



CLUSIF

Panorama 2008 de la Cybercriminalité

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1	Présentation
2	Introduction du panorama
3	Web 2.0 et Réseaux Sociaux : les menaces se précisent
4	Sécurité hardware et confiance sur Internet
5	La criminalité organisée et le numérique
6	Effets d'annonce et failles de sécurité non exploitées : quelle est la réalité de la menace ?
7	Du sabotage interne aux atteintes de sécurité sur les infrastructures
8	Conclusion
9	Pour aller plus loin

1 Présentation

Le CLUSIF (Club de la Sécurité de l'Information Français) est une association sans but lucratif créée en 1980 qui regroupe près de 600 membres, professionnels de la sécurité de l'information. Chaque année, le CLUSIF revient sur les événements marquants de l'année passée. Ce document résume le panorama qui a été présenté le 15 janvier 2009 à Paris.

2 Introduction du panorama 2008

Par M. Pascal Lointier - Conseiller Sécurité de l'Information - AIG Europe



2.1 Présentation du CLUSIF

Depuis 8 ans, le CLUSIF présente un panorama de la cybercriminalité qui permet de revenir sur des faits réels en matière de délits numériques.

De nombreux acteurs issus de différents horizons (entreprises & autorités de pays comme la France ou le Québec) participent au CLUSIF qui est un espace d'échanges pour les responsables de la sécurité informatique. Une des grandes spécificités de ce club est de proposer gracieusement au grand public, des documents traduits dans différentes langues.

A noter qu'en 2008, des groupes de travail sur la PCI-DSS (Payment Card Industry Data Security Standard) ainsi que sur la sécurité des applications web ont été créés.

2.2 Retour sur le panorama 2007

Le panorama 2007 évoquait déjà les risques liés aux mondes virtuels. En 2008, ceux-ci ont d'ailleurs largement été confirmés. Pour preuve, des faits d'actualité y relatifs très représentatifs ont été relatés par la presse spécialisée.

Le premier concernait une femme arrêtée par la police pour avoir supprimé de manière illicite le personnage de son mari « virtuel » qui avait demandé le divorce dans un jeu sur Internet.

Le deuxième cas répertorié était celui d'un divorce demandé par une femme trompée « virtuellement » par son mari.

Les prévisions du CLUSIF concernant les volontés de perturber ou déstabiliser des personnes se sont révélées exactes dans les domaines :

- des attaques en réputation : une vidéo du président de la fédération internationale de l'automobile dans une « orgie nazie » a ainsi été divulguée,
- du hacking pour attirer l'attention : modification des permis d'abattage dans les forêts brésiliennes,
- de l'espionnage industriel : un cadre de Michelin aurait cherché à vendre des informations à Bridgestone,
- des risques liés aux réseaux sociaux : Megan, adolescente de 13 ans, se suicide après sa rupture avec « Josh Evans », rencontré sur MySpace. Celui-ci s'est en fait révélé être Lori Drew, une mère de famille de 49 ans qui voulait venger sa fille dont Megan avait rejeté l'amitié,

- les attaques se sont sophistiquées, avec notamment une prolifération des attaques par iframe et des botnets de plus en plus efficaces,
- le e-commerce est devenu un vaste terrain de jeu pour les malfaiteurs qui ont multiplié les fraudes à la carte bancaire,
- des « cyber-guerres » ont été lancées, on peut citer par exemple les infrastructures SCADA mises à mal puisque le réseau téléphonique de la FEMA a été piraté.

3 Web 2.0 et Réseaux Sociaux : les menaces se précisent

Par M. François PAGET - Chercheur de Menaces - McAfee Avert Labs



Le Web 2.0 est généralement décrit comme un vaste réseau social où les internautes sont des acteurs qui interagissent entre eux.

Tous les réseaux sociaux fonctionnent de manière similaire :

- Un utilisateur est amené à s'inscrire et saisit un certain nombre d'informations personnelles,
- Il peut ensuite inviter ses « amis » à s'inscrire sur le réseau, ou s'ils le sont déjà, à rejoindre son cercle « virtuel » d'amis.

Il est essentiel de comprendre que toutes les informations publiées (textes, mais aussi vidéos et images) peuvent être vues par les « amis », voire par tous les utilisateurs d'Internet si le paramétrage du partage n'est pas correctement configuré.

Les menaces qui n'existaient que sous forme d'e-mails utilisent à présent les réseaux sociaux. Ainsi, les « Arnaques nigérianes » sont dorénavant envoyées dans les messageries de ces réseaux. Le spam envahit ces mes-

sageries car les adresses des utilisateurs sont très souvent publiques.

De plus, certains malwares n'hésitent pas à utiliser de tels réseaux pour se propager (le ver Koobface sur Facebook par exemple), tandis que les failles XSS (Cross Site Scripting) qui permettent à un attaquant de voler la session de l'utilisateur par exemple, sont légion. Les utilisateurs « font confiance » à leur réseau social et à toutes les applications qui s'y rattachent. Ainsi, une application preuve de concept a été créée afin de montrer que les réseaux sociaux pouvaient servir de support pour un réseau « botnet ». Cette application a été découverte et installée par de nombreux utilisateurs malgré l'absence de publicité faite autour elle...

L'application « Preuve de concept »

Le social engineering est une technique de manipulation de la personne. Elle vise à obtenir l'accès à des informations confidentielles ou à des ressources à accès restreint et est facilitée par les réseaux sociaux. En effet, de nombreuses informations utilisables pour une attaque d'ingénierie sociale sont accessibles grâce au réseautage. De même, les atteintes à la réputation sont facilitées par ce biais : il suffit de lancer une rumeur, de publier vidéos et photos pour que tous les contacts de la personne ciblée soient très vite au courant (voir l'exemple du président de la FIA et sa vidéo, cité précédemment).

Un autre risque inhérent à ces réseaux provient du fait que de nombreux jeunes croient être en contact avec des personnes de leur âge, alors qu'en fait il s'agit d'adultes qui cherchent à les abuser. En effet, comment être certain de l'identité de son interlocuteur sur Internet ? On peut notamment parler ici des profils sur les réseaux tels que Facebook, Twitter, etc. Il faut savoir que de nombreuses personnalités (dont un membre de la famille royale de Mohammed VI) ont vu leur profil être « usurpé ».

Enfin, peu de personnes ont conscience qu'Internet est en fait un réseau mondial sur lequel les informations publiées seront « à tout jamais » publiques. De fait, l'on peut citer le cas de salariés dénigrant leur entreprise sur Internet et licenciés peu après, tel cet employé de Michelin en mars 2008.

The screenshot shows the Facebook homepage layout. At the top is the Facebook logo and navigation links. Below is a green 'Inscription' button and a tagline: 'Facebook vous permet de rester en contact et d'échanger avec les personnes qui vous entourent.' The main content area features a 'Photo of the Day' section with a large yellow smiley face image. To the right of the image is a call to action: 'Inscrivez-vous à cette application et connectez-vous avec vos amis.' with another 'Inscription' button. Below this is a section titled 'À propos de cette application' showing a 3.2 star rating from 10 reviews, 91 active users per month, and the category 'Juste pour le plaisir'. At the bottom, it says 'Cette application n'a pas été développée par Facebook.' and 'À propos des développeurs' with a profile picture for 'Andreas'.

4 Sécurité hardware et confiance sur Internet

Par M. Franck VEYSSET - Expert Senior - Orange Labs



Nombreux sont les pirates qui n'hésitent plus à « bricoler » des ordinateurs, des lecteurs de cartes à puce, etc. afin d'exécuter leurs forfaits.

La technologie RFID (Radio Frequency IDentification), de plus en plus utilisée dans la vie quotidienne, (elle sert par exemple dans les cartes d'abonnement de transport en commun et les nouveaux passeports), est également l'objet de « reconfigurations ».

L'objet « tagué » RFID (c'est-à-dire identifié par un système RFID) est équipé d'une antenne ainsi que d'une mémoire de taille réduite (une puce). Une des spécificités de cette technologie est qu'elle est alimentée par les ondes radio émises par le lecteur.

Les données présentes sur les objets RFID sont cryptées. En effet, il ne faut pas qu'elles soient modifiables (sinon les usagers des transports en commun utilisant des cartes équipées par des RFID n'auraient plus besoin de payer pour recharger leurs cartes par exemple) ni consultables librement (pour des soucis de données personnelles qui doivent rester confidentielles). Les algorithmes utilisés pour crypter ces données ne sont pas publics. Cependant, beaucoup ont déjà été « cassés » (ce qui veut dire que quelqu'un a découvert comment ils fonctionnent et peut décrypter les informations protégées).

Dans ce contexte, des pirates n'hésitent plus à fabriquer de faux passeports. En effet, quelques pays ont équipé certains de leurs documents d'identité avec des puces RFID. Evidemment, les informations stockées sur ces passeports sont cryp-

tées sinon il serait possible de les recopier / modifier. Ainsi, les pays doivent s'échanger les informations pour décrypter les données afin de vérifier l'identité des personnes possédant les passeports lors des contrôles. En octobre 2008, à peine 10 pays sur 50 ont accepté d'échanger de telles données, et seulement 5 les ont effectivement partagées. Alors, comment peut-on être sûr des informations d'un passeport ?

Un autre exemple de piratage « physique » est le refroidissement de la mémoire « volatile » (comme la mémoire vive RAM) des ordinateurs pour en extraire les données. En effet, les données restent en mémoire beaucoup plus longtemps si le support est refroidi. Ainsi, on peut extraire celles qui sont présentes dans la mémoire d'un ordinateur en veille « active » (ou allumé, ou éteint depuis peu) On peut donc très souvent espérer trouver des clés de chiffrement, des mots de passe, etc. La manière la plus simple de se protéger de ce genre d'attaque est de toujours éteindre son ordinateur quelques minutes avant de s'en éloigner.

(Source : <http://citp.princeton.edu/memory/medical/>)



La confiance que les gens placent en Internet est mise à rude épreuve. Citons par exemple, le cas de BGP (Border Gateway Protocol), protocole utilisé par la majorité des fournisseurs d'accès pour définir des routes entre leurs serveurs. Il existe sur Internet environ 30 000 systèmes autonomes (AS) qui échangent des informations, ceci est rendu possible grâce à BGP qui permet la collaboration entre ces systèmes. Ainsi, chacun d'eux connaît des routes et les échange avec ses voisins, ce qui permet en général à toutes ces machines de pouvoir communiquer entre elles. Toutefois, ce système est basé sur la confiance, ce qui peut créer certains soucis. Par exemple, en février 2008 le Pakistan a repéré un contenu offensant sur You-

tube. Le pays a émis une note à tous ses ISPs afin qu'ils bloquent le site au Pakistan. Cependant une personne a commis une erreur de paramétrage et en l'espace de quelques minutes, grâce au protocole BGP, Youtube est devenu inaccessible pour le monde entier. Toutes les requêtes sur ce serveur ont été redirigées vers le Pakistan, car la « route » définie par eux était « prioritaire ». Il s'agissait d'un problème technique dû à une manipulation hasardeuse mais on peut imaginer les nombreux dénis de service basés sur ces systèmes qui pourraient voir le jour. De même, on peut « forcer » tout le trafic vers un site à passer par un serveur prédéterminé (en déclarant une « meilleure route ») et donc filtrer toutes les requêtes vers ce site !

Un autre exemple d'insécurité possible est la fonction de hachage MD5. En 2004, certaines attaques ont permis de démontrer que cette fonction était « faible ». En décembre 2008, une équipe de chercheurs a présenté le fruit de ses travaux en ce sens. Elle souhaitait réussir à fabriquer un faux certificat HTTPS et le faire signer par une autorité de certification. Grâce à des failles liées au MD5 (qui a servi à la fabrication de ce certificat), ils ont pu générer un second certificat HTTPS, également valide et signé alors que l'autorité de certification n'en n'avait même pas eu connaissance. Potentiellement, ceci démontre que des attaques de phishing peuvent être menées sur des sites web sécurisés en HTTPS. Il est donc primordial que les autorités de certification abandonnent MD5 pour utiliser dès lors SHA-1 (plus sécurisé que MD5) et se tournent vers SHA-3 dès qu'il sera finalisé.

5 .La criminalité organisée et le numérique

Par le Lieutenant-colonel **Éric FREYSSINET** - Chargé des projets cybercriminalité - Direction générale de la gendarmerie nationale / Sous-direction de la police judiciaire



CONTREFAÇON :

La contrefaçon est omniprésente sur Internet. On pense bien sûr à celle qui touche de plein fouet les logiciels mais il ne faut pas oublier que la contrefaçon « matérielle » y est également particulièrement développée. On peut ainsi se procurer très facilement des objets contrefaits en quelques clics : médicaments, logiciels, cigarettes, chaussures de sport, etc. La contrefaçon est un sujet d'actualité depuis les débats sur la loi « Créations et Internet » en France et chez ses équivalents un peu partout dans le monde.

Prenons comme exemple les cas de faux antivirus auxquels chacun a été confronté, un jour ou l'autre. Une fenêtre apparaît sur l'ordinateur (le plus souvent lorsque vous êtes en train de surfer) et vous explique qu'un virus a été détecté sur votre ordinateur.



Cette fenêtre vous propose alors d'installer une solution pour pallier ce problème. Bien entendu, les utilisateurs apeurés par le message installent très souvent le logiciel qui, évidemment, n'est pas un vrai antivirus. L'installation est gratuite mais, bien entendu, votre numéro de carte bancaire est très vite requis... De plus, une fois le numéro obtenu, le compte sera débité plusieurs fois et les fenêtres intempestives ne s'arrêteront pas pour autant !

Un autre cas répertorié est celui d'une fabrique chinoise qui a revendu aux Etats-Unis et au Canada du faux matériel CISCO. A cette occasion, du matériel contrefait a été saisi pour la somme de 76 millions de dollars. Un des soucis majeurs est que ce sont des marchands réputés de confiance qui ont vendu ces objets. On peut ainsi s'interroger : que se passerait-il si de nombreux produits informatiques contrefaits se retrouvaient comme composants dans les réseaux informatiques? Comment peut-on être sûrs que les appareils contrefaits n'espionnent pas le trafic ?

HEBERGEMENT ILLICITE :

Sous couvert de la « liberté d'expression », un grand nombre d'hébergeurs que l'on pourrait qualifier de « malhonnêtes » a vu le jour. Le plus connu d'entre eux est certainement le Russian Business Network (RBN), en partie démantelé en 2007. Ces réseaux servent à héberger des contrôleurs de botnets (qui permettent de contrôler la totalité des ordinateurs du botnet), du contenu illégal (pédophilie, pédopornographie, fichiers protégés par les droits d'auteurs, phishing, etc.) et permettent ainsi aux criminels de continuer leurs actions « en toute impunité ». Heureusement, certains acteurs du net se mobilisent pour fermer ce genre de réseaux en enquêtant et en les dénonçant aux autorités compétentes. C'est notamment grâce à eux qu'Atrivo -également connu sous le nom d'*Interpage*- qui était un réseau hébergeant principalement du contenu illicite, a été fermé. Un autre hébergeur de ce type, McColo, a également été démantelé. Un journaliste a mené une enquête sur les services proposés par cet hébergeur et a mis à jour des anomalies évidentes, telles des étrangetés concernant l'adresse postale : à l'aide de GoogleStreetView, l'adresse de McColo

montrait un simple magasin... Les fournisseurs d'accès Internet d'Atrivo ont fini par lui couper l'accès et c'est à ce moment précis que l'on a pu constater une baisse du Spam au niveau mondial de l'ordre de 50-60% ! En parallèle, les transactions bancaires frauduleuses ont été réduites, bien que les banques n'aient pas officiellement confirmé cet état de fait. Malheureusement, d'autres hébergeurs ont aujourd'hui pris la place d'Atrivo... C'est pourquoi, afin de persévérer dans la voie de ces succès manifestes, une collaboration entre la police, la justice et les professionnels tels que les ISPs serait extrêmement souhaitable.

FRAUDE AU JEU :

Les jeux, tels les fausses loteries, sont en nette recrudescence depuis 2008. Rappelons que, dans ce contexte, pour recevoir son ou ses lots il est illégalement demandé au « gagnant » de s'acquitter d'une certaine somme... Certains professionnels, tels Microsoft ou Yahoo!, ont donc mis en ligne un système permettant de dénoncer ces fraudes. Au Luxembourg, la plateforme <http://www.lisa-stopline.lu> permet ainsi de signaler tout contenu illicite. En France, il est possible de faire la même chose sur <https://www.internet-signalement.gouv.fr>. En Allemagne, on peut s'adresser à l'Office Fédéral pour la sécurité des technologies de l'information : <http://www.bsi.bund.de>

MALWARES :

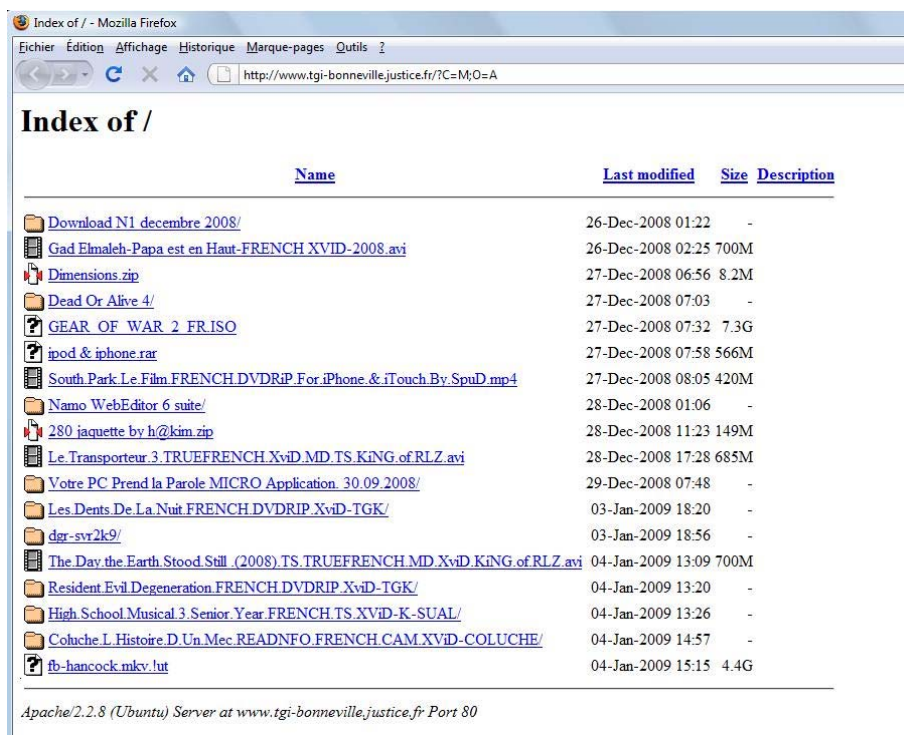
Un nouveau type de malware attaque les téléphones portables et se propage par Bluetooth et/ou MMS. Au moment de sa première exécution, il pratique le chantage en demandant à sa victime de payer une certaine somme, si elle ne s'exécute pas, le malware bloquera le téléphone pour le rendre « inutilisable ». Pour l'heure, ces malwares sont écrits et se propagent principalement en Chine, mais il y a fort à parier qu'ils seront vite traduits et contamineront de ce fait à d'autres pays. Ils se présentent sous la forme de kit (ils sont donc très simples à mettre en œuvre) et fonctionnent sur Symbian OS (système d'exploitation très utilisé sur les téléphones mobiles en Europe).

Cependant, les cibles des criminels ne sont pas toujours celles que l'on croit ! On peut citer l'exemple du botnet « Loads.cc » dont les « distributeurs » ont été attaqués par... des concurrents, grâce à une attaque de déni de service ! Il suffit en effet de 80 dollars pour attaquer n'importe qui au moment choisi ! Pour le moment, ce genre de « services » spéciaux sont utilisés dans l'underground mais qui sait ce qui pourrait se passer lorsqu'ils se généraliseront ? Il est en effet très tentant d'attaquer les systèmes d'un concurrent pour « faire monter » son propre marché.

Enfin, certaines personnes, à priori innocentes, se retrouvent devant les tribunaux pour avoir hébergé du contenu illicite ou pour s'être introduites illégalement dans d'autres systèmes informatiques que les leurs. Le plus souvent, ces personnes font partie d'un botnet mais ne s'en sont pas rendu compte. Leur image et leur réputation peuvent donc être atteintes (une descente de police visible du voisinage n'est jamais du meilleur effet...) ; si cela met en cause une société (dans le cadre d'affaires sensibles telles que des images pédopornographiques) elle peut très bien ne jamais s'en relever. Ainsi, le tribunal de grande instance de Bonneville en France, qui à cause d'une erreur technique a été redirigé vers la page Internet personnelle d'un citoyen (voir ci-dessous), a subi un préjudice certain en terme d'image. A ce jour, le message expliquant ce fait est toujours visible en page d'accueil du site du tribunal :



La page du TGI de Bonneville aujourd'hui



La page affichée lorsqu'un internaute tentait d'accéder à l'URL du TGI (Source : PCINpact)

6 Effets d'annonce et failles de sécurité non exploitées : quelle est la réalité de la menace ?

Par M. Hervé SCHAUER - Consultant en sécurité des systèmes d'information - Hervé Schauer Consultants



En 2008, de nombreuses failles ont fait parler d'elles dans les médias quand, lorsqu'elles ont été découvertes, la fin d'Internet a été annoncée (à tort). D'autres par contre sont quasiment passées inaperçues alors que leurs effets se sont révélés être bien plus nuisibles.

En juin 2008, une faille sur le DNS a été découverte. Le DNS (Domain Name System) permet de faire correspondre une adresse IP (xx.yy.zz) avec le nom complet qu'il faut entrer pour afficher une adresse web. Cette faille révèle un vrai problème conceptuel dans le fonctionnement du DNS (problème similaire à celui de BGP évoqué par F. Veysset). Cette vulnérabilité peut être illustrée de la manière suivante :

- un internaute souhaite accéder au serveur web www.site-web.lu.
- un attaquant utilise son serveur DNS malveillant afin de lui répondre plus rapidement que le serveur DNS légitime
- il est donc possible de faire croire à l'internaute que le site de l'attaquant est le « vrai ». N'importe quel site Internet, même le plus malveillant, peut passer pour un site totalement légitime, surtout lorsque cette technique est couplée à des attaques de phishing.

Cependant, Dan Kaminsky (le découvreur de cette faille) a attiré l'attention de tous sur l'importance de mettre à jour ses ordinateurs et serveurs mais sans en indiquer immédiatement la raison (ceci pour faire sa propre promotion lors de la présentation de cette faille en août 2008 à la conférence de sécurité Black Hat), néanmoins une erreur a fait que la faille a été révélée dès le mois de juillet. Les médias ont alors rapidement relayé l'information en se basant sur les propos du découvreur tout en exagérant les faits et les conséquences. On pouvait alors lire sur les unes de journaux : *c'est très grave, Internet va s'effondrer...* Aujourd'hui, les médias en parlent encore et M. Kaminsky est toujours à la « une ». Au final, le problème est réel mais est surtout l'affaire des fournisseurs d'accès Internet et des administrateurs réseaux...

Un cas similaire de « buzz » médiatique portait sur une faille concernant le TCP (Transmission Control Protocol). De faux avis ont même été édités, affirmant que la même faille touchait SNMP – Simple Network Management Protocol - (révélant une faille connue depuis longtemps). De même, les médias ont évoqué un « lundi noir des virus »...et il ne s'est rien passé. Des chercheurs ont montré que le MD5 pouvait être cassé par des PlayStation 3 ; en fait, les chiffres annoncés pour les performances de cette attaque étaient exagérés, néanmoins ceci prouve la puissance de la machine qui peut porter de telles attaques.

Par ailleurs, il est possible que des failles ne soient pas relayées à leur juste niveau. Par exemple, la majorité des sociétés utilisent les cartes Mifare Classic (RFID) pour sécuriser leurs accès physiques. Néanmoins, si l'une de ces cartes venait à être clonée, un étranger à la société pourrait entrer dans des locaux protégés ! Il faudrait alors changer les cartes d'accès de tout le personnel... Mais qui fait cela, et qui même le prévoit ?

Il existe une faille qui permet de réaliser de faux certificats HTTPS signés par une autorité de certification. Ainsi, tous les utilisateurs surfant sur le site web « protégé » par ce certificat voient bien dans leur navigateur Internet le

logo d'un cadenas signalant que le site est sécurisé et « digne de confiance »...et pourtant, il n'en est rien.

Enfin, il faut parler des failles Microsoft qui sont souvent relayées dans la presse comme étant toutes du même niveau de menace. Cependant, la faille décrite dans l'avis MS08-67 est loin d'être anodine. Qui a entendu parler de cette vulnérabilité qui permet une exploitation à distance de tous les systèmes Windows (jusqu'à la version 2003 serveur SP2 incluse) ? Et pourtant, aujourd'hui il existe toujours des malwares qui l'utilisent.

De manière générale, il faut savoir que les failles « côté client », celles qui ont le pouvoir d'impacter les ordinateurs des internautes, sont bien plus dangereuses que celles « côtés serveur », impactant les serveurs qui régissent Internet. En effet, les postes clients sont plus nombreux et sont donc autant de cibles potentielles pour les pirates. Il est nécessaire de sensibiliser sur ces failles car le plus dur reste d'apprendre aux Internautes à rester vigilants et à ne pas se faire piéger...

A ce titre, la presse est un acteur majeur dans le monde de la sécurité de l'information. Aujourd'hui, il existe pléthore de très bons articles rédigés par des journalistes bien informés, participant aux campagnes de sensibilisation ciblant le grand public. De nos jours il est essentiel de lutter contre la crédulité et le manque de connaissances des utilisateurs de NTIC. Ce faisant, on peut informer la population des réels problèmes de sécurité auxquels ils peuvent être confrontés. Les médias peuvent ainsi efficacement servir de vecteur de sensibilisation. De fait Il est très important que chacun soit conscient qu'il est essentiel d'utiliser avec prudence et en toute connaissance de cause son ordinateur, tant à son bureau qu'à son domicile.

7 Du sabotage interne aux atteintes de sécurité sur les infrastructures

Par M. Pascal LOINTIER - Conseiller Sécurité de l'Information - AIG Europe



2008 a connu de nombreux « cas d'école » en matière de sabotage informatique. Tout d'abord, il y a eu le licenciement d'un salarié, administrateur du réseau de la mairie de St-Francisco, qui avait notamment accès à des routeurs « stratégiques » gérant 50% des données de la ville. Avant son départ forcé, il a configuré sur ces routeurs un mot de passe administrateur pour son accès exclusif. Par la suite, il n'a jamais voulu révéler ce mot de passe (même après une procédure judiciaire) et la mairie a dû faire appel à des experts pour résoudre ce délicat problème. Ceci prouve qu'il faut s'entourer de précautions en ce qui concerne les personnes occupant un poste « stratégique », tels les administrateurs réseau de l'entreprise.

Une autre affaire de licenciement a porté sur un administrateur réseau ayant considéré insatisfaisantes les négociations de son départ. Il a donc menacé son entreprise de procéder à une attaque sur ses systèmes puis de divulguer ce fait aux médias. Les machines de l'entreprise ont dû être arrêtées afin de pouvoir trouver les portes dérobées « backdoors ». De nouveaux systèmes ont été installés et les accès à distance ont dû être coupés... Bien sûr, tout cela n'a pas été inutile mais ces actions ont été réalisées dans

l'urgence, avec tous les risques que cela comporte.

La chaîne de supermarchés Hannaford a également connu les affres du piratage. 300 de ses serveurs ont été compromis par la divulgation de 4.2 millions de références bancaires (numéro des cartes et dates d'expiration). Les coûts engendrés par ces incidents ont été très élevés : 100 000 cartes réémises, une « class-action » lancée pour réclamer 5 millions de dollars de dommages et intérêts et installation d'un système de monitoring 24h/24 et 7 jours/7. Suite à cette affaire, un processus de révision de PCI-DSS (Payment Card Industry Data Security Standard) a été initié dans le cadre d'une amélioration continue de la norme.

Des données « perdues » peuvent aussi être le début d'affaires de rançon. En Allemagne, des journalistes sont entrés en contact avec des criminels qui leur ont proposé 21 millions de données personnelles en échange de 12 millions d'euros. Pour preuve de leur « bonne foi », les criminels ont fourni un CD contenant plus d'un million d'informations.

La compagnie Express Scripts quant à elle, a été victime d'un problème avec ses systèmes, ce qui a permis à un criminel de récupérer 75 de ses dossiers. Celui-ci a entamé des négociations officieuses mais la société était prête à payer 1 million de dollars pour toute aide apportée permettant d'arrêter le criminel...Là aussi, les coûts de sécurisation se sont avérés très élevés : de nombreux frais pour corriger les failles plus le recours à une société spécialisée en investigation...

Des événements accidentels peuvent également être considérés comme graves par l'opinion publique alors qu'il n'en est (apparemment) rien. Par exemple des câbles sous-marins ont été coupés au Qatar, en Inde...quasiment au même moment, ce qui pu faire penser à une attaque « coordonnée » et a relancé les débats sur la théorie du complot. Cependant, les statistiques sur les ruptures de ces câbles ont démontré que ce n'était pas le cas et que les chiffres ne sortaient pas de la normale.

Les hôpitaux non plus n'ont pas été épargnés par les problèmes liés aux technologies de l'information. Ainsi, en novembre 2008, 3 hôpitaux de Londres ont dû éteindre leurs ordinateurs pendant au moins 3 jours à cause d'un virus dont la souche initiale datait de 2005. Il n'y aurait pas eu de conséquences sur les malades hospitalisés...

De même, un développeur a introduit une « bombe logique » (un malware) dans un programme de formation médicale et l'a activé plus tard dans tous les hôpitaux munis de ce logiciel.

Dans un hôpital militaire, après installation d'un client peer-to-peer, un fichier contenant des données concernant un millier de personnes a été rendu visible. C'est une société de datamining qui a prévenu l'hôpital qui ne s'était rendu compte de rien.

Pour finir, en Pologne, un enfant de 14 ans a cherché à comprendre comment fonctionnait la signalisation lumineuse du tramway ainsi que son système d'aiguillage. Pour ce faire il a fabriqué une télécommande dans le but de modifier la signalisation existante. Il n'avait pas de mauvaises intentions mais au final il a tout de même blessé 12 personnes. Que se passerait-il si un criminel réalisait des « expériences » identiques !!!?

Le tramway en Pologne après le déraillement

(Source :

<http://storage.canalblog.com/06/60/13/8145/21066336.jpeg>)

8 Conclusion

Le panorama 2008 du CLUSIF a permis de revenir et d'insister sur les failles présentes dans les systèmes d'informations. Il est très important de sensibiliser le public sur ce sujet encore et toujours d'actualité car un grand nombre d'incidents pourraient, de fait, être évités.

Aussi n'hésitez pas à consulter très régulièrement le site de CASES (www.cases.lu) afin de rester informés sur tout ce qui touche à la sécurité de l'information.

9 Pour aller plus loin

Vous trouverez ci-dessous des références permettant d'approfondir les sujets abordés dans ce dossier.

La présentation du CLUSIF dans sa totalité est disponible sur le site officiel :

<http://www.clusif.asso.fr/fr/infos/event/#conf090115>



Concernant le RFID, consulter le site d'Adam Laurie: <http://rfidiot.org/>. C'est un acteur très connu du monde de la sécurité qui vous expliquera notamment comment cloner des cartes RFID.

Pour la copie de la mémoire vive grâce au refroidissement, visiter le site de Jacob Appelbaum <http://www.appelbaum.net/> avec notamment un lien vers ses recherches sur la question <http://citp.princeton.edu/memory/>.

A propos de la lutte contre les « ISP complaisants », le CERT-IST a publié un article contenant de nombreuses sources sur http://www.cert-ist.com/fra/ressources/Publications_Articles/Bulletins/Environnementreseau/McColo/

Pour le « cassage » des MD5, le lien ci-dessous démontre que cela n'était pas possible avec les chiffres annoncés :

<http://sid.rstack.org/blog/index.php/282-casser-du-md5-avec-classe-ou-pas>

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu