalité

Attaques de maliciels visant des services financiers suisses

Comme indiqué au chapitre 2.1, les attaques lancées contre des instituts financiers suisses au moyen de maliciels ont fortement augmenté au premier semestre 2007. Elles ont culminé en mai et juin, avec l'envoi de deux courriels au nom d'expéditeur falsifié.

La première vague de *pourriels* transmis à des adresses électroniques suisses feignait d'être une communication officielle de ricardo.ch, célèbre maison de ventes aux enchères en ligne. Le destinataire y était informé, au nom de l'équipe de Ricardo, qu'il devait encore régler une facture ouverte. Pour voir les détails de la facture, il fallait ouvrir une annexe ressemblant à un document au format PDF. En réalité, il s'agissait d'un programme exécutable. Une fois le document ouvert, le *maliciel* Nurech / Wsnpoem infectait l'ordinateur de la victime.

Une attaque similaire est intervenue quelques semaines plus tard. Cette fois le courriel était envoyé au nom d'une étude d'avocats bernoise – qui n'y était pour rien. Le maliciel se dissimulait dans une prétendue facture au format PDF. Les criminels avaient adressé leur courriel à un nombre impressionnant d'adresses électroniques valables. En quelques jours, le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) a reçu plus de 600 annonces concernant cet incident, ce qui constitue un record.

Dans les deux cas, les victimes ayant ouvert l'annexe de la prétendue facture ne pouvaient pas savoir que leur ordinateur avait été affecté. Car la plupart des logiciels antivirus n'étaient pas encore en mesure d'identifier le maliciel. Celui-ci restait inactif jusqu'à ce que la victime accède à son compte bancaire par e-banking. Ce n'est qu'à ce moment que des dysfonctionnements trahissaient la présence du maliciel. Par exemple, une page blanche

apparaissait avec une barre indiquant le lent chargement en pourcentage du site, ou des fenêtres contextuelles s'ouvraient. Ces annonces étaient censées faire croire à la victime à une surcharge momentanée de son application de e-banking. En réalité, la liaison au serveur était interrompue pour permettre aux criminels d'effectuer des transactions financières au nom de la victime.

Dans les exemples qui précèdent, l'utilisateur infecte lui-même son ordinateur en cliquant sur la prétendue facture, contrairement aux cas d'*infection par «drive-by download»* (voir chapitres 2.2, 2.4, 5.1 et 6). Pour rendre leur courriel plus plausible, les pirates avaient adapté leur message au contexte local – le même maliciel a servi à l'étranger contre des banques, mais avec un texte différent ou sous forme de drive-by download (voir chapitre 5.2). MELANI recommande de ne jamais cliquer sur les annexes ou les liens de courriels sans s'assurer d'abord qu'ils émanent de personnes de confiance et qu'il s'agit bien des documents que l'on attend.

Ces attaques visent à prendre le contrôle des sessions de e-banking. Au cas où vous auriez déjà cliqué sur une annexe ou un lien douteux, assurez-vous avant votre prochaine session de e-banking que votre ordinateur ne contient aucun maliciel. Demandez dans tous les cas le conseil d'un spécialiste. Et si un incident (tels ceux indiqués plus haut) se produit pendant une session de e-banking, prenez immédiatement contact avec votre banque.

Les attaques lancées après les vagues de pourriels ont connu un certain succès. MELANI ne connaît bien entendu ni les montants exacts dérobés, ni le nombre d'incidents. Ils se situent toutefois à un niveau très bas en comparaison des escroqueries basées sur les cartes de crédit ou les cartes EC.

MELANI évalue au chapitre 2.1 les attaques de maliciels lancées contre des services financiers. Le chapitre 3.1 expose les grandes tendances, et le chapitre 5.2 est consacré à la situation internationale. La rubrique qui suit est consacrée aux attaques classiques de phishing visant des prestataires suisses de services financiers. L'argent escroqué est souvent transféré à l'étranger par des complices, appelés «money mules» (voir chapitre 4.3).

Attaques classiques de phishing contre des services financiers suisses

Vagues de phishing visant la clientèle suisse de Visa

Au premier semestre 2007, trois vagues de *phishing* ont été observées contre la clientèle suisse des cartes de crédit Visa. Toutes se sont déroulées selon le même modèle. Un *pourriel* prétendument envoyé par le département de la sécurité de Visa invitait le destinataire à vérifier les données de sa carte de crédit, en expliquant qu'un abus avait peut-être été commis. A cet effet, il fallait scanner le recto et le verso de sa carte et les transmettre, sous forme de document PDF, à l'adresse électronique créée par les pirates.

Ce pollupostage présentait un détail intéressant, à savoir qu'il appelait tous les destinataires par leur nom de famille. Or l'adresse électronique ne livrait pas toujours cette information. Autrement dit, les pirates disposent de listes de courriels susceptibles de contenir d'autres données que la seule adresse électronique. Ils peuvent ainsi donner une apparence plus professionnelle à leur escroquerie et s'adresser par exemple personnellement aux victimes, comme indiqué plus haut. Il est également intéressant de noter que les courriels des deux premières vagues étaient rédigés en anglais, avant d'être traduits en allemand. Cela montre que les deux premières tentatives n'avaient guère été fructueuses, et que les pirates ont voulu réagir. Il reste à signaler que MELANI a pu rapidement désactiver à chaque fois les domaines (avec les adresses électroniques) utilisés pour cette escroquerie, et donc que les escrocs ont eu très peu de temps pour commettre leur forfait.

Les attaques «classiques» de phishing sont devenues inoffensives

Au semestre passé, des tentatives «classiques» de phishing ont également visé des prestataires suisses de services financiers. Elles sont toutefois restées infructueuses, en raison de leur piètre qualité et faute d'une masse critique suffisante. Les attaques ne recueillaient par exemple que le nom d'utilisateur et le mot de passe, et non le numéro de la liste à biffer. Le manque de préparation des pirates ainsi que leur dilettantisme contrastent avec le professionnalisme des attaques précédentes (voir début de la dernière rubrique). Il est tout aussi intéressant de constater que ces attaques visaient aussi de petits prestataires financiers peu connus. En outre, une vague de phishing en français a été observée pour la première fois en Suisse.

De façon générale, les attaques «classiques» de phishing ne constituent plus une menace sérieuse en Suisse – le risque venant désormais des attaques lancées à l'aide de maliciels.

MELANI évalue au chapitre 2.1 les attaques de maliciels lancées contre des services financiers. Le chapitre 3.1 expose les grandes tendances, et le chapitre 5.2 est consacré à la situation internationale. Une dernière section (voir page précédente) est consacrée aux attaques lancées contre des banques suisses.

4.3 Divers

Fausses informations boursières, banques fictives et agents financiers: avalanche de pourriels dans les boîtes aux lettres électroniques suisses

Fausses informations boursières

Le deuxième rapport semestriel 2006 de MELANI a déjà signalé l'existence de fausses informations boursières appelées «stock pump and dump *spams*» (chapitre 2.2). Des pourriels recommandent d'acheter certaines actions, pour en faire grimper le cours. Pendant ce temps, les spammeurs se défont de leurs actions acquises peu avant et réalisent un bénéfice. Aux brèves annonces des débuts ont succédé de véritables analyses financières, rédigées dans un langage savant pour convaincre. De nouvelles techniques sont parfois utilisées, notamment la prise de contact téléphonique.

Banques fictives

La réputation de la place financière helvétique stimule toujours la création de banques fictives dont l'adresse électronique se réfère à notre pays. Au premier semestre 2007, plusieurs liens URL ont été enregistrés, avec des noms comme www.swissbank-offshoreuk.page.tl ou www.swissbank.page.tl. Les sites en question publiaient même des photos de la direction générale de la Banque nationale pour suggérer un caractère officiel.

Agents financiers

La perspective d'obtenir un revenu accessoire en échange d'un effort minimal et sans qualifications particulières a incité bien des personnes à se laisser recruter comme «agents financiers» par des réseaux criminels. Les agents financiers doivent prévoir chaque jour du temps pour se faire envoyer de l'argent sur leur compte et le transférer à des tiers. Un pourcentage fixe du montant viré leur est réservé, en tant que commission pour services rendus. Ces intermédiaires, connus sous le nom de «money mules», sont toujours plus prisés des criminels pour blanchir l'argent obtenu lors d'escroqueries en ligne (phishing en

particulier). Les nombreux cas signalés à MELANI attestent de l'ampleur prise par ce phénomène dans la cybercriminalité. Le recrutement d'agents financiers s'intensifie au rythme des attaques basées sur des *maliciels* visant les portails de e-banking (voir chapitres 2, 4.1 et 5.2), qu'il précède généralement de peu. Les pourriels envoyés parlent d'activités simples et lucratives, et l'annonce renvoie souvent à un site Internet créé à cet effet.

Plusieurs sites Internet de ce genre ont été enregistrés au premier semestre 2007. Tous portaient des noms similaires et la stratégie utilisée était souvent la même. Les sociétés en question se prétendent actives dans toutes sortes de domaines, du secteur financier au commerce en ligne, en passant par les bonnes œuvres. Elles possèdent des sites d'apparence sérieuse, avec des noms comme Mimotrans, GammaFinance, Next Level ou Donation Europe, cherchant ainsi à dissiper les doutes éventuels de leurs agents potentiels quant à la légalité de leurs activités.[16]

Beaucoup de (cyber) criminels recourent à Western Union, MoneyGram, etc. pour transférer leur butin à l'étranger. Comme de tels systèmes ne laissent aucune trace écrite, il n'est pas possible de remonter à la source des versements effectués. La prudence est donc de mise chaque fois qu'une personne ou organisation inconnue insiste pour qu'une transaction financière passe par de tels services de transfert d'argent. La remarque ne vaut d'ailleurs pas seulement pour le cas susmentionné des agents financiers, mais s'applique aussi aux enchères en ligne, aux réservations de chambres d'hôtel ou encore aux gains inattendus à la loterie. MELANI conseille de recueillir un maximum d'informations sur la personne (ou l'organisation) qui demande un transfert en espèces. En cas de doute, il convient de s'abstenir. Il est bon de rappeler que quiconque collabore au transfert de fonds provenant d'activités illégales risque d'être inculpé de blanchiment.

Internet: vagues de pourriels contenant des menaces de mort

Un courriel envoyé au début de mai invitait ses destinataires à verser une certaine somme d'argent, en les menaçant de mort s'ils ne s'exécutaient pas. De très nombreuses personnes et des petites et moyennes entreprises ont reçu de tels *pourriels* rédigés dans un allemand approximatif et diffusé depuis un serveur basé à l'étranger. L'envoi avait été fait au hasard, sans règle systématique quant au choix des destinataires. Le contenu et les menaces n'étaient qu'une mauvaise plaisanterie.

D'entente avec les cantons, l'Office fédéral de la police (fedpol) a publié un communiqué officiel à la population. Il y recommande aux personnes ayant reçu ce genre de message de n'y répondre en aucun cas et de ne communiquer aucune information personnelle les concernant.

[16] Un exemple de prétendue offre d'emploi est décrit sous: http://www.melani.admin.ch/dienstleistungen/archiv/01023/index.html?lang=fr ainsi que sous http://www.melani.admin.ch/dienstleistungen/archiv/00441/index.html?lang=fr (état au 21.08.2007).

5 Bilan international de l'infrastructure TIC

5.1 Attaques

Attaques DDoS contre l'Estonie: un acte de guerre?

L'Estonie a subi à la fin d'avril une série d'*attaques par déni de service distribué (DDoS)* qui se sont succédé sur plusieurs semaines. La plupart des sites visés sont restés paralysés. L'Estonie a dû suspendre temporairement ses liaisons Internet internationales pour maîtriser ce fléau. Les attaques ont fait suite au déplacement d'un monument à un «soldat (russe) inconnu» du centre de Tallinn, la capitale, dans un cimetière militaire de banlieue. Cette action avait suscité de violentes protestations parmi la minorité russe établie à Tallin, et la jeunesse moscovite s'en était prise à l'ambassade estonienne. En effet, si les Russes voient dans ce monument un symbole de la victoire des Alliés, les Estoniens l'associent à l'occupation russe durant la guerre froide. Leur pays se targue par ailleurs d'être à l'avant-garde dans le domaine des technologies de l'information et de la communication.[17]

Peu après le début des attaques, les sites Web du président d'Estonie, du premier ministre, du Parlement et de presque tous les ministères ont cessé d'être atteignables. Dès le 30 avril, les attaques se sont intensifiées et étendues aux fournisseurs de services Internet, à la presse, aux serveurs de messagerie du Parlement estonien, au e-banking, aux universités et à divers autres services Internet. Elles ont atteint leur point culminant le 9 mai, journée commémorative de la victoire russe contre l'Allemagne nazie. Les attaques DDoS lancées ce jour-là ont mobilisé un *réseau de zombies* qui comptait visiblement plus d'un million d'ordinateurs disséminés à travers le monde. Tout est rentré dans l'ordre le 10 mai, soit à l'expiration des 24 heures pendant lesquelles le réseau de zombies avait été loué.[18]

Peu après le début des attaques, des officiels estoniens ont déclaré avoir des preuves que les attaques émanaient du Kremlin.[19] Or les analyses ultérieures – dues aux experts internationaux dépêchés sur place par l'OTAN, les Etats-Unis, Israël et l'UE – ont montré que l'attaque ne venait pas de Moscou. Au contraire, on peut considérer qu'il s'agissait d'un cas typique de «hactivisme» (piratage informatique à mobile politique). L'hypothèse est corroborée par le fait que les attaques provenaient de sources différentes, étaient d'intensité variable et n'ont pas toutes eu la même durée. En outre, elles étaient bien trop peu élaborées pour pouvoir être attribuées à un gouvernement.[20] En pareil cas, comme pour la cybercriminalité en général, il est extrêmement difficile d'identifier à coup sûr l'auteur.

Les attaques DDoS lancées contre l'Estonie n'ont pas été le seul incident de grande envergure du premier semestre 2007. Alors qu'en février une attaque (vaine) visait plusieurs

---

[17] Des informations complètes sur cet incident figurent sous: http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598; http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868 (état au 16.07.2007).

[18] Voir http://www.nytimes.com/2007/05/29/technology/29estonia.html?hp ainsi que http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (état au 16.07.2007).

[19] Voir aussi: http://www.heise.de/tp/r4/artikel/25/25218/1.html; http://www.tagesspiegel.de/politik/International;art123,1785339 (état au 16.07.2007).

[20] L'analyse la plus complète est due à Arbor Networks: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/; le US-CERT parvient à la même conclusion: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/print_view/ (état au 16.07.2007).

serveurs de noms de domaine (*domaine name server, DNS)*, en juin des fabricants d'antispams étaient pris pour cibles.[21] De telles attaques montrent les ressources dont dispose désormais le crime organisé. Ses réseaux de zombies ne sont plus seulement loués pour l'envoi de *pourriels*. Une clientèle est prête à commanditer des attaques DDoS, comme cela s'est très probablement passé dans le cas de l'Estonie.

Les attaques DDoS à mobile politique – tout comme les défigurations de sites par des pamphlets politiques (*defacement*) – n'ont rien de nouveau. Des attaques similaires avaient déjà eu lieu lors du bombardement par méprise de l'ambassade de Chine durant la guerre du Kosovo à la fin des années 1990, au début de la dernière guerre d'Irak en 2003 ou encore en 2006, lors de l'affaire des caricatures de Mahomet dans la presse danoise. A nouveau, on a pu observer comment les instructions ont circulé dans les forums spécialisés, et avec quelle aisance même des personnes sans connaissances techniques sont parvenues à attaquer des sites estoniens. La nouveauté tient à l'ampleur des agressions, qui ont privé un pays entier de l'usage normal des technologies de l'information.

Selon l'état actuel des connaissances, les attaques lancées contre l'Estonie ne peuvent être attribuées ni à la Russie officielle, ni à aucun autre acteur concret. Des indices suggèrent bien qu'elles pourraient émaner des milieux nationalistes russes. Mais il est impossible d'y démêler le rôle des ententes entre auteurs présumés, de connaître les instigateurs et de savoir qui a bénéficié du soutien de qui. Des questions essentielles restent par ailleurs ouvertes: Comment faut-il qualifier, en droit international/ droit de la guerre, une attaque cybernétique déclenchée contre un Etat? Que représente-t-elle pour l'OTAN et l'article 5 du Traité de l'OTAN, qui prévoit qu'une attaque armée contre un membre de l'OTAN sera automatiquement considérée comme une attaque contre tous les membres de l'OTAN (cas de la défense collective)?[22]

L'OTAN a déjà inscrit à l'ordre du jour la question des opérations d'information (OI, «operation informations») et vise, d'une part, à améliorer son potentiel de défense contre les attaques visant ses systèmes de l'information et, d'autre part, à étendre le champ d'application de l'article 5 à de tels incidents.[23] De façon générale, la question des cyberattaques n'est pas réglée dans le droit international public, alors même que l'exemple estonien montre à quel point les économies publiques dépendent aujourd'hui des technologies de l'information.

Outre l'OTAN, des Etats sont en train de s'équiper et de renforcer leurs capacités existantes dans le domaine de la guerre de l'information (voir chapitre 7.1).

[21] Voir à propos d'attaques DDoS comparables le rapport semestriel MELANI 2006/I, chapitre 5.3; et à propos des attaques visant les serveurs de noms de domaine DNS: http://asert.arbornetworks.com/2007/06/february-2007-root-server-attacks-a-qualitative-report/ (état au 16.07.2007).

[22] Voir http://www.economist.com/world/international/displaystory.cfm?story_id=9228757 (état au 16.07.2007).

[23] Voir http://www.nato.int/docu/pr/2007/p07-067f.html (état au 16.07.2007).

Attaques via le World Wide Web (infection par "drive-by download"): l'exemple de «MPack»

Les cas de *infection par «drive-by download»* (installation de *maliciels* lors de la visite de sites infectés) ont augmenté au premier semestre 2007, pour constituer l'une des plus graves menaces actuelles (voir chapitres 2.2, 2.4 et le dernier rapport semestriel). La meilleure illustration de cette tendance vient de «MPack» – une application pour serveurs Web qui, au mois de juin, a infecté les ordinateurs de dizaines de milliers d'internautes au cours de la visite de sites spécialement préparés. On peut l'obtenir au marché noir, avec assistance et mises à jour régulières (voir à propos du marché noir, des prix, etc. le chapitre 5.2).[24]

En Italie notamment, des pirates ont manipulé de nombreux sites Web – visiblement plus de 10 000[25] –, en y ajoutant une ligne de code pour que lors du chargement du site, un maliciel soit téléchargé d'un autre serveur. Le maliciel contient MPack, logiciel doté d'une fonction d'infection automatique. MPack vérifie d'abord le système d'exploitation et le navigateur utilisés par la victime puis teste dans l'ordre, en fonction des applications utilisées, les *exploits* adéquats, tirant simultanément parti de plusieurs *lacunes de sécurité* (p. ex. produits Microsoft comme Internet Explorer ou les services du système d'exploitation Windows, Media Player, etc., mais aussi WinZip ou Apple QuickTime). MPack n'a exploité jusqu'ici que des lacunes de sécurité connues. Par conséquent, les systèmes régulièrement actualisés ont été épargnés. Il serait néanmoins envisageable d'inclure les *0-day-exploits* dans ce genre d'outil de piratage.

Dès qu'un code malveillant fonctionne, d'autres maliciels peuvent être chargés à volonté sur le système infecté. A l'instar de «Torpig» (voir chapitres 4.2 et 5.2), qui s'est limité jusqu'ici aux sites étrangers de e-banking, ou des maliciels servant à recueillir des données personnelles. Les ordinateurs infectés risquent également d'être intégrés dans un *réseau de zombies*, utilisable par exemple pour des envois de *pourriels*. L'attaque lancée via les sites Web italiens a visiblement infecté plus de 80 000 ordinateurs. Les sites manipulés relevaient du tourisme, de l'hôtellerie, de la location de véhicules, etc. et donc étaient parfaitement recommandables.[26]

Selon l'analyse d'ISC SANS, les milliers de sites compromis n'étaient hébergés que par quelques serveurs. Il a donc manifestement suffi d'une lacune de sécurité sur un seul site, pour que les pirates puissent modifier tous les autres sites du serveur, en tirant parti d'une configuration défectueuse au niveau de l'hébergeur. En d'autres termes, un seul site négligé fait courir un risque à tous les autres sites hébergés sur le même serveur.[27]

Ce type d'attaque a pour particularité de faire toujours plus de victimes parmi les sites sérieux, qui diffusent ensuite des maliciels à l'insu de leur administrateur (voir chapitre 2.2). Il

[24] Informations générales sur MPack: http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=8656&ver=21&pagina=3&numprod=&entorno=, http://reviews.cnet.com/4520-3513_7-6745285-1.html; http://www.heise.de/newsticker/meldung/91542 ainsi que http://blog.washingtonpost.com/securityfix/2007/06/the_mother_of_all_exploits_1.html (état au 17.07.2007).

[25] Voir http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782 (état au 17.07.2007).

[26] Des informations détaillées concernant MPack figurent sous: http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares et sous http://isc.sans.org/diary.html?storyid=3015 (état au 17.07.2007).

[27] Voir http://isc.sans.org/diary.html?storyid=3078 (état au 17.07.2007).

devient par conséquent risqué de naviguer si l'on détient les pleins droits d'administrateur, a fortiori dans les entreprises.

Il est possible d'être infecté par un maliciel sans le moindre clic, sans avoir ouvert d'annexe ni réagi à un courriel – en théorie même avec un système d'exploitation et des applications à jour – lors de la visite de sites sérieux. Or dans la pratique, les pirates n'exploitent jusqu'ici presque que des lacunes de sécurité connues, absentes des ordinateurs tenus à jour.

Le chapitre 2.2 traite de l'augmentation des attaques contre des serveurs Web, tandis que le chapitre 6 présente les mesures préventives contre les infections par « drive-by download ».

5.2 Criminalité

Attaques de phishing et de maliciels contre les services financiers: bilan international

Les attaques de *phishing* et de *maliciels* sont un phénomène actuel, et pas seulement en Suisse (voir chapitres 2.1 et 4.2). Sur le plan international aussi, la tendance est aux attaques de maliciels lancées contre des prestataires financiers. L'Anti-Phishing Working Group évoque notamment, dans ses statistiques du premier semestre 2007, la recrudescence des sites diffusant des maliciels à cet effet.[28]

L'incident le plus spectaculaire a été annoncé en début d'année en Suède, aux dépens de Nordea, la plus grande banque scandinave. Près de 900 000 euros ont été dérobés, sur au moins 250 comptes de clients. Un maliciel créé sur mesure avait été acquis au noir pour quelques milliers de dollars à un programmeur se faisant appeler «The Corpse» (voir deux contributions plus loin). Ce genre de maliciel est livré avec la garantie que les logiciels antivirus ne le détecteront pas. L'*authentification à deux facteurs* utilisée par la banque Nordea – comparable aux systèmes en usage dans les banques suisses – a été déjouée.[29] D'autres attaques de l'intermédiaire (*man-in-the-middle,* MITM) ont été menées avec succès, notamment en avril aux Pays-Bas, contre ABN Amro.[30]

Une forte augmentation des sites de phishing a été observée au premier semestre 2007, en avril notamment, le nombre d'incidents signalés restant quant à lui stable.[31] Ce phénomène tient sans doute à la popularisation des «phishing kits».[32] Ces outils prêts à l'emploi, souvent dotés d'une interface graphique simple, sont mis en vente par des programmeurs ayant des connaissances d'experts et permettent même à un néophyte de nuire assez facilement (voir la section consacrée à RockPhish dans le dernier rapport semestriel et ci-dessous, deux contributions plus loin). Les outils existants permettent de réaliser des centaines de sites de

[28] Voir: http://www.antiphishing.org; http://www.darkreading.com/document.asp?doc_id=123771 (état au 18.07.2007).

[29] Informations sur l'incident de Nordea: http://www.nytimes.com/2007/01/25/technology/25hack.html?ex=1327381200&en=58990497ce27b2b2&ei=5088&partner=rssnyt&emc=rss (état au 18.07.2007).

[30] Voir sur l'incident d'ABN Amro: http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/ (état au 18.07.2007).

[31] Voir les rapports de l'Anti-Phishing Working Group: http://www.antiphishing.org (état au 18.07.2007).

[32] Voir: http://blogs.iss.net/archive/PhishingIncreases.html; http://blogs.iss.net/archive/PhishingKits.html; http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0607.pdf; http://www.rsa.com/press_release.aspx?id=7667; http://asert.arbornetworks.com/2007/04/peeling-the-covers-off-of-rock/; http://blog.washingtonpost.com/securityfix/2007/05/phishing_attacks_soar_nets_wid_1.html (état au 18.07.2007).

phishing (ou de sites relais/proxy pour les attaques MITM), d'autant plus difficiles à éradiquer qu'ils sont nombreux.[33] Le nombre de groupes possédant un niveau élevé de maîtrise du phishing semble quant à lui être resté constant.

Les attaques classiques de phishing lancées à l'aide d'un courriel demandant le nom d'utilisateur et le mot de passe continuent d'être pratiquées contre les systèmes d'authentification simples, et visent notamment la clientèle des sites de réseautage personnel comme MySpace.[34]

La recrudescence des attaques par maliciels découle du recours toujours plus fréquent, dans l'espace anglo-saxon, à l'authentification à deux facteurs. PayPal, eBay et Barclays, l'une des principales banques britanniques, en sont les principaux exemples.[35] Il faut dire qu'en août 2006, l'autorité américaine de surveillance des banques a réitéré sa recommandation d'octobre 2005 aux banques de recourir à l'authentification à deux facteurs. Cette recommandation est toujours plus suivie; à la fin de cette année, la plupart des banques anglo-saxonnes devraient en effet s'aligner sur les normes de sécurité élevées en place en Europe, en Suisse notamment.[36] Alors qu'auparavant, la présence de nombreuses cibles plus accessibles épargnait aux pirates la peine d'attaquer les systèmes protégés par deux facteurs, la situation a changé.

Il convient de noter que des maliciels de la même famille ont parfois servi à l'étranger et en Suisse pour attaquer des services financiers. Ils se sont propagés soit à l'aide de courriels rédigés différemment, soit par des infections de type *infection par «drive-by download»* (voir aussi chapitres 2.2, 2.4 et 5.1). Les pirates adaptent par conséquent leurs méthodes de *social engineering* au contexte régional.

Le chapitre 2.1 livre une appréciation des attaques de phishing et de maliciels, ainsi que sur la sécurité de l'authentification à deux facteurs. Des commentaires sur les incidents survenus en Suisse figurent également au chapitre 4.2.

La divulgation de données liée à l'espionnage industriel ou la perte de supports de données restent d'actualité: l'exemple de TJX

Les pertes de données sont le plus souvent dues à la perte ou au vol d'ordinateurs portables, de bandes de sauvegarde, de CD-ROM, de clés USB ou d'autres supports de sauvegarde. Le FBI lui-même a égaré 160 ordinateurs en quatre ans et n'était pas en mesure d'indiquer lesquels renfermaient des données confidentielles.[37] Comme signalé aux chapitres 2.2 et 2.3, toujours plus de pertes de données sont désormais dues à des attaques ciblées (*social engineering*) contre des collaborateurs, des serveurs Web ou d'autres systèmes.

---

[33] Un aperçu concret de la tactique figure sous: http://blogs.iss.net/archive/PhishingMicroscope.html (état au 18.07.2007).

[34] Voir: http://isc.sans.org/diary.html?storyid=2808; ou une interview avec un MySpace-Phisher: http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/ (état au 18.07.2007).

[35] Voir: http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html; http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html (état au 18.07.2007).

[36] Voir: http://www.ffiec.gov/press/pr101205.htm; http://www.ffiec.gov/press/pr081506.htm; ainsi que http://www.darkreading.com/document.asp?doc_id=129868&f_src=darkreading_default (état au 18.07.2007).

[37] Voir le rapport du département américain de la Justice: http://www.usdoj.gov/oig/reports/FBI/a0718/exec.htm (état au 19.07.2007).

Un exemple spectaculaire d'incident concerne TJX, entreprise de distribution basée aux Etats-Unis. Comme annoncé en début d'année, les informations contenues dans plus de 45 millions de cartes de crédit ont fait l'objet, depuis juillet 2005, d'un pillage systématique grâce à une faille des systèmes de paiement et de sauvegarde de cette société. L'intrusion n'a été décelée qu'en décembre 2006. L'enquête qui a suivi a révélé que les pirates avaient régulièrement accédé aux systèmes de TJX. Ce n'est qu'à partir de janvier 2007 qu'ils en ont été définitivement empêchés. Il s'agit à ce jour du plus grave vol de numéros de cartes de crédit. Aux dires des associations de banquiers, jusqu'à 30 % de la population de la Nouvelle-Angleterre pourrait être concernée. Un réseau criminel se servant des données subtilisées à TJX a manifestement déjà été arrêté en Floride. Les données des cartes de crédit étaient vendues par Internet, sur des sites spécialisés. Quant au préjudice subi par TJX, on sait seulement que l'enquête sur l'incident et les mesures de renforcement de la sécurité de l'information ont coûté 5 millions de dollars. TJX s'expose toutefois à des coûts sensiblement plus élevés, au vu des actions en cours, d'autant plus que les banques ont manifestement déjà compensé des dizaines de millions de dollars de pertes de leur clientèle. Le Wall Street Journal estime à près d'un milliard de dollars les coûts à long terme pour TJX. Les pirates ont manifestement tiré parti de réseaux locaux sans fil (WLAN) mal protégés, qui leur ont permis de lire les mots de passe, ainsi que de l'utilisation des logiciels d'espionnage.[38]

Comme indiqué au chapitre 2.3, la plupart des attaques lancées contre des entreprises ont aujourd'hui un caractère ciblé. En dehors de courriels habilement rédigés envoyés à des personnes clés et contenant soit un lien à un site infecté d'un *maliciel*, soit un maliciel dans leur annexe (voir chapitre 2.3), de nombreuses attaques visent les serveurs Web (voir chapitres 2.2 et 5.1) ou les réseaux locaux sans fil, comme dans le cas de TJX.

Il importe donc que les entreprises stockent leurs données sensibles sous forme cryptée (notamment sur les ordinateurs portables, les agendas électroniques (PDA), les clés USB, les CD-ROM ou les bandes de sauvegarde). La mésaventure de TJX montre qu'il faudrait également crypter les réseaux locaux sans fil (WLAN).

Marché noir et cybercriminalité: nouvelles tendances et prix en vigueur

La division du travail dans les milieux de la cybercriminalité a déjà été traitée dans le dernier rapport semestriel et ci-dessus, au chapitre 3.1. Quelques exemples récents serviront ici à montrer quelles prestations peuvent être ainsi obtenues, et à quel prix.

Au premier semestre 2007, une tendance a été constatée à l'usage des kits servant à la création de maliciels (*malware* kits), comme le montre l'exemple de MPack (voir chapitre 5.1). Cet outil, proposé avec un service d'assistance et des mises à jour régulières des *exploits*, se monnayait à l'origine 1000 dollars sur le marché noir russe, auprès d'un certain «$aSH».[39] Suite au succès rencontré, d'autres sources l'ont proposé à des prix sacrifiés.[40]

---

[38] Voir:
http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/;
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009300;
http://www.infoworld.com/article/07/03/29/HNtjxfiling_2.html ainsi que
http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html.
Un aperçu des vols de données aux Etats-Unis figure sous:
http://www.privacyrights.org/ar/ChronDataBreaches.htm (état au 19.07.2007).

[39] Une étude des milieux criminels russes figure sous: http://www.verisign.com/static/042139.pdf (état au 26.07.2007).

L'équipe de développement est apparemment composée de trois personnes, qui ont fait appel à $aSH comme directeur commercial. Les exploits du kit auraient fait l'objet d'échanges, certains ayant été conçus à partir de *lacunes de sécurité* connues et d'autres acquis au marché noir. Ce groupe est visiblement constitué de développeurs ayant un travail légal, qui ne se considèrent pas comme criminels mais développent et vendent des maliciels pendant leurs loisirs.[41]

Le maliciel utilisé pour l'attaque contre la banque suédoise Nordea, du nom de Haxdoor (voir la première contribution du chapitre 5.2) est disponible sur le marché noir. Un journaliste suédois s'est vu proposer pour 3000 dollars une version adaptée et non reconnue par les logiciels antivirus. Ce maliciel est visiblement l'œuvre d'un développeur agissant seul et se faisant appeler «Corpse», qui le commercialise personnellement – avec un service d'assistance et, au besoin, une zone pour le stockage en ligne sécurisé des données dérobées.[42]

Pratiquement tout ce qui est nécessaire à la cybercriminalité s'obtient sur le marché auprès d'«experts»: maliciels, exploits, informations sur les lacunes de sécurité, *réseaux de zombies* pour l'envoi de *pourriels* ou pour le chantage à l'attaque *DDoS*, hébergement sécurisé de maliciels ou de données obtenues illégalement.[43] Les prix sont facturés par unité de temps (une attaque DDoS coûtant de US$ 10 à 20 par heure), par serveur d'envoi de pourriels ou par pourriel expédié (10 000 000 pourriels par jour coûtant US$ 600), par compte d'accès Internet (US$ 50 par site d'affaires électroniques russe, US$ 7 par compte eBay ou PayPal) ou par carte (US$ 500 par numéro de carte de crédit avec PIN, US$ 25 sans PIN mais avec toutes les indications utiles aux affaires électroniques). Les *keylogger*s se négocient à partir d'US $40, un *cheval de Troie* pour quelques centaines ou milliers de dollars, selon son degré de complexité.[44] Il règne apparemment une forte concurrence sur ce marché.[45]

Un nombre croissant d'acteurs du domaine de la sécurité informatique cherchent désormais à mettre en place un marché légal des lacunes de sécurité et des exploits, soit en payant eux-mêmes à cet effet, soit en entretenant des plates-formes de vente aux enchères en

---

[40] Voir http://isc.sans.org/diary.html?storyid=3015; ainsi que http://www.theregister.co.uk/2007/07/06/pirate_mpack_toolkit/ (état au 24.07.2007).

[41] Voir l'entretien avec le développeur nommé DCT sur SecurityFocus: http://www.securityfocus.com/news/11476 (état au 24.07.2007).

[42] Voir les propos de «Corpse» parus sous: http://computersweden.idg.se/2.2683/1.93344 (état au 24.07.2007).

[43] Voir p. ex.: http://asert.arbornetworks.com/2007/04/botconomics-the-monetization-of-your-digital-assets/; http://www.networkworld.com/news/2007/050907-fbi-organized-crime-cybercrime.html; http://www.theregister.co.uk/2007/06/13/black_hat_list/ ainsi que http://www.washingtonpost.com/wp-dyn/content/article/2007/03/13/AR2007031301522.html (état au 24.07.2007).

[44] Chiffres tirés de: http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/04/23/Cybercrime_2E002E002E00_-for-sale-_2800_I_2900_.aspx; http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/03/Cybercrime_2E002E002E00_-for-sale-_2800_II_2900_.aspx; http://www.heise.de/security/news/meldung/82679; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025464&intsrc=industry_list (état au 24.07.2007).

[45] Voir p. ex. http://www.theregister.co.uk/2007/07/01/malware_gang_war/; http://www.viruslist.com/en/analysis?pubid=204791938#inet; http://www.darkreading.com/document.asp?doc_id=122116&WT.svl=news1_1 (état au 24.07.2007).

ligne[46]. On ignore cependant dans quelle mesure les acheteurs douteux peuvent être tenus à l'écart et une telle initiative permettra d'endiguer l'essor du marché noir.[47]

Le marché de la cybercriminalité, basé sur le principe de la division du travail, possède une organisation efficace. Il propose à toute personne intéressée des tâches conformes à ses connaissances et à son degré d'énergie criminelle. Tandis que des «experts» développent des maliciels, exploits, kits pour créer des programmes malveillants, etc., dont ils assurent généralement eux-mêmes la vente, d'autres s'en servent par exemple pour gérer des réseaux de zombies, pour dérober des données ou à des fins d'espionnage industriel. Un marché noir est également en place pour les données pillées.[48]

Autrement dit, les «experts» ont besoin pour leur travail de moins d'énergie criminelle que les acquéreurs de leurs produits, qui n'ont pas besoin de connaissances spécialisées. Ces derniers s'emparent ensuite de données, puis pillent les comptes ou commettent les vols d'identité, ou recrutent du personnel à cet effet.

Le chiffre d'affaires généré par la cybercriminalité est difficile à estimer – mais il s'agit indiscutablement d'un secteur lucratif, dont les risques demeurent jusqu'ici très faibles.[49]

[46] Voir p. ex.: http://www.wslabi.com/wabisabilabi/initPublishedBid.do? (état au 24.07.2007).
[47] Voir: http://www.economist.com/science/displaystory.cfm?story_id=9507422; http://www.theregister.co.uk/2007/01/25/bug_brokers_offering_higher_bouties/; http://www.securityfocus.com/news/11468 ainsi que le rapport d'un chercheur officiel sur ses expériences dans la vente des résultats de ses travaux: http://weis2007.econinfosec.org/papers/29.pdf (état au 24.07.2007).
[48] Voir p. ex.: http://blog.washingtonpost.com/securityfix/2007/03/stolen_identities_two_dollars.html; http://www.itseccity.de/content/virenwarnung/statistiken/070327_vir_sta_symantec.html (état au 25.07.2007).
[49] Voir p. ex.: http://www.vnunet.com/2189322, http://www.theregister.co.uk/2007/03/19/fbi_crime_report_2006/ ainsi que le rapport du FBI Internet Crime Complaint Center contenant les chiffres américains: http://www.fbi.gov/page2/march07/ic3031607.htm (état au 24.07.2007).

5.3 Terrorisme

Londres: attentat déjoué contre le réseau Internet

En mars dernier, Scotland Yard a révélé avoir découvert dès 2006 sur les disques durs de terroristes présumés, lors de perquisitions domiciliaires, des projets d'attaques terroristes visant le «London Internet Exchange» (LINX), principale plate-forme Internet de Grande-Bretagne.[50]

Selon les plans retrouvés, les suspects prévoyaient de s'introduire dans le quartier général de Telehouse Europe, situé à Telehouse Docklands, où se trouve physiquement une grande partie de LINX, pour y déposer une bombe et paralyser ainsi l'Internet britannique. Or même si les articles consacrés à cette affaire prétendent que les îles britanniques auraient été quasiment privées d'Internet, ce n'est nullement le cas. Car LINX exploite deux réseaux absolument indépendants, répartis entre sept sites géographiquement distincts. Une panne locale n'aurait donc pas eu les conséquences redoutées, même dans le cas du principal site, celui de Telehouse Docklands. De tels centres névralgiques sont d'ailleurs extrêmement bien protégés physiquement, ce qui laisse sceptique quant à l'issue d'un tel attentat.[51] Outre Internet, les autres cibles visées étaient des conduites de gaz, des entrepôts d'essence et des infrastructures de communication. Les projets n'en étaient toutefois qu'au stade initial.

Le plan découvert montre que les milieux terroristes s'intéressent toujours plus aux attaques contre les *infrastructures vitales (nationales)*. Mais comme indiqué dans les derniers rapports semestriels (notamment 2005/II), ils ne disposent pas (encore) du savoir-faire requis pour mener leurs attaques à l'aide des seules technologies de l'information. L'accent reste par conséquent mis sur les moyens conventionnels (y compris contre de telles cibles).

Outre le souci de faire un maximum de victimes et le caractère symbolique de la cible, le choix des objectifs semble désormais dicté par les dommages économiques potentiels.

[50] Voir: http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece; http://www.technologyreview.com/blog/garfinkel/17561/ ainsi que http://www.daniweb.com/blogs/entry1345.html (état au 25.07.2007).

[51] Voir: https://www.linx.net/pubtools/topology.html; http://en.wikipedia.org/wiki/London_Internet_Exchange; http://en.wikipedia.org/wiki/Telehouse (état au 25.07.2007).

6 Prévention

6.1 Thème-clé: infections par «drive-by download»

Le comportement individuel des utilisateurs est d'une importance décisive pour la sécurité des ordinateurs. La prudence est de mise avec les courriels ou les logiciels à télécharger. Chacun devrait en particulier se méfier s'il reçoit des factures électroniques d'entreprises, a fortiori s'il n'a jamais eu affaire à elles. De tels courriels sont conçus pour que le destinataire ouvre d'instinct l'annexe, sans se demander si un tel courriel fait sens. En l'occurrence, mieux vaut se méfier une fois de trop qu'une de pas assez. Or même en suivant scrupuleusement ces règles élémentaires de conduite, nul n'est à l'abri d'un incident.[52]

Les *infections par «drive-by download»* sont en effet toujours plus fréquentes. On entend par là l'intrusion d'un *maliciel* lors de la simple visite d'un site Internet. Depuis longtemps, contrairement à une opinion répandue, les sites louches (pornographie, jeu, etc.) ne sont plus seuls en cause. Tout utilisateur de moteur de recherche – soit presque chacun de nous – court des risques. Une enquête par échantillonnage portant sur les sites indexés par les moteurs de recherche a ainsi révélé que près de 10 % des sites provoquent des *infections par «drive-by download»* (voir aussi chapitre 2.2).[53] Ce nombre élevé tient à la tactique des pirates, qui commencent par s'emparer de serveurs Web entiers, en infectant tous les sites hébergés (voir chapitre 5.1). Au printemps dernier par exemple, un site consacré au hockey sur glace a été piraté et utilisé pour répandre des maliciels. Cet incident s'est produit le week-end même de la finale de coupe du monde de hockey sur glace. La méthode est d'une efficacité redoutable. Le typosquattage constitue une variante pour répandre des maliciels via des sites Web. Concrètement, les domaines enregistrés ont quasiment la même adresse qu'un site connu. Quiconque commet une faute de frappe dans l'adresse du site risque d'installer le maliciel sur son logiciel.

Déroulement de l'infection

Les navigateurs actuels sont configurés pour prévenir le téléchargement et le lancement automatique des fichiers. Une interaction est à chaque fois nécessaire, et l'utilisateur est d'ailleurs rendu attentif aux risques liés au téléchargement. Or les *infections par «drive-by download»* se produisent sans une telle interaction. Elles sont possibles parce que presque tous les logiciels utilisés comportent des *lacunes de sécurité*. Tant qu'elles n'ont pas été comblées, soit que le fabricant n'ait pas fourni de *patch*, soit que l'utilisateur ne l'ait pas encore installé, des sites ou documents spécialement préparés peuvent provoquer une infection. Le risque est spécialement élevé si la vulnérabilité concerne le navigateur ou d'autres programmes d'accès à Internet. A l'instar des *plugins* intégrés aux navigateurs, comme Movie Player (Flash, QuickTime, RealPlayer, Windows Media Player) ou d'Adobe Reader. Si le programme correspondant n'est pas entièrement à jour, l'internaute risque d'être infecté par maliciel sur un site spécialement préparé.

Au premier semestre 2007, un maliciel répandu par une carte de vœux a beaucoup fait parler de lui. Le courriel contenait un lien à une *adresse IP*. Si l'on cliquait sur ce lien, un

---

[52] Des règles de comportement figurent sous:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=fr (état au 20.08.2007).

[53] Voir: http://scmagazine.com/us/news/article/657903/google-450000-websites-launching-drive-by-attacks/ (état au 20.08.2007).

maliciel tentait de s'introduire sans l'intervention de l'utilisateur, en exploitant les lacunes de son navigateur. Divers *exploits* étaient testés à cette occasion, en fonction du navigateur. Si aucun d'entre eux ne convenait, une dernière tentative était faite pour amener l'utilisateur à installer manuellement le maliciel.

Le danger vient également des images, susceptibles de diffuser les exploits. Par exemple, si un fichier graphique spécialement préparé parvient à s'introduire dans le serveur d'une entreprise spécialisée dans la commercialisation de publicité sur le Web, des sites connus se mettront à leur tour à diffuser des maliciels. Par ailleurs, les plates-formes Web2.0 comme YouTube ou MySpace sont également très prisées pour l'installation de maliciels. En effet, les visiteurs y visionnent des films à l'aide des lecteurs multimédia susmentionnés, qui comportent souvent des lacunes de sécurité.

Mesures à prendre

L'une des principales mesures consiste à actualiser constamment son système d'exploitation et tous les programmes installés. Le temps qui s'écoule entre la publication du programme correctif et son installation est déterminant. Etant donné le professionnalisme des milieux cybercriminels et la division du travail rigoureusement appliquée, quelques heures suffisent désormais à la diffusion du premier exploit basé sur la lacune de sécurité à l'origine d'un programme correctif. On constate cependant que même les anciennes lacunes de sécurité sont très appréciées des criminels. A ce propos, un premier programme tout juste publié contrôle automatiquement si le système d'exploitation et les programmes sont à jour.[54] Les *0-day-Exploits* en circulation font toutefois que même un système entièrement à jour ne garantit pas une protection à 100 %.

Une possibilité de limiter les risques consiste à désactiver ActiveX dans Internet Explorer ou Javascript dans d'autres navigateurs, ou du moins à en restreindre l'utilisation. De nombreux sites requièrent toutefois ces composantes. MELANI a publié des instructions sur la manière de configurer ActiveX pour n'accepter que certains sites dignes de confiance.[55]

Tout utilisateur peut éviter des dommages, moyennant une attention accrue et une prise de conscience des dangers encourus. Si des dysfonctionnements sont constatés, la prudence est de mise. Ainsi le navigateur peut se bloquer, ou des fenêtres contextuelles apparaître lors de la visite d'un site. Le cas échéant, les collaborateurs devraient signaler le site en question à leur administrateur informatique. Une annonce à MELANI peut aider, car le site sera dûment analysé et éventuellement le fournisseur Internet prévenu de façon à éloigner le maliciel.

Une autre possibilité de réduire le risque dû aux infections par «drive-by download» consiste à créer sur l'ordinateur un compte spécial destiné à la navigation sur Internet (surf account). Ce compte sera paramétré de façon à limiter autant que possible les droits d'administration, et donc à prévenir l'exécution automatique de maliciels. Lorsqu'on travaille sans Internet, on passera à un compte dont les droits sont plus étendus.

Le risque que comportent les infections par «drive-by download» est évalué aux chapitres 2.2 et 2.4. Des exemples sont présentés au chapitre 5.1.

[54] Voir: http://secunia.com/software_inspector (état au 20.08.2007); seule la version bêta est disponible à ce jour.
[55] Voir: http://www.melani.admin.ch/themen/00166/00172/00176/index.html?lang=fr (état au 20.08.2007).

7 Activités / Informations

7.1 Collectivités publiques

Suisse : MELANI poursuivra son activité

Le 24 janvier, le Conseil fédéral a décidé que la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) poursuivrait ses activités. La centrale MELANI est opérationnelle depuis le 1er octobre 2004 ; elle a pour tâche de protéger les *infrastructures vitales* de notre pays, en particulier quand ces dernières dépendent du bon fonctionnement des infrastructures d'information et de communication.

Le Conseil fédéral a pris sa décision sur la base d'une évaluation menée par l'EPF de Zurich. Les résultats de cette étude sont fondés sur des enquêtes auprès des gestionnaires d'infrastructures vitales pour l'économie suisse, auprès de services comparables à l'étranger, et auprès des services de la Confédération. L'étude évalue très positivement le degré d'efficacité et d'opportunité des activités de MELANI.[56]

UE : renforcement de la collaboration dans le domaine de la sécurité intérieure

Au premier semestre 2007, l'Union européenne a intensifié la collaboration dans le domaine de la sécurité intérieure. Sous la présidence allemande, le Conseil de l'UE a renforcé les compétences opérationnelles d'Europol, ainsi que les échanges d'information au niveau européen. Les points suivants méritent concrètement d'être mentionnés :

Le renforcement opérationnel d'Europol est devenu une réalité à l'entrée en vigueur des protocoles modifiant la convention Europol. A l'avenir, les agents d'Europol pourront participer à des groupes d'enquête communs aux Etats membres. En outre, dans l'optique d'améliorer les échanges d'information, d'autres autorités des Etats membres que le point central national auront un accès direct au système d'information d'Europol. Par ailleurs, des experts provenant d'Etats tiers pourront directement coopérer avec Europol, au sein d'un groupe d'analyse. Ce dernier point revêt une importance particulière pour la coopération entre l'UE et les Etats-Unis dans le domaine de la lutte contre le terrorisme. Enfin, l'intégration prévue de la convention Europol dans le cadre institutionnel de l'UE doit étendre le mandat d'Europol à toutes les formes de criminalité grave ayant une dimension transfrontière.[57]

Europol est également appelé à jouer un rôle central dans la surveillance d'Internet. Ainsi, un portail d'information créé au sein d'Europol centralisera les observations ou analyses des Etats membres concernant l'utilisation d'Internet à des fins d'activités terroristes. Ce projet

[56] Voir http://www.isb.admin.ch/aktuell/medieninfo/00126/index.html?lang=fr&msg-id=10361 (état au 10.8.07).
[57] Voir: http://www.bmi.bund.de/cln_012/nn_175818/Internet/Content/Nachrichten/Pressemitteilungen/2007/04/JI__Rat__Europol__DE.html; http://www.heise.de/newsticker/meldung/88599 (état au 10.8.07).

de surveillance appelé «Check the Web» a officiellement démarré au début de mai. Des réunions d'experts ont régulièrement lieu dans ce cadre.[58]

La Commission européenne aimerait élaborer un cadre politique cohérent à l'échelle internationale, afin d'améliorer la coordination de la lutte contre la cybercriminalité. En mai, elle a adopté la communication «Vers une politique générale en matière de lutte contre la cybercriminalité». Ce document souligne notamment la nécessité de renforcer le dialogue entre le secteur public et l'économie privée.[59]

Etats-Unis : alors que la sécurité informatique reste un défi pour le Département de la sécurité intérieure (DHS), l'armée cherche à contrôler le cyberespace

Le département américain de la sécurité intérieure (Department of Homeland Security, DHS) est entre autres chargé de la cybersécurité aux Etats-Unis. Il a attendu septembre 2006 pour désigner un responsable de la cybersécurité afin de mieux protéger les Etats-Unis contre les cyberattaques.[60] Le DHS continue d'ailleurs à être critiqué pour ses mesures de sécurité internes inadéquates et pour l'insuffisance de ses contrôles dans le domaine de la sûreté de l'information. En juin dernier, l'organisme de contrôle de l'action gouvernementale américaine (Government Accountability Office, GAO) a déploré une nouvelle fois, dans un rapport destiné au Congrès, les problèmes du DHS au niveau de la sûreté de l'information. Le GAO a laissé entendre que des progrès avaient été réalisés, mais qu'il reste de «graves lacunes» et qu'ainsi des menaces pèsent sur la confidentialité des informations, l'intégrité des systèmes du DHS et leur accessibilité.[61]

En même temps, les Etats-Unis prennent très au sérieux l'importance militaire de leur cyberespace. C'est ainsi que l'armée de l'air américaine a créé une nouvelle unité appelée «Cyber Command». Ce centre de cyber commandement vise notamment à contrôler le cyberespace et à améliorer les capacités de mener la guerre dans le cyberespace. Les Etats-Unis sont en effet convaincus qu'avec la terre, la mer et les airs, la maîtrise de ce nouveau champ de bataille et la supériorité au niveau de l'information sont devenus indispensables pour remporter une guerre.[62]

Divers autres Etats se sont déjà dotés de capacités militaires dans le cyberespace. Les efforts d'armement consentis par la Chine sur ce plan motivent concrètement les Etats-Unis à vouloir garantir la supériorité américaine dans le domaine de l'information.[63]

Le chapitre 5.1 traite des questions soulevées par les attaques lancées à l'aide de moyens informatiques et donne des informations sur la cyberattaque d'avril 2006 contre l'Estonie.

---

[58] http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2007/05/Check__the__web.html; http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=fr (chapitre 7.1) (état au 10.8.07).

[59] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:FR:PDF (état au 10.8.07).

[60] Voir le rapport semestriel MELANI 2006/2, chapitre 7: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=fr (état au 10.08.2007).

[61] Voir http://www.gao.gov/new.items/d071003t.pdf; http://homeland.house.gov/hearings/index.asp?ID=65 (état au 10.8.07).

[62] Voir www.af.mil; http://www.heise.de/newsticker/meldung/91131 (état au 10.8.07).

[63] Voir l'évaluation des capacités militaires de la Chine faite par le ministère américain de la Défense: http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf (état au 10.08.2007).

7.2 Secteur privé

Suisse : blocage d'accès aux sites de pornographie enfantine

Dans le cadre d'un projet commun à la Prévention suisse de la criminalité (PSC), au service spécialisé «ECPAT Switzerland» de l'Association suisse pour la protection de l'enfant et au Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI), les fournisseurs suisses d'accès à Internet ont été invités à bloquer spontanément les sites qui commercialisent des contenus à caractère pédophile. Entre-temps, une large majorité des intéressés ont accepté de collaborer au projet et le blocage de certains sites est déjà actif. Le but est de mettre un terme à toute consommation de pédopornographie et de dissuader les amateurs par une intervention étatique concrète.

L'action de blocage est dirigée contre les fournisseurs de contenus Internet relevant de la pornographie enfantine à l'étranger. L'Office fédéral de la police (fedpol) établit et complète régulièrement la liste des sites à bloquer. Cette liste est enregistrée dans un filtre. Si un internaute cherche à consulter l'un de ces sites, il est renvoyé à une page de mise en garde. Une partie des adresses de pornographie enfantine ont été reprises, moyennant les clarifications juridiques requises, des autorités scandinaves qui utilisent déjà de tels filtres. Les autres proviennent des investigations du SCOCI.

En 2007, la pornographie reste le principal motif des communications au Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI). L'action de blocage des sites vise à endiguer la demande de pornographie enfantine et, par là, à protéger de nouvelles victimes potentielles.

8 Bases légales

Nouvelle législation suisse en matière de pourriels

Depuis le 1er avril 2007, l'envoi de pourriels (spams) est interdit en Suisse. Le publipostage de masse par voie de télécommunication n'est plus autorisé que sous certaines conditions. Selon la loi fédérale contre la concurrence déloyale, la publicité de masse n'ayant aucun lien direct avec une information demandée doit en principe satisfaire aux trois conditions suivantes :

1. la publicité de masse doit être envoyée avec le consentement du destinataire (modèle opt-in) ;

2. l'adresse de l'expéditeur doit être correcte ;

3. le destinataire doit avoir la possibilité de refuser gratuitement le document publicitaire.

Exception : une personne qui communique son adresse à l'occasion d'un achat et qui est alors informée des possibilités de refus peut recevoir de la publicité de la part du vendeur. Si la publicité de masse envoyée par voie de télécommunication ne remplit pas ces critères, il s'agit de pourriels et de concurrence déloyale.

Si l'analyse de l'expéditeur d'un pourriel (*adresse IP*) révèle qu'il s'agit d'un fournisseur d'accès suisse, vous pouvez l'informer de l'envoi des spams par l'intermédiaire de son service clients. Une fois qu'ils en ont été informés, les fournisseurs d'accès sont tenus d'empêcher que leurs clients n'envoient ou ne transfèrent des spams.

L'envoi de spams est punissable lorsqu'il est fait intentionnellement. L'élément constitutif du caractère intentionnel repose dans le fait que l'action est commise en connaissance de cause. S'il s'agit d'un spam, en d'autres termes d'une publicité illicite envoyée intentionnellement, en lien avec la Suisse, vous avez alors la possibilité de déposer une plainte contre l'expéditeur auprès d'un poste de police local. C'est à vous d'estimer si le dommage justifie une éventuelle poursuite pénale. L'envoi de spams est un délit poursuivi sur plainte et la poursuite pénale relève des cantons.

Le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) a mis au point un formulaire d'analyse en matière de spams, solution simple pour suggérer la provenance d'un pourriel.[64] Chacun peut ainsi savoir s'il a été envoyé depuis la Suisse ou s'il a été transféré et, si c'est le cas, par l'intermédiaire de quel fournisseur d'accès (fournisseur Internet). Pour qu'il soit possible d'analyser un pourriel, il est nécessaire d'en connaître l'en-tête. Les explications nécessaires figurent au même endroit.

La nouvelle législation est toutefois sans effet contre les pourriels envoyés de l'étranger en Suisse. Et comme la plupart des pourriels proviennent de l'étranger, la situation ne devrait guère s'améliorer dans les boîtes aux lettres électroniques suisses.[65]

[64] Voir: http://www.cybercrime.ch/spamanalyse/spam_fr.php#spam (état au 20.08.2007).

[65] http://www.bakom.admin.ch/dienstleistungen/info/00542/00886/index.html?lang=fr (état au 20.08.2007).

Allemagne : perquisitions en ligne

Internet est un moyen de communication toujours plus prisé, y compris des criminels ou des personnes qui pourraient mettre en danger la sécurité publique. D'où de vives discussions, en Suisse comme dans toute l'Europe, pour savoir jusqu'où l'Etat peut aller en matière de surveillance d'Internet et des ordinateurs. A ce propos, il convient de distinguer entre les recherches effectuées sans soupçon concret et la surveillance exercée dans le cadre d'une poursuite pénale.

En Allemagne, la Cour constitutionnelle de Karlsruhe a décidé, le 5 février 2007, que les perquisitions secrètes en ligne par la police sont illégales, faute de base juridique explicite. La Cour a expliqué que le code de procédure pénale ne légitimait pas une telle méthode de recherche. En effet, les prescriptions sur les perquisitions ne peuvent être invoquées pour justifier des perquisitions en ligne, qui ne sont pas non plus comparables aux autres mesures d'enquête que sont la surveillance téléphonique ou la surveillance de domicile. Le Ministère fédéral de l'intérieur a annoncé qu'il adapterait la législation en vigueur. Dans le contexte de la lutte contre le terrorisme, il mise en effet sur l'élargissement des méthodes de recherche aux médias électroniques. Le contrôle d'Internet et des systèmes informatiques est à ses yeux nécessaire dans la mesure où les terroristes utilisent toujours plus ce moyen de communication moderne.

Dans le cadre de leurs enquêtes, les autorités policières de certains Länder allemands peuvent déjà depuis longtemps se procurer des informations en perquisitionnant les systèmes informatiques.

En Suisse, les perquisitions en ligne de systèmes informatiques ne sont pas autorisées pour le moment, en l'absence de présomption sérieuse. Le nouveau projet de loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) permet bien, sous certaines conditions très strictes, d'accéder aux ordinateurs. Mais le projet n'en est qu'au stade des délibérations parlementaires. L'emploi de logiciels espions peut toutefois être autorisé dans le cadre de la poursuite pénale. La loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) ainsi que différents codes de procédure pénale peuvent servir de base juridique dans ce contexte.

Plusieurs anciens rapports semestriels MELANI évaluent l'usage fait d'Internet par les terroristes (éditions 2006/2, 2006/1 et surtout 2005/2, à chaque fois au chapitre 5.4).

9 Statistique

Saturation de la demande de nouvelles connexions en Suisse

L'Office fédéral de la statistique (OFS) a publié au premier semestre 2007 une étude consacrée à l'utilisation d'Internet dans les ménages suisses. Les résultats de l'enquête de 2004 montrent que 71 % des ménages disposent d'un ordinateur et que 61 % ont un accès à Internet. La Suisse se classe ainsi en cinquième position en comparaison internationale. Selon la même étude, l'accès à Internet continue de se diffuser au sein des ménages,

quoiqu'à un rythme moins élevé qu'à la fin des années 1990 et qu'au début des années 2000. Un cinquième des ménages du pays ne souhaite pas de connexion ou n'en a pas l'utilité. On doit donc envisager une saturation de la demande de nouvelles connexions dans un proche avenir. Les autres raisons invoquées pour la non utilisation d'Internet à domicile sont le manque de compétence, le coût trop élevé ainsi que le fait de disposer d'un accès ailleurs.[66]

La crainte de problèmes de sécurité des données et la protection de la vie privée ne jouent qu'un rôle marginal dans les raisons ne pas être connecté, puisque moins de 1 % de l'ensemble des ménages mentionnent ces arguments.

Les entreprises suisses pratiquement toutes reliées par Internet

L'informatique et Internet ne cessent de gagner en importance au sein des entreprises suisses, notamment dans les petites et moyennes entreprises (PME). Bénéficiant de connexions aussi étendues que les grandes entreprises, elles recourent de plus en plus à des prestations en ligne spécifiques. Comme l'a révélé une étude réalisée du 5 au 25 février 2007 par l'institut de recherche gfs.bern, le taux de notoriété le plus élevé parmi les administrations publiques a été attribué aux sites cantonaux. Cette étude, commandée par le secrétariat d'Etat à l'économie (SECO) et par la Chancellerie fédérale, portait sur 1050 entreprises.[67]

91 % des personnes interrogées dans des entreprises de plus de 10 employés ont un accès direct à Internet depuis leur poste de travail. Dans les micro-entreprises, 63 % des collaborateurs utilisent quotidiennement Internet, ce pourcentage dépassant 71 % dans les entreprises de taille plus importante. 72 % des sondés jugent important, voire fondamental, de pouvoir disposer d'un compte de messagerie et 76 % estiment particulièrement important que les collaborateurs puissent bénéficier de services mobiles comme un téléphone portable, un smartphone ou un agenda électronique PDA.

Même les PME ne peuvent plus se permettre de négliger la protection de leurs infrastructures d'information, laquelle revêt une importance croissante. MELANI a commandé une étude consacrée à la sécurité informatique dans les entreprises suisses. Il s'avère qu'une panne de plusieurs jours déjà peut menacer la survie d'une entreprise.[68]

[66] http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/22/publ.html?publicationID=2487 (état au 20.08.2007).
[67] http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=fr&msg-id=12087 (état au 20.08.2007).
[68] http://www.melani.admin.ch/dokumentation/00123/00125/index.html?lang=fr (état au 20.08.2007).

10 Glossaire

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

0-day-Exploit	*Exploit* paraissant le jour même où une *lacune de sécurité* est rendue publique.
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
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 DoS	Attaque par déni de service (denial of service). Vise à rendre impossible l'accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs.
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.)
Bot / Malicious Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (malicious bots) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
Cheval de Troie	Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.
Defacement	Défiguration de sites Web.
DNS	Domain Name System 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).
Exploit Code	(Exploit). Programme, script ou ligne de code utilisant les lacunes de systèmes informatiques.

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.
Infrastructures vitales (nationales)	Infrastructure ou pan de l'économie dont la panne ou l'endommagement aurait un impact majeur sur la sécurité nationale ou sur le bien-être économique et social d'une nation. En Suisse, les infrastructures critiques comprennent l'approvisionnement en énergie et en eau, les services de secours et de sauvetage, les télécommunications, les transports, les banques et les assurances, le gouvernement et les administrations publiques. A l'ère de l'information, leur fonctionnement dépend de plus en plus du soutien de systèmes d'information et de communication, appelés infrastructure d'information critique.
Jeton	Composante informatique créant un facteur d'authentification (voir *authentification à deux facteurs*) (p. ex. carte à puce, jeton USB, identifiant sécurisé, etc.).
Keylogger	Appareil ou programme intercalé entre l'ordinateur et le clavier qui permet d'enregistrer toute saisie au clavier.
Lacunes de sécurité	Aussi faille de sécurité. Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Malware (Maliciel)	Maliciel. Le terme anglais « malware » est la contraction de « malicious » et de « software ». Voir malicious code.
MITM	Man-in-the-Middle attack, attaque de l'intermédiaire. Attaque où le pirate s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
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.
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.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage

	(spamming).
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.
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.