1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée. L'objectif est de retracer les événements marquants de 2010 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Dans un premier temps, nous examinons au chapitre 2 les principales attaques survenues au cours de l'année.

Ensuite au chapitre 3, nous analysons plus largement l'évolution des technologies et identifions les domaines pour lesquels la sécurité est une préoccupation croissante.

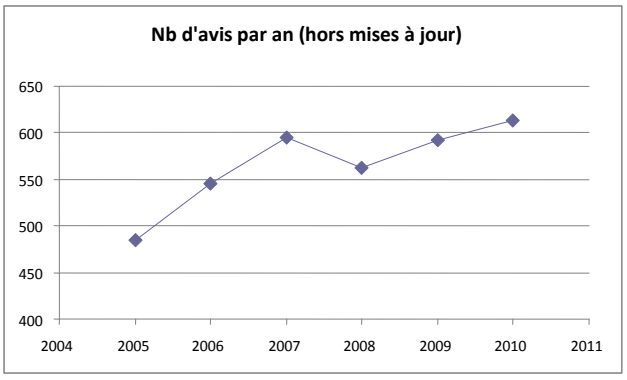
2) Les attaques vues en 2010

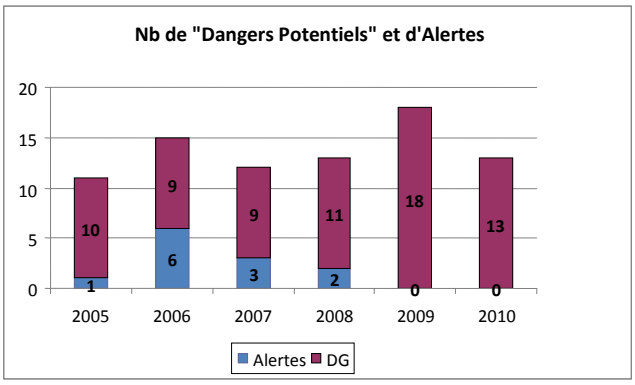
2.1 Quelques chiffres clés

Le Cert-IST publie tout au long de l'année des messages adressés aux structures opérationnelles de ses adhérents, afin de les informer sur les attaques potentielles, et leurs proposer des actions de protection pour y faire face. Ainsi, en 2010, le Cert-IST a émis :

- **613 avis de sécurité**. Ces avis décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis ont été suivis de façon continue et ont donné lieu au cours de l'année à 1798 mises à jour mineures et 82 mises à jour majeures (ces dernières correspondent typiquement au cas où des programmes d'attaque -des "exploits"- ont été publiés). Le nombre d'avis est en augmentation par rapport à 2009 (cf. la courbe). Microsoft participe pour une grande part à cette augmentation puisque 2010 est une année record, avec 106 bulletins de sécurité émis par Microsoft.

- **13 Dangers Potentiels et 0 Alerte**. Les Dangers Potentiels décrivent des menaces significatives mais non encore imminentes (ou d'une gravité modérée) pour lesquelles le Cert-IST recommande des mesures de protection spécifiques. Les Alertes sont utilisées pour les menaces majeures nécessitant un traitement prioritaire. En 2010, le nombre de Dangers Potentiels est en retrait par rapport à 2009 (cf. l'histogramme ci-dessous), et revient à une valeur comparable aux années antérieures. Tout comme pour 2009, il n'y a pas eu en 2010 d'Alerte. La dernière Alerte reste donc celle émise fin 2008 pour le ver Conficker. Globalement, la menace se maintient, mais les attaques généralisées (du type Conficker) pour lesquelles le Cert-IST émet des alertes ne se produisent plus. Nous analysons plus en détail au chapitre suivant la nature des menaces traitées en 2010.





Nota : De nouveaux produits sont ajoutés au fur et à mesure des besoins de ses adhérents. Au 31/12/2010 le Cert-IST suivait les vulnérabilités concernant 996 produits et 8216 versions de produits.

2.2 La nature des menaces

Les 13 Dangers Potentiels émis par le Cert-IST en 2010 correspondent tous à des attaques qui visent le poste de travail de l'utilisateur. Ceci confirme et accentue une tendance déjà mise en avant en 2009 (nous avions observé en 2009 que 70% des attaques visaient le poste de travail et 30% les équipements d'infrastructure).

La menace principale à laquelle les entreprises sont confrontées, est donc l'attaque visant l'utilisateur. Le scénario type d'attaque consiste à attirer l'utilisateur sur un site web piégé afin d'infecter son poste de travail automatiquement dès son arrivée sur le site (attaque baptisé "drive-by download", c'est-à-dire téléchargement "en passant"). Pour cela, le pirate peut :

- soit envoyer à l'utilisateur un email l'incitant à visiter un site web piégé. Il peut également attirer sa victime par d'autres moyens, comme un message Twitter, un commentaire sur un blog, etc… (attaque directe),
- soit infecter des sites web légitimes mal protégés et en modifier le contenu de façon invisible pour attaquer ensuite les visiteurs (attaque indirecte),
- soit même insérer une publicité piégée au milieu des annonces publicitaires légitimes gérées par une régie publicitaire. La publicité piégée est ensuite diffusée (involontairement) sur les sites web ayant vendu de l'espace à la régie publicitaire et attaque finalement les internautes visitant ces sites web (attaque doublement indirecte).

Ces scénarios sont connus depuis plusieurs années, et ont été détaillés dans notre bilan 2009. Ils constituent la phase préliminaire à l'attaque elle-même, qui consiste à envoyer un code d'attaque exploitant une vulnérabilité dans un des logiciels présents sur le poste de la victime. Le tableau ci-dessous donne le détail des nouvelles vulnérabilités découvertes en 2010 pour lesquelles le Cert-IST a émis un message "Danger Potentiel" (parce que le risque d'attaque au moyen de cette vulnérabilité était grand. On remarque que :

- Pour la seconde année de suite les vulnérabilités PDF et Flash sont en tête de ce classement. Cette catégorie accentue son avance puisqu'elle représente maintenant 46% (au lieu de 31% en 2009)
- Microsoft Office, ou les ActiveX n'apparaissent plus dans ce classement 2010, mais Internet Explorer reste lui présent.

Nombre de "Dangers Potentiels" émis par le Cert-IST en 2010 (classés par type de vulnérabilité)	
Attaques lors de la navigation web	
- Attaques contre PDF (Adobe Reader) ou Flash (Adobe Flash Player)	6 (46%)
- Autres attaques web (QuickTime, Centre d'aide Windows, sites web piégés)	3 (23%)
- Attaques contre Internet Explorer	2 (15,5%)
Attaques visant Windows - hors navigation web (.lnk/stuxnet et dll hijacking)	**2** (15,5%)

Les vulnérabilités que nous décrivons ici correspondent à de nouvelles attaques apparues en 2010. Elles s'ajoutent en fait à la panoplie des attaques dont disposent les pirates, et en particulier aux "Exploit-kits" (outil pirate tout-en-un spécialement conçu pour attaquer leurs visiteurs au moyen d'un ensemble d'attaques pré-enregistrées). Les Exploit-kits sont apparus en fin 2006 (Mpack est le premier exemple connu) et se sont largement développés depuis : Eleonore, Fragus, NeoSploit sont des exemples d'exploit-kit contemporains.

3) Les phénomènes marquants de 2010

Au-delà des vulnérabilités identifiées quotidiennement (telles que présentées au chapitre 2) le Cert-IST analyse également les tendances, et l'évolution globale de la sécurité informatique. Ce chapitre présente les phénomènes les plus marquants de 2010 :

- Les attaques par infiltration : APT (Advanced Persistent Threat)
- Stuxnet et la sécurité SCADA
- iPhone, Android ou Phone7 : une mutation des usages de la téléphonie mobile
- Cloud computing
- Renforcement du cadre législatif
- Botnets : attaques et ripostes se succèdent

3.1 Les attaques par infiltration : APT (Advanced Persistent Threat)

Le terme anglo-saxon de « APT » existe depuis au moins 2007, mais est devenu vraiment populaire à partir de 2010. Il est utilisé pour désigner les attaques informatiques par infiltration qui consistent à :

- Infecter un composant interne du système d'information,
- Rester invisible et survivre le plus longtemps possible sur le système infecté,
- Effectuer des actions malveillantes, le plus souvent en étant téléguidé par un attaquant distant.

Ce qui différencie une APT d'une attaque classique (par exemple l'infection par un botnet) c'est que dans le cas de l'APT l'attaque a souvent un caractère « stratégique » et vise explicitement une entreprise particulière. L'attaque informatique n'est donc pas une fin en soit, elle n'est qu'un moyen pour l'attaquant de s'infiltrer dans l'organisation pour ensuite mener une action offensive dans un but précis, par exemple l'espionnage industriel.

Deux attaques ont particulièrement marqué l'année de 2010 du fait d'une forte médiatisation :

- En janvier 2010 l'affaire « **Aurora** ». Google avait alors annoncé publiquement avoir subi une attaque provenant de Chine (infiltration au sein de son système d'information). Plus d'une vingtaine d'autres sociétés américaines (dont Adobe et Juniper Network) ont ensuite confirmé avoir été également visées. Les pirates auraient utilisé des fichiers PDF piégés, ou des vulnérabilités dans Internet Explorer 6, pour infecter le poste de travail de certains employés ciblés des sociétés visées.

- En juillet 2010 le ver « **Stuxnet** » visant les systèmes industriels (SCADA) est découvert. Ce ver a été conçu pour se propager d'ordinateur en ordinateur jusqu'à atteindre des postes utilisés pour piloter des équipements industriels. Il semblerait (mais cela est difficilement vérifiable) que Stuxnet ait été conçu par le gouvernement Israélien pour détruire des équipements d'enrichissement nucléaire iraniens.

Ce type d'attaque ciblée, à caractère d'espionnage industriel, ne date pas de 2010. Des exemples (moins médiatisés et sans doute moins sophistiqués) existent depuis très longtemps (voir par exemple en 2004 l'affaire Titan rain à propos d'attaques supposées chinoises contre des sites militaires américains, ou l'affaire Michaël Haephrati qui a mis en évidence l'utilisation de chevaux de Troie pour l'espionnage industriel). D'ailleurs, en juillet 2005, nous avons consacré l'éditorial de notre bulletin mensuel à ce sujet. Mais la médiatisation faite en 2010 pour ces attaques APT montre que désormais ces cyber-attaques font partie de l'arsenal standard pour attaquer un compétiteur.

3.2 Stuxnet et la sécurité SCADA

Stuxnet, que nous venons de citer, a eu pour second effet de mettre en évidence un risque que l'on considérait jusque là simplement comme un risque théorique : l'attaque d'une installation industrielle au moyen d'un virus informatique.

Au-delà des spéculations sur les auteurs de Stuxnet et leurs intentions (s'agit-il d'une cyber-arme pour détruire des centrifugeuses nucléaires iraniennes ?), le phénomène Stuxnet est avant tout inquiétant à deux titres :

- Tout d'abord, il montre que les systèmes industriels doivent se préparer à faire face à des attaques informatiques, et que ces attaques peuvent être très sophistiquées et spécifiquement conçues pour toucher des environnements critiques.

- Ensuite, il montre que même les sites industriels qui estiment ne pas être des cibles potentielles sont concernés. En effet, Stuxnet visait sans doute une cible unique, mais il a aussi infecté par "effet collatéral" près de 100 000 autres machines. Il est conçu pour reconnaitre sa cible et déclencher sa charge active uniquement sur celle-ci. Mais peut-on être sûr de la fiabilité de ce mécanisme ?

Stuxnet est indubitablement un événement majeur pour le monde de l'informatique industrielle (souvent appelé par commodité « monde SCADA »). C'est un révélateur d'une menace latente que les entreprises connaissaient déjà mais qu'il devient urgent de traiter. Il donnera sans aucun doute un coup d'accélérateur aux travaux de sécurisation déjà en cours sur ces infrastructures.

Nota : Depuis début 2010, le Cert-IST a intégré à son domaine d'activité la surveillance des menaces pouvant impacter le monde SCADA.

3.3 iPhone, Android ou Phone7 : une mutation des usages de la téléphonie mobile

- **Les attaques actuelles sont majoritairement des tentatives d'escroquerie**

Depuis quelques années, avec la généralisation de l'usage de la téléphonie mobile, on redoute que les attaques qui touchent déjà les systèmes d'informations classiques (virus, botnet, spam) n'atteignent également les téléphones mobiles. Jusqu'à présent cette menace ne s'est pas réalisée, ou en tout cas pas à une échelle suffisamment large pour constituer un problème majeur. Plusieurs raisons sont le plus souvent avancées pour expliquer ce constat :

- Les systèmes d'exploitation des téléphones mobiles sont hétérogènes : au moins 5 OS différents existent sur ce marché, et pour un même OS, le code développé pour une version donnée n'est pas toujours compatibles avec les autres versions de l'OS. Cette segmentation du marché rend donc difficile la conception d'un code d'attaque universel susceptible de créer des attaques de grande ampleur.

- Les pirates ne sont pas forcement intéressés à créer des attaques de grande ampleur car les motivations ont évolué. Il vaut mieux réaliser de petites attaques discrètes et en tirer un bénéfice, plutôt que de lancer de grandes attaques juste pour perturber le fonctionnement des infrastructures.

En 2010, on a continué à voir une activité malveillante montrant que ce risque d'attaque visant la téléphonie mobile existe toujours. Par exemple le premier cas de « botnets » visant Android a été découvert en décembre 2010 (Cheval de Troie "Geinimi"). Les exemples d'escroqueries ponctuelles

(visant à générer des appels vers des numéros surtaxés) restent également nombreux (voir cet exemple visant Windows Mobile en avril 2010).

- **Les nouveaux usages induisent un risque nouveau**

Plus que ces attaques conventionnelles, 2010 marque selon nous un changement significatif des usages. Ce changement est dû à la démocratisation des smartphones (typiquement iPhone, Blackberry, Android) :

- Il s'agit de terminaux multi-fonctions (téléphone, agenda électronique, terminal Internet) sur lesquels l'utilisateur peut installer des applications tierces (téléchargées sur des portails spécialisés comme l'Apple Store, ou l'Android Market).
- Ils sont souvent utilisés par des utilisateurs connectés en permanence sur Internet, par exemple via des applications comme Twitter et Facebook

En fait la frontière entre le monde de l'entreprise et la vie privée est de plus en plus difficile à identifier pour ces utilisateurs :

- Le téléphone est utilisé pour des usages professionnels aussi bien que personnels. Il n'est même pas rare que l'employé décide d'acheter son propre terminal et de l'utiliser aussi pour un usage professionnel (plutôt que d'utiliser un terminal fourni par l'entreprise)
- Il a un accès direct à Internet (via un abonnement « data »), qui ne passe pas forcement par les infrastructures de l'entreprise. Afin d'avoir un accès universel à ses données (aussi bien personnelles que professionnelles) où qu'ils soient (à l'intérieur ou à l'extérieur de l'entreprise) certains utilisateurs seront même tentés de mettre sur Internet des données professionnelles (par exemple son carnet d'adresse ou son agenda sous Google).
- L'utilisateur installe des applications tierces sans précautions : l'offre d'applications gratuites est importante et l'utilisateur n'a pas conscience que ces applications peuvent être malveillantes.

Il en résulte un risque significatif que le smartphone devienne :

- une source de fuite de données pour l'entreprise,
- et un vecteur d'attaque privilégié pour les attaques ciblées.

Ce constat est renforcé par le fait que lorsque des failles de sécurité sont découvertes, la mise à jour des OS des smartphones reste une opération délicate (il ne s'agit pas d'une opération de routine), et aussi parce que l'entreprise dispose d'un parc d'appareils souvent hétérogènes.

Pour l'ensemble de ces problèmes, 2010 est une année frontière. Il apparait désormais indispensable que les entreprises analysent ces nouveaux risques et étudient les solutions pour la mise en place d'une politique de sécurité adaptée à la gestion de flotte d'équipements mobiles. Consciente de cette évolution, l'ENISA (Agence Européenne pour le Sécurité des systèmes d'informations) a publié fin 2010 un guide sur les risques induits par les smartphones. Elle y attire l'attention des entreprises sur la nécessité de gérer la flotte des smartphones (et par exemple de prévoir des procédures d'effacement des données) et de protéger l'entreprise contre les fuites de données.

3.4 Cloud computing

Le "cloud" est resté très présent dans l'actualité marketing tout au long de l'année 2010. Le Gartner a d'ailleurs indiqué en septembre dans son rapport annuel sur les technologies émergeantes que le "cloud" avait atteint son pic en termes d'espoirs suscités (les attentes) et qu'il faudrait maintenant plusieurs années pour qu'il soit réellement adopté. Si le "cloud" génère autant d'intérêt, c'est parce qu'il est vu par les Directions Informatiques et les Directions Générales comme une opportunité pour réduire les coûts.

Au cours de 2010, le paysage du "cloud" s'est quelque peu précisé et les domaines les plus susceptibles de se concrétiser sont :

- Le cloud "privé" : il s'agit ici d'une infrastructure technique strictement interne à l'entreprise qui permet d'accueillir les applications de l'entreprise sur des plates-formes virtuelles réparties. Cette offre est aujourd'hui encore du domaine du concept (les offres sont naissantes). Elle peut être vue comme un prolongement des travaux déjà réalisés ces dernières années dans le domaine de la virtualisation. Les problèmes de sécurité dans ce cas restent limités à l'intérieur de l'entreprise, ce qui diminue grandement les risques.

- Le SaaS (Software as a Service) : il s'agit ici du cas où un fournisseur propose des applications accessibles à l'entreprise via Internet. Ce domaine est en pleine explosion et les fournisseurs proposant des solutions SaaS se multiplient. Il s'agit d'applications pour l'entreprise (par exemple pour la gestion de la relation client avec le CRM de SalesForce.com, ou pour le travail collaboratif avec des solutions de conférence-web ou d'espaces de stockage partagés) ou même le grand public (avec des offres gratuites comme GoogleDoc ou Microsoft Skydrive). L'offre ici est nombreuse et très attractive. Elle présente de réels risques de sécurité pour l'entreprise si son utilisation n'est pas encadrée et guidée.

Le déploiement anarchique de solutions SaaS est un risque réel pour l'entreprise parce que, comme pour les smartphones et les réseaux sociaux, ces offres sont fortement attractives pour l'utilisateur. Il peut par exemple être tenté d'utiliser l'environnement bureautique gratuit proposé par GoogleDoc pour travailler sur des documents avec des partenaires, ou les solutions de stockage "en ligne" gratuites (comme Dropbox) pour accéder à ses données professionnelles depuis n'importe où (depuis son téléphone mobile, depuis son domicile, depuis son bureau). Les risques de sécurité sont pourtant multiples: fuites de données, bien sûr, mais aussi la perte de contrôle pour l'entreprise sur ces données stockées "dans le cloud". Par exemple :

- à qui appartient un document créé par un collaborateur sur un service "cloud" gratuit ? : au fournisseur du service, à l'utilisateur ou à l'entreprise ?
- ou comment l'entreprise peut-elle récupérer ces documents si l'utilisateur quitte l'entreprise ou est absent ?
- ou encore, peut-on faire une analyse à posteriori d'un système de "cloud" victime d'une attaque ?

On le voit, la politique de sécurité de l'entreprise peut être battue en brèche par une utilisation non structurée de ce type de solutions, et l'absence éventuelle de recours légaux (qui est responsable en cas de problème ?).

En termes d'incidents de sécurité, nous avons noté au cours de 2010, plusieurs incidents affectant les solutions "cloud" (voir ci-dessous). Aucun de ces incidents n'est pour le moment réellement préoccupant. Ils montrent avant tout que les pirates aussi s'intéressent au "cloud" et qu'ils sont en train d'en explorer les possibilités :

- Les créateurs de codes malveillants conçoivent des méthodes leurs permettant de contourner les protections antivirales basées sur le cloud (voir par exemple cet article : Bohu, premier virus Cloud officiel),

- La puissance de calcul des solutions "cloud" peut être exploitée aussi à des fins malveillantes : par exemple pour le cassage des mots de passe (voir par exemple cet article : GPUs crack passwords in the cloud), ou pour réaliser des attaques DOS (Amazon Cloud DoS attacking ITSPs),

- Même un service "cloud" n'est pas à l'abri de pannes (voir par exemple cet article à propos de l'indisponibilité pendant plusieurs jours du service de Hotmail de Microsoft : Hotmail Data Loss Reveals Cloud Trust Issues).

3.5 Renforcement du cadre législatif

L'année 2010 marque un renforcement des aspects légaux dans le domaine de la SSI, et plus particulièrement dans celui de la protection des données personnelles. En effet, le projet de loi Détraigne et Escoffier (déposé fin 2009), qui propose de rendre obligatoire la fonction de CIL (Correspondant Informatique et Liberté) et la déclaration des incidents de sécurité (s'ils concernent des données nominatives), a provoqué beaucoup d'interrogations. S'il n'est pas sûr que cette proposition soit adoptée par l'Assemblée Nationale, il est probable que cette obligation de déclaration des incidents arrivera un jour ou l'autre dans le Droit français. En effet, elle existe déjà dans le Droit européen pour les opérateurs de Télécom (cf. le « Paquet Télécom » qui a été adopté par la CE en novembre 2009) et la communauté européenne envisage d'étendre cette obligation aux autres secteurs du marché.

Cette obligation a des conséquences importantes pour toutes les entreprises (puisque toutes, exploitent ou hébergent des fichiers clients et autres données nominatives) et il faut donc s'y préparer.

Ce renforcement législatif nous semble en fait un prolongement naturel des efforts fait au cours de la dernière décennie dans le domaine réglementaire (la loi Sarbanes-Oxley date de 2002) et plus récemment dans le domaine normatif (ISO-27001 par exemple).

3.6 Botnets : attaques et ripostes se succèdent

Depuis plusieurs années déjà la lutte contre les cyber-criminels s'organise. Dans notre bilan 2008 déjà nous mentionnions les actions entreprises pour faire fermer des hébergeurs complaisants (McColo et Atrivo) utilisés pour héberger des serveurs de commandes de botnets. Ces actions se poursuivent et s'intensifient. Par exemple, en début d'année 2010 plusieurs opérations de démantèlement de réseaux de botnets ont été annoncées dans la presse: Kneber, Waledac, Mariposa. Le grand public découvre peut-être à cette occasion que le piratage organisé à grande échelle existe et qu'un groupe pirate est capable de construire un botnet en prenant le contrôle de plusieurs dizaines de milliers d'ordinateurs.

Mais ces opérations de démantèlement démontrent surtout que la capacité de réaction face à ces actions malveillantes a largement gagné en efficacité au cours de ces dernières années. Des groupes multinationaux d'experts informatiques et d'autorités judiciaires sont aujourd'hui capables de coopérer pour mener à bien des actions de grande envergure, y compris à l'échelle mondiale. Ce constat illustre à nouveau, comme nous le disions en conclusion de notre bilan 2008, que sur le front des attaques les positions se sont professionnalisées et durcies : attaquants et défenseurs sont de plus en plus expérimentés et déterminés.

Bien-sûr le phénomène des botnets n'est pas pour autant enrayé. Aujourd'hui, l'objectif principal des attaques visant le poste de travail (phénomène analysé au chapitre 2) est justement la création de nouveaux botnets regroupant des machines compromises. Ces botnets servent ensuite à réaliser des actions malveillantes comme l'envoi de Spam ou les attaques DDOS. La gestion de ces botnets est une activité très organisée : certains groupes sont spécialisés dans la constitution de botnets, d'autres dans leur gestion et leur mise à disposition (la location) pour des utilisateurs finaux qui eux achètent simplement un service (une campagne de spam ou une attaque DDOS). Dorénavant, des kits pour « construire soit même son botnet » sont également disponibles. Pour éviter d'être la cible d'opérations de démantèlement les cyber-criminels déploient diverses techniques. Par exemple ils morcellent leurs botnets (pour éviter de perdre l'ensemble des machines infectées d'un seul coup) ou infectent la même machine avec plusieurs malwares aux caractéristiques différentes. Nous présentions par exemple cette dernière technique dans un article intitulé Kneber, l'histoire d'un botnet que nous avons rendu public en février 2010.

Dans le domaine des botnets on peut noter enfin pour 2010, l'arrivée du malware bancaire SpyEye. Apparu en décembre 2009, ce malware spécialisé dans le vol de données bancaires s'est très

rapidement présenté comme le rival du malware Zeus en intégrant des fonctions pour combattre ce dernier et lui voler ses victimes. Finalement, en fin d'année 2010, ce combat a fini par un accord "à l'amiable", et Zeus a fusionné avec SpyEye. Cette fusion donne naissance à une nouvelle version de SpyEye encore plus sophistiquée et malveillante, et constitue à ce jour le malware le plus sophistiqué dans le domaine de la malveillance bancaire.

4) Conclusions

En termes d'attaques, l'année 2010 est dans la continuité des années précédentes. Le nombre de failles découvertes chaque année reste important (plus de 600 nouveaux avis Cert-IST, et presque 2000 mises à jours au cours de l'année). Ces failles sont utilisées le plus souvent pour tenter de compromettre le poste de l'utilisateur final, avec comme objectif :

- soit d'inclure ce poste dans un réseau de machines compromises (un botnet) qui est utilisé ensuite pour des malveillances à grande échelle (envoi de SPAM, attaque DDOS, etc…),
- soit pour infiltrer en profondeur une entreprise dans un but bien précis (vol d'information, sabotage, etc) en restant le plus discret possible.

L'année 2010 marque même une accentuation de ce phénomène :

- Les botnets sont toujours très nombreux. Le démantèlement médiatisé de certains d'entre eux (Mariposa, Waledac) montre qu'une lutte active existe entre attaquants et défenseurs.
- Des cas d'attaques ciblées ont également été fortement médiatisées (Attaque Aurora contre Google ou ver Stuxnet contre les systèmes SCADA). Le fait que ces attaques sont maintenant rendues publiques montre que ce phénomène prend de l'ampleur.

Qu'il s'agisse de botnets ou d'attaques ciblées, les codes malveillants vus en 2010 étaient, comme les années précédentes, d'un haut niveau de complexité et d'ingéniosité.

Pour l'entreprise la prise en compte de cette menace peut se faire suivant plusieurs axes complémentaires :

- Tout d'abord le maintien à jour du poste de travail de l'utilisateur (en termes de correctifs de sécurité) aussi bien pour le système d'exploitation que pour les logiciels tiers (lecteur PDF, runtime Java, etc…). Cet axe est primordial car le plus souvent les attaques contre le poste de travail utilisent des vulnérabilités anciennes, pour lesquelles des correctifs sont déjà disponibles auprès des constructeurs. La veille sur les vulnérabilités, et la capacité à déployer les correctifs de sécurité au sein de l'entreprise, sont donc des éléments clés de la maitrise de la sécurité.
- La capacité à détecter le plus vite possible les postes compromis. L'utilisateur est souvent le premier à détecter le comportement anormal de son poste de travail. S'il est sensibilisé aux risques d'attaques et dispose d'un canal pour signaler les anomalies qu'il constate, il peut être un maillon clé dans la détection des attaques ciblées.
- Le renforcement de la sécurité du poste de travail. Au-delà des protections classiques (de type antivirus) qui ont montrés leurs limites ces dernières années, des nouveaux outils de protection restent à trouver. La virtualisation du navigateur web est une solution qui est souvent évoquée pour ces attaques, mais qui reste encore peu appliquée pour des déploiements de grandes ampleurs.

En termes d'évolutions technologiques la demande des utilisateurs continue d'être dans un sens de plus d'ouverture. Elle pousse vers :

- Une connexion permanente à Internet, par exemple au travers de smartphones, avec comme conséquence une frontière de moins en moins marquée entre la sphère professionnelle et la sphère personnelle,

- Et une information toujours disponible, avec la tentation pour ce faire de déplacer les données de l'entreprise vers Internet (par exemple via des solutions de "cloud").

Sans rejeter ces demandes, les responsables sécurité doivent rester vigilants puisque les risques de sécurité sont ici multiples. La fuite ponctuelle de données (par exemple en cas de perte d'un smartphone) ou même la perte de contrôle sur des données externalisées (par exemple gérées par des solutions "cloud") en sont des exemples. L'analyse des risques et la définition de règles pour une utilisation encadrée et guidée de ces solutions sont donc indispensables.

Enfin, et de façon assez logique, après les efforts fait ces dernières années dans le domaine réglementaire et normatif (par exemple Sarbanes-Oxley et ISO-27001), et face à la montée des enjeux sur la protection des données personnelles, le cadre législatif de la SSI se renforce. Le rôle croisant des CIL (Correspondants Informatiques et Libertés) et les discussions en cours sur les obligations de déclaration d'incidents impliquant des données personnelles en sont l'illustration.

Fin du document