# Bilan 2009 des failles et attaques



# 1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée. L'objectif est de retracer les événements marquants de 2009 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger. Ce bilan s'appuie sur l'ensemble des publications fournies aux adhérents du Cert-IST au fil des mois et en particulier sur les synthèses données dans les bulletins mensuels.

## 1.1 Quelques chiffres

En 2009 le Cert-IST a publié **592 nouveaux avis de sécurité** (décrivant de nouvelles vulnérabilités) et a suivi leur évolution au travers de 1590 mises à jour (dont 56 mises à jour majeures). Le nombre de nouvelles vulnérabilités découvertes en 2009 reste donc très proche de celui des années précédentes (563 avis émis en 2008, 595 en 2007, 546 en 2006, etc.).

Toutes ces vulnérabilités représentent des menaces latentes, dont le Cert-IST suit l'évolution (par exemple en surveillant l'apparition de programmes d'attaques, ou en constatant les premières attaques réelles) afin d'identifier au plus tôt les situations à fort risque. Il informe sa communauté de ces montées de risques au travers deux types de communications :

- Les messages de "Danger Potentiel" pour une menace significative mais non encore imminente ou d'une gravité modérée.
- Les messages "d'Alerte" pour mes menaces majeures nécessitant un traitement prioritaire.

Si le nombre de vulnérabilités émises en 2009 est comparable à ce qu'il était les années précédentes (cf. les chiffres annoncés ci-dessus), sur le plan de la montée des menaces par contre, l'année 2009 a connu une évolution bien différente. En effet :

- Aucune Alerte n'a été émise en 2009, alors que nous avions émis 2 alertes (Conficker et DNS-poisoning) en 2008.
- Et surtout, 18 messages "Dangers Potentiels" ont été émis, soit près du double de ce que nous avons émis les années précédentes.

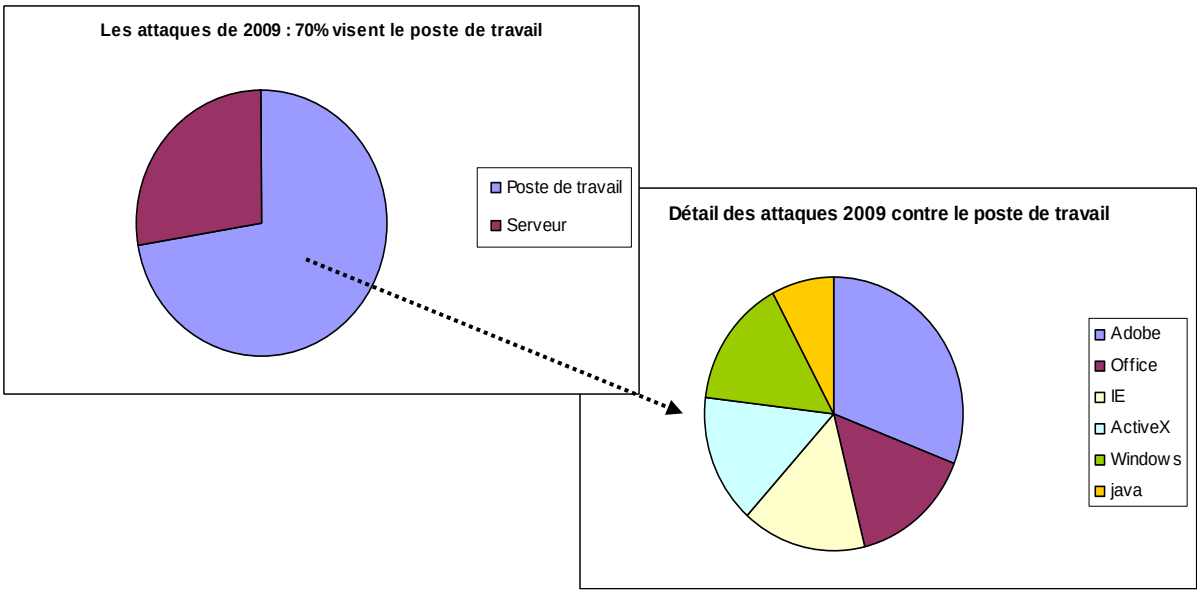
**Nous analysons plus en détail cette évolution ci-dessous dans notre présentation des faits marquants, mais nous pouvons dès maintenant la résumer en disant que la menace s'est accrue en 2009 (presque 2 fois plus de situations à risque ont été identifiées) mais que les attaques sont restées d'ampleurs limitées (aucune "alerte générale" n'a été lancée).**

Globalement, le Cert-IST suit actuellement les vulnérabilités concernant 837 produits et 7217 versions de produits.

## 1.2 Les principaux faits marquants

Si l'on compare 2009 à ce que nous avions observé en 2008 (cf. notre bilan 2008), plusieurs éléments se dégagent :

- **Les attaques visant les logiciels applicatifs se sont poursuivies**. Tout comme en 2008, les attaques 2009 ont visé le plus souvent des logiciels applicatifs (comme Acrobat Reader, QuickTime, Excel, ou Internet Explorer) et avaient pour objectif de compromettre les postes des utilisateurs finaux. Plus 70% des menaces qui ont donné lieu à l'émission d'un danger potentiel par le Cert-IST sont des attaques visant les utilisateurs finaux (les 30 % restant concernent des attaques visant des serveurs). Acrobat Reader (le lecteur de PDF) a été en 2009 le logiciel le plus visé (30 % des attaques). Les autres logiciels visés par ces attaques ont été Microsoft Office, Internet Explorer, …




- **Les attaques massives** observées au premier semestre de 2008 (en particulier les attaques de sites web par "SQL injection") **n'ont pas été aussi nombreuses** en 2009. Elles ont été observées (voir par exemple les Dangers Potentiels **CERT-IST/DG-2009.010** et **CERT-IST/DG-2009.011** émis en juillet 2009), mais sont restées en nombre limité. Il n'y a pas eu non plus d'attaque d'ampleur significative concernant les logiciels serveurs (cf. le chapitre 2.2).
- **Conficker** (pour lequel le Cert-IST a émis une alerte en novembre 2008) est resté très présent en 2009. C'est la seule attaque massive de 2009.

Ces différents aspects sont développés au chapitre 2, intitulé "Les attaques majeures de 2009".

Si l'on analyse l'évolution des technologies et les menaces qu'elles induisent l'année 2009 a été aussi l'année où :

- **les réseaux sociaux (du type FaceBook ou Twitter) ont atteint un niveau de diffusion jusqu'alors inégalé**. Ils sont désormais profondément ancrés dans les usages et deviennent des composantes incontournables à prendre en compte dans le paysage de la sécurité informatique.
- **Le "cloud computing" a envahi les offres**. Bien que le niveau de maturité en sécurité de cette technologie soit encore insuffisant, il s'agisse d'une évolution fortement attractive qui,

comme ce fut le cas pour la virtualisation ces dernières années, marquera sans aucun doute nos prochaines années.

Ces aspects sont développés dans le chapitre 3, intitulé "Les menaces montantes".

Enfin, en 2009 **l'effort des constructeurs pour prendre en compte les vulnérabilités découvertes dans leurs produits s'est renforcé** et les processus déployés ont gagné en maturité. Cette amélioration est souvent déclenchée par le fait qu'un produit devient la cible d'attaques répétées. La prise en compte de la sécurité est alors incontournable pour préserver l'image de marques. Mais cette évolution nous semble plus profonde, comme nous le décrivons ci-après au chapitre 4, intitulé "Les grandes campagnes de corrections".

# 2) Les attaques majeures de 2009

## 2.1 Les attaques visant les postes utilisateurs

L'année 2009 a confirmé une tendance déjà identifiée en 2008 : la grande majorité des attaques visent l'utilisateur final et tentent d'infecter son poste de travail :

- au cours de sa navigation web (au moyen d'attaques dites "drive-by download", qui consistent à déclencher le téléchargement d'un code malveillant sur le poste de la victime au moment où celle-ci passe sur un site web piégé).
- ou, en lui envoyant un e-mail contenant une pièce jointe piégée.

En général ces attaques sont d'abord utilisées à petite échelle (attaques en 0-day visant un nombre très limité de victimes) puis sont ensuite reprises par d'autres pour réaliser ces attaques à large échelle. Le scénario type est le suivant :

- tout d'abord le pirate a connaissance d'une vulnérabilité non publique (on appelle ce type de vulnérabilité un « 0-day »), qu'il a découvert lui-même ou qu'il a acheté auprès de chercheurs de failles peu scrupuleux. Ces vulnérabilités concernent le plus souvent des faiblesses affectant des logiciels comme les navigateurs web, Adobe Reader ou Excel.
- Il utilise cette vulnérabilité pour réaliser des attaques « ciblées », c'est-à-dire des attaques visant un nombre très limité de victimes. Par exemple un document piégé sera envoyé par e-mail à quelques personnes dans une entreprise dans le but d'infecter leurs postes.
- Si ces attaques sont détectées et rendues publiques, alors débute une deuxième phase dans laquelle le risque est que l'attaque 0-day dévoilée soit reprise par d'autres pour réaliser des attaques massives, soit en lançant une campagne de SPAM pour propager un document malveillant, soit via des sites web compromis. Pour l'entreprise ce risque persiste ensuite jusqu'à ce que les correctifs soient déployés sur l'ensemble du parc.

Face à ce phénomène la menace pour l'entreprise est de deux types :

- Elle peut être la victime de la première vague d'attaque : l'attaque ciblée par e-mail visant un nombre de limité de victimes. Ce cas d'attaque, vient d'être largement médiatisé suite à l'annonce en janvier 2010 d'attaques de ce type ayant visé Google et d'autres entreprises nord américaines (série d'attaques qui a été baptisée "Aurora"). Il ne s'agit en fait pas d'un phénomène nouveau et ce type d'attaque se produit depuis plusieurs années. Les premiers rapports publics sur ce sujet datent de l'été 2005, et nous avions en particulier consacrée la "Une" de notre bulletin mensuel de juillet 2005 à la montée de cette menace.
- L'entreprise peut être victime également de la seconde vague d'attaque : celle qui se produit lorsque d'autres attaquants, apprenant qu'une nouvelle vulnérabilité existe, décident à leur tour d'utiliser ce vecteur. Il s'agit alors le plus souvent d'attaques qui utilisent un grand nombre de sites web silencieusement compromis pour attaquer l'internaute lors de sa navigation sur le web.

La première vague est discrète (peu de victimes) et difficile à anticiper (elle utilise une vulnérabilité que personne ne connait encore). Une gestion méthodique des informations sensibles de l'entreprise,

des défenses en profondeur, et une bonne capacité de détection des attaques subies sont ici les éléments clés pour la maitrise de ce risque.
La seconde vague est plus facile à éviter. La maitrise du risque repose ici sur une veille efficace (pour détecter l'arrivée de la première vague) et sur la capacité de déclencher les moyens de protection adéquat pour stopper la menace (mise ne place de mesures de protection périmétriques et déploiement de correctifs).

Au cours de l'année 2009, les attaques visant le poste de travail sont toutes restées au stade d'attaques ciblées (1ere vague d'attaque) et aucune n'a pas donné lieu à des attaques d'ampleur vraiment significative (2eme vague).

- **Détail des attaques ayant visé en 2009 les postes utilisateurs**

Ce chapitre décrit les 13 Dangers Potentiels que le Cert-IST a émis en 2009 pour informer ses adhérents d'attaques visant les postes utilisateurs. Les lecteurs qui souhaitent avoir un aperçu rapide de l'évolution des attaques pourront, en première lecture, sauter ce chapitre.

**Février 2009 : CERT-IST/DG-2009.001 (Internet Explorer 7 - MS09-002)**

Le 17/02/2009 des attaques via des **documents Word piégés** ont été identifiées. Ces documents Word provoquaient le lancement d'Internet-Explorer et tentaient d'exploiter la vulnérabilité MS09-002 décrite dans l'avis **CERT-IST/AV-2009.064**. Cette situation à risque a donné lieu à l'émission du Danger Potentiel **CERT-IST/DG-2009.001** (Exploitation d'une vulnérabilité dans Internet Explorer 7 - MS09-002).

**Février 2009 : CERT-IST/DG-2009.002 (Fichiers PDF malveillants)**

Trois jours plus tard (20/02/2009) des **fichiers PDF** exploitant une vulnérabilité jusque là inconnue (**attaque 0-day**) dans Adobe Reader et Acrobat ont déclenché l'émission par le Cert-IST d'un nouveau Danger Potentiel: **CERT-IST/DG-2009.002** (Propagation de fichiers PDF malicieux). Cette menace est suivie ensuite dans le Hub de Crise "**Adobe 02/09**".

**Février 2009 : CERT-IST/DG-2009.003 (Vulnérabilité dans Excel)**

Le 24/02/2009 Microsoft publiait un avis de sécurité concernant une **vulnérabilité (0-day) dans Excel** utilisée dans des attaques ciblées. Cette nouvelle menace a donné lieu à l'émission du Danger Potentiel **CERT-IST/DG-2009.003** et au Hub de Crise **Excel 0day**

**Avril 2009 : CERT-IST/DG-2009.004 (Fichiers PowerPoint malveillants)**
**Avril 2009 : CERT-IST/DG-2009.005 (Vulnérabilité Adobe Reader et Acrobat)**

En avril deux nouvelles menaces de ce type sont apparues et ont donné lieu à l'émission des messages "Danger Potentiel" suivants :

**CERT-IST/DG-2009.004** : Diffusion de fichiers Microsoft PowerPoint malicieux (03/04/2009)
**CERT-IST/DG-2009.005** : Vulnérabilités "0-day" dans Adobe Reader et Acrobat (30/04/2009)

Dans les deux cas, les vulnérabilités découvertes permettaient de construire des fichiers malveillants qui, s'ils étaient ouverts par la victime, provoquaient l'exécution de code arbitraire sur son poste. La vulnérabilité Adobe pouvait de plus être activée directement depuis un navigateur web (puisqu'un plugin Adobe PDF est installé sur la plupart des navigateurs web).

**Mai 2009 : CERT-IST/DG-2009.008 (Vulnérabilité DirectX sous Windows)**

Le 29 mai, nous avons émis le Danger Potentiel **CERT-IST/DG-2009.008** (Vulnérabilité "0-day" dans DirectX sous Microsoft Windows). Cette vulnérabilité pouvaitt être exploitée via une attaque de type "phishing" classique, dans laquelle une personne malveillante redirige sa victime vers un site piégé qui chargeait un fichier vidéo malicieux (Quicktime, avi). Dans une des attaques qui a été observées la vulnérabilité installait un cheval de Troie (par exemple "Trojan.Cipevas") qui permet ensuite à l'attaquant d'exécuter des commandes sur le poste de la victime. Les correctifs pour cette vulnérabilité ont finalement été diffusés par Microsoft le 14 juillet 2009.

**Juillet 2009 : CERT-IST/DG-2009.010 (Vulnérabilité DirectShow sous Windows)**
**Juillet 2009 : CERT-IST/DG-2009.011 (Vulnérabilité Office Web Component sous Windows)**

Ces 2 Dangers Potentiels sont très similaires : « CERT-IST/DG-2009.010 - Attaques web via un 0-day dans DirectX/DirectShow (msvidctl.dll) sur Microsoft Windows » et « CERT-IST/DG-2009.011 - Vulnérabilité 0-day dans Office Web Components de Microsoft Windows » . Dans les deux cas, des hackers ont initialement compromis des sites web via des attaques « classiques » (injections SQL …), puis ont utilisé ces sites dans le but d'infecter les utilisateurs lors de leur navigateur web. Ces deux menaces étaient aussi semblables du point de vue du risque induit :

- Il s'agissait de l'exploitation d'une vulnérabilité dans un contrôle ActiveX instanciable dans le navigateur Internet Explorer. Ces vulnérabilités permettaient, comme bien souvent lorsqu'il s'agit de contrôles ActiveX, d'exécuter un code arbitraire sur le système victime avec les privilèges de l'utilisateur connecté. Lorsque l'utilisateur en question visitait une page spécialement construite, il était alors automatiquement infecté par le code malveillant (drive-by attack).
- Même si le risque intrinsèque lié à ce genre de vulnérabilité est de notre point de vue critique, la fenêtre d'exposition des utilisateurs peut être facilement réduite grâce aux « kill-bits » (identifiants des contrôles ActiveX à bloquer). L'ajout de « kill-bits » est dans la majorité des cas une solution suffisante pour protéger les postes des utilisateurs (elle empêche l'invocation du contrôle ActiveX depuis Internet Explorer) et n'a pas d'inconvénient.

**Juillet 2009 : CERT-IST/DG-2009.012 (Vulnérabilité Adobe Flash Player)**

Il s'agit à nouveau d'une faille 0-day, mais cette fois dans Adobe Flash Player (CERT-IST/DG-2009.012 - Vulnérabilité 0-day dans Adobe Reader, Acrobat et Flash Player). Cette menace avait la particularité qu'elle est initialement apparue sous la forme de fichiers PDF malicieux, si bien qu'on pouvait penser que la vulnérabilité se situait dans Adobe Reader. En réalité, Adobe ayant donné quelques éclaircissements un peu plus tard, les fichiers PDF exploitaient une faille dans le plug-in Flash intégré au lecteur PDF, du code qui est partagé avec le lecteur multimédia Flash Player. Le point intéressant ici, c'est que cela augmente le nombre de vecteurs d'attaques possibles :

- Attaque via un fichier PDF malveillant envoyé par e-mail ou téléchargé sur un site web,
- Attaque automatique et transparente lorsqu'un utilisateur visite un site web compromis exploitant la vulnérabilité via le plug-in Flash Player instancié dans le navigateur.

**Novembre 2009 : CERT-IST/DG-2009.016 (Vulnérabilité EOT dans Windows)**

Il s'agit ici d'une **vulnérabilité** (CVE-2009-2514) **dans le moteur de traitement des polices EOT par le noyau Windows** (bulletin Microsoft MS09-065). Cette vulnérabilité permet à un utilisateur distant de prendre le contrôle total d'un système vulnérable. Cette vulnérabilité décrite dans l'avis de sécurité CERT-IST/AV-2009.515 a fait l'objet du danger potentiel CERT-IST/DG-2009.016, car il existait un fort

risque qu'elle soit exploitée de façon massive à l'aide de fichiers Office malveillants ou via Internet Explorer lors de la navigation sur un site spécifiquement construit.

### Novembre 2009 : CERT-IST/DG-2009.017 (Vulnérabilité dans Internet Explorer)

Cette vulnérabilité (CVE-2009-3672) de type **0day dans Internet Explorer** était due à une erreur dans la gestion de certains objets CSS par Internet Explorer. Elle permettait à un attaquant distant de provoquer un déni de service partiel d'un navigateur vulnérable, ou même d'exécuter du code arbitraire avec les privilèges de l'utilisateur connecté. Nous avons émis le danger potentiel CERT-IST/DG-2009.017 dès que des programmes d'exploitation ont été publiés sur Internet. Bien que certains de ces programmes semblaient peu fiables, des versions plus robustes pouvaient en effet rapidement apparaitre. Cette vulnérabilité a été corrigée début décembre par Microsoft (MS09-072) et a donné lieu à l'avis CERT-IST/AV-2009.554.

### Décembre 2009 : CERT-IST/DG-2009.018 (Vulnérabilité Adobe Reader et Acrobat)

Cette vulnérabilité (**CVE-2009-4324**) permet à un document PDF spécifiquement construit, d'exécuter des actions malveillantes lors de son ouverture avec une version vulnérable des logiciels Adobe Reader et Acrobat. Cette vulnérabilité a été découverte en analysant des attaques ciblées survenues à la mi-décembre. Ces attaques consistaient à envoyer par e-mail un document PDF piégé vers un nombre très limité de destinataires et d'inciter ceux-ci à les ouvrir.

A l'annonce de ces attaques ciblées, le Cert-IST a averti notre communauté en envoyant le 15/12/2009 le message **VulnCoord-2009.020** (Nouvelle vulnérabilité - CVE-2009-4324- exploitée dans Adobe Reader et Acrobat). Deux jours plus tard, nous avons émis le Danger Potentiel **CERT-IST/DG-2009.018** (Risque d'attaque via le "0-day" CVE-2009-4324 dans Adobe Reader et Acrobat) car des codes permettant de réaliser l'attaque avaient été publiés sur Internet, ce qui multipliait le risque d'en être victime. A cette occasion nous ouvrions le hub de crise « Adobe 12-2009 » afin de suivre l'évolution de cette menace. Comme nous l'indiquions le 04/01/2010 dans un billet de ce hub, des attaques ciblées ponctuelles ont été signalées ensuite par diverses sources, ce qui montrait la montée de plus en plus importante du risque d'attaque. Adobe a finalement publié les correctifs à cette vulnérabilité le 12/01/2010, à l'occasion de son patch trimestriel.

Comme nous le rappelons systématiquement dans nos publications, **il est impératif pour se protéger de ces attaques de désactiver l'interprétation du JavaScript dans Adobe Reader et Acrobat**. En effet ces attaques utilisent un code JavaScript malveillant inséré dans le fichier PDF piégé pour s'exécuter lors de son ouverture. Cette mesure de protection n'a pas d'inconvénient majeur car il est très rare que des documents PDF légitimes utilisent du code JavaScript.

## 2.2 Les attaques visant les infrastructures informatiques

Cette catégorie regroupe les attaques visant les logiciels serveurs (serveurs web, serveurs DNS, etc…) ainsi que les attaques qui se propagent de façon automatique de systèmes en systèmes au moyen de codes malveillants de type "vers".

En 2009, 30 % des "Dangers Potentiels" émis par le Cert-IST concernaient des menaces de ce type. Nous les passons en revue ci-dessous. Ces Dangers Potentiels ont concernés les produits suivants :

- DNS BIND (vulnérabilité dans la fonction de "dynamic update")
- Microsoft Vista et 2008 (vulnérabilité SMB2)
- Microsoft IIS 5 et 6 (vulnérabilité dans WebDAV puis dans le service FTP)
- Adobe ColdFusion (vulnérabilité FCKEditor)

Chacune de ces vulnérabilités avait un potentiel de nuisance assez important. Mais heureusement, aucune n'a donné lieu à des attaques d'une ampleur significative, et il n'a donc pas été nécessaire pour le Cert-IST d'émettre une "Alerte de sécurité" au sein de notre communauté.

Nota : Quand le Cert-IST estime qu'une attaque massive est imminente il émet une "Alerte" de sécurité. Pour toutes les autres attaques significatives, et pour les menaces d'attaques massives non imminentes, le Cert-IST émet un message de "Danger Potentiel".

- **Détail des vulnérabilités serveur de 2009**

Nous donnons ci-dessous une description des vulnérabilités 2009 impactant les serveurs et pour lesquelles le Cert-IST a émis un Danger Potentiel. Les lecteurs qui souhaitent avoir un aperçu rapide de l'évolution des attaques pourront, en première lecture, sauter ce chapitre.

**Mai 2009 : CERT-IST/DG-2009.006 (Microsoft IIS 6.0)**

Le 18 mai 2009, suite à la publication d'un programme d'exploitation, utilisant une faille jusque-là inconnue (0day) dans Microsoft Internet Information Server 6.0, nous avons émis le Danger Potentiel **CERT-IST/DG-2009.006**. Cette vulnérabilité dans la fonctionnalité WebDAV des serveurs IIS 6.0 permet à une personne malveillante de contourner à distance des restrictions d'accès mises en place sur un serveur IIS vulnérable (cf. avis **CERT-IST/AV-2009.204**). A cette date aucun correctif Microsoft n'était disponible (seuls des palliatifs avaient été fournis par Microsoft). Ces correctifs ont finalement été diffusés par Microsoft le 8 juin via le bulletin de sécurité MS09-020.

**Juillet 2009 : CERT-IST/DG-2009.009 (Adobe ColdFusion)**
**Juillet 2009 : CERT-IST/DG-2009.013 (DNS BIND)**

La période d'été est souvent l'occasion d'un regain d'activité sur le front des attaques. L'année 2009 confirme cette tendance puisque qu'en juillet 2009 nous avons émis 5 « Dangers Potentiels » mais également ré-émis 11 avis de sécurité suite à une élévation du risque associé à ces avis à « élevé » ou « très élevé ».

Deux de ces 5 « Dangers Potentiels » concernaient des logiciels serveurs (Adobe ColdFusion et le serveur DNS BIND). Les 3 autres ont déjà été mentionnés au chapitre 2.1.

Le premier « Danger Potentiel » (CERT-IST/DG-2009.009) que nous avons envoyé concernait l'exploitation d'une **vulnérabilité dans l'environnement web Adobe ColdFusion**. Plus précisement, la vulnérabilité se trouvait dans le composant open-source FCK-Editor (un éditeur HTML s'intégrant dans des pages web), et permettait à des attaquants de déposer des scripts Shell sur le serveur. Comme on peut l'imaginer, ces scripts Shell permettent ensuite d'ajouter, de modifier ou de supprimer des pages web sur ce serveur. Dans la majorité des attaques constatées, le site web compromis était modifié de manière à exploiter des vulnérabilités dans les navigateurs des utilisateurs visitant le site. Dans le cas de cette attaque, on constate que même si un serveur a été compromis, ce sont bien les applications côté client qui sont finalement visées via les pages web infectées.

Le second « Danger Potentiel » concerne **une faille découverte dans les serveurs DNS BIND** (CERT-IST/DG-2009.013 - Exploitation d'une vulnérabilité dans le serveur DNS BIND). Cette fois heureusement, les correctifs pour les différentes distributions Linux/Unix ont été fournis très rapidement, sans doute parce qu'un programme d'exploitation était joint au rapport de bug initial. La faille était particulièrement critique puisqu'elle permettait à un attaquant de provoquer l'arrêt d'un serveur DNS à distance grâce à l'envoi d'un paquet UDP de mise à jour dynamique de zone. On notera au passage qu'il n'était pas nécessaire que le serveur DNS ait activé cette fonctionnalité de mise à jour dynamique pour être vulnérable et que le seul fait d'être maître (master) pour au moins une zone suffisait. La plupart des caches et des résolveurs DNS étaient également concernés puisqu'il est très courant de définir sur ces configurations des zones d'autorité telles que "localhost" ou "0.0.127.in-addr.arpa".

### Septembre 2009 : CERT-IST/DG-2009.014 (Microsoft IIS 5 et 6)

Le 1er septembre le Cert-IST a émis le Danger Potentiel **CERT-IST/DG-2009.014** (**Vulnérabilité "0-day" dans le serveur FTP de Microsoft IIS 5 et 6**). Cette faille dans le serveur FTP de IIS était très critique pour les serveurs IIS sur Windows 2000 lorsque le serveur FTP était configuré pour autoriser le dépôt de fichiers : des programmes d'exploitation étaient en effet disponibles pour ce type de configuration et permettaient de prendre le contrôle total de la machine vulnérable.

### Septembre 2009 : CERT-IST/DG-2009.015 (Microsoft Vista et 2008)

Il s'agit ici d'une vulnérabilité de type **0day impactant les systèmes Windows Vista et Windows Server 2008**. Cette vulnérabilité permettait à un attaquant distant, via des paquets SMB spécifiquement formatés, de provoquer un déni de service sur un système vulnérable, voire d'exécuter du code arbitraire sur ce système avec des privilèges élevés sur ce dernier.

Les principales étapes du suivi de cette menace ont été les suivantes :

- 08/09/2009 : Cette vulnérabilité est suivie par le Cert-IST sous la référence FA-2009.0176 dans la section des failles en cours d'analyse.
- 17/09/2009 : Nous avons émis le danger potentiel **CERT-IST/DG-2009.015**, parce qu'un programme d'exploitation avait été publié sur internet. Bien qu'à l'état de "Proof-of-Concept" (car non fiable), ce programme démontrait la possibilité d'exécuter du code sur la machine vulnérable.
- 18/09/2009 : Microsoft propose une solution temporaire de contournement accompagnée d'un FixIt, ne corrigeant cependant pas la vulnérabilité.
- 30/09/2009 : Nous faisions état dans le "Hub de crise" consacré a cette menace de la publication d'un programme d'exploitation fiable permettant d'exécuter du code arbitraire.
- 13/10/2009 : Publication des correctifs Microsoft via le bulletin MS09-050.

## 2.3 Conficker

Bien qu'apparu en 2008, Conficker est restée, au moins jusqu'en avril 2009, une préoccupation majeure du fait de ses mutations successives.

Tout d'abord, début janvier, le ver **Conficker** a connu une recrudescence en termes de propagation, en particulier du fait d'une nouvelle variante (Conficker-B). Cette évolution a été suivie par le Cert-IST au travers de plusieurs billets postés dans le hub de crise [MS08-067] ouvert le 24/10/2008 pour suivre cette menace. A la demande de certains adhérents, le Cert-IST a également créé une liste de discussion dédiée à ces infections, ce qui a permis aux adhérents d'échanger leur expérience dans la gestion de cette crise. Conficker est un malware très sophistiqué. Des chercheurs ont d'ailleurs découvert en l'analysant que les mécanismes de Windows interdisant l'exécution automatique des périphériques amovibles (fonction "Autorun.ini") étaient inefficaces et permettaient à une clé USB infectée par Conficker de propager l'infection.

En mars, Conficker est revenu au devant de l'actualité car les analyses du code des deux nouvelles variantes du malware (Conficker-B++ et Conficker-C) ont montré que le comportement de ce dernier allait changer le 1er avril 2009. Cet évènement programmé a alors généré une sur-médiatisation et des réactions disproportionnées de la presse informatique spécialisée et généraliste.

Dans ces nouvelles variantes (B++ et C) l'auteur de Conficker a développé de nouvelles fonctions de mise à jour, de propagation, de téléchargement de chevaux de Troie mais surtout des fonctions cherchant à désactiver les outils de sécurité susceptibles d'entraver sa propagation. De façon plus anecdotique, mais révélatrice du niveau de sophistication de ce ver, on peut noter que la dernière variante implémente l'algorithme de prise d'empreinte (hashage) MD6. A notre connaissance c'est le seul logiciel à ce jour qui implémente ce nouvel algorithme publié en octobre 2008. Malheureusement, ces divers constats démontrent le « professionnalisme » dans le développement de ce malware.

Depuis avril, Conficker a quitté le devant de l'actualité, mais il reste néanmoins présent. Tout au long de l'année des infections localisées ont été identifiées et fin 2009 plusieurs sources ont lancé une alerte pour signaler que malgré les efforts déployés par la communauté le nombre de machinées infectées par Conficker reste important. Ils appellent la communauté à un nouvel effort pour éradiquer cette nuisance.

Conficker nous a appris plusieurs choses :

- Des infections de grande ampleur peuvent toujours se produire
- Même si les patches ont été déployés des foyers infectieux peuvent toujours se déclencher (Cela a été le cas dès que Conficker a intégré dans ses vecteurs d'attaques l'infection via des clés USB) et qu'il faut être prêt à combattre ces infections locales
- L'éradication complète (au niveau mondial) de ce type de virus est difficile. Cela est probablement dû à l'existence d'un parc machines « hors contrôle » (machines domestiques non administrées) important.

## 2.4 Les attaques traditionnelles perdurent

Les menaces traditionnelles, telles que le Phishing, le Spam et les virus, sont restées omniprésentes en 2009. Elles constituent sur le front des attaques un bruit de fond auquel il faut rester attentif.

- **Les attaques via des SPAM malveillants qui suivent le fil de l'actualité**

Par exemple, fin juin, l'US-Cert a rapporté de nombreux cas d'exploitation, par diverses campagnes de spam et phishing notamment, d'événements "people" tels que les décès de Farrah Fawcett et de

Michael Jackson. C'est notamment le cas de vidéos piégées qui permettent de compromettre le poste de victimes crédules lors de la visualisation de ces vidéos et d'installer toute sorte de malwares. Toujours en exploitant ces événements "people", et comme le rappelle TrendMicro, ce fut au tour du réseau MSN d'être utilisé par un "bot". Ce dernier tente de compromettre les utilisateurs MSN crédules, avides des "cancans" vidéos des deux stars, en les incitants à cliquer sur des liens piégés.

De même, fin novembre 2009 nous rappelions dans notre bulletin mensuel que la période de fin d'année approchant on pouvait s'attendre à une recrudescence d'arnaques en tout genre, allant des faux emails promotionnels, aux tentatives de phishing profitant des achats de Noël ou du nouvel an. Cette mise en garde faisait suite à la découverte, courant novembre, d'un faux site marchand imitant un site de commerce en ligne français.

- **Les virus qui ont fait parler d'eux**

Au mois de mai nous avons émis le message Virus-Coord "Infection de sites web par JSRedir-Gumblar", suite à plusieurs rapports d'infection de sites web par le cheval de Troie "Gumblar", aussi appelé "JSRedir". Notons qu'au-delà de ces caractéristiques de "drive-by-download", ce malware présente également la capacité de rediriger les recherches Google effectuées depuis les systèmes infectés.

En octobre, une nouvelle variante du **malware Zeus** (connu aussi sous le nom de "Zbot") a connu une propagation massive sous forme d'e-mails de spam prétendant être une mise à jour de certificat SSL, puis une mise à jour Outlook Web Access. Dans tous les cas, les e-mails incitaient les destinataires à télécharger un exécutable … qui était en fait un virus (cheval de Troie "Zeus").

Le malware **Virut** (que nous décrivions en 2007 dans l'avis **CERT-IST/AV-2007.428**) a également connu une propagation significative en 2009.

- **Les faux antivirus ("scamware") continuent d'être omniprésent**

La diffusion de faux antivirus est une escroquerie qui existe depuis plusieurs années et que l'on désigne désormais sous le terme de "scamware" (les logiciels "arnaques"). Elle avait pris en 2008 des proportions inégalées, et en décembre 2008 nous analysions ce phénomène dans un article de notre bulletin mensuel intitulé : Le marché lucratif des faux antivirus.

En 2009 ce phénomène de vente forcée de faux antivirus s'est poursuivi au même rythme qu'en 2008, au point de devenir une nuisance courante et récurrente sur Internet.

Le principe est simple : en navigant sur Internet un internaute déclenche une fenêtre "Popup" qui l'avertit que son poste semble infecté, et lui propose d'acheter un logiciel antivirus pour y remédier. Bien sur il s'agit d'une arnaque mais souvent l'utilisateur est contraint d'acheter le produit proposé parce que c'est le seul moyen qu'il a de se débarrasser du virus qu'entre temps le faux antivirus a installé sur son poste…. En décembre 2008, nous analysions ce phénomène.

# 3) Les menaces montantes

## 3.1 Les nouvelles frontières du SI de l'entreprise

En juin 2009, le Cert-IST a consacré son "Forum annuel" sur le thème : "La sécurité et le Cert-IST face aux nouvelles frontières de l'entreprise". Cette journée était dédiée à l'étude de l'impact sur la sécurité des évolutions actuelles des Systèmes d'Information. L'externalisation des traitements (via le "Cloud computing" ou le "SaaS"), le DLP, les systèmes industriels, ou encore la virtualisation, ont été quelques uns des sujets abordés aux cours des présentations et de la table ronde de cette journée.

Ce sujet des "nouvelles frontières de l'entreprise" est clairement un des sujets marquants de 2009 et souligne les nouvelles tendances et préoccupations des entreprises.

**Le "Cloud computing"** est devenu en 2009 omniprésent dans les offres de services. Après la virtualisation des serveurs (qui a, au cours de ces dernières années, dématérialisé les plates-formes qui hébergent les SI), l'offre "Cloud" propose désormais d'externaliser la solution logicielle et de la rendre disponible à l'entreprise au travers d'Internet. Cette externalisation libère l'entreprise des contraintes relatives à la mise en place et au maintien opérationnel de la solution (qui sont maintenant pris en charge par le fournisseur de service); mais l'entreprise reste in-fine responsable de la sécurité de l'information qui est confiée à la solution "Cloud", et elle doit s'assurer que les solutions mises en place par le fournisseur, garantissent la sécurité de cette information au niveau visé. Pour le moment l'offre "Cloud" manque clairement de maturité d'un point de vue sécurité :

- La première moitié de l'année 2009 a été marquée par des annonces tonitruantes de la part des offreurs qui présentaient l'offre "Cloud" comme la solution universelle pour la maitrise des SI (et de leurs coûts)
- Pendant la seconde moitié de l'année des mises en gardes multiples ont répondu à l'enthousiasme initial en mettant en évidence le manque de sécurité de l'offre actuelle.

Indépendamment du fait que les entreprises aillent ou non vers le "Cloud", les frontières de l'entreprise sont remises en question aussi par le changement de comportements des utilisateurs du fait du déferlement sur Internet des **outils Web 2.0 (forum, blogs et réseaux sociaux)**. Ces outils sont largement présents sur Internet et ils sont utilisés par un nombre croissant d'employés d'entreprises. En postant un message dans un blog ou sur un forum, un employé peut nuire à la réputation de son entreprise ou transmettre des informations sensibles. En changeant la relation entre l'utilisateur et l'Internet, le Web 2.0 déforme les frontières de l'entreprise : le Web 2.0 rentre dans l'entreprise et son principe collaboratif induit un risque significatif de fuite de l'information vers l'extérieur de l'entreprise.

La dernière illustration que nous donnerons sur ce phénomène de déplacement des frontières est la montée en puissance de la sécurité **SCADA**. La sécurité des installations d'informatique industrielle (les systèmes de conduite et de contrôle des processus industrielles) est devenue une préoccupation majeure des industriels. En effet la conjonction du phénomène technique de la migration vers le "tout IP" et du phénomène géopolitique de montée de la menace cyber-terroriste rendent le besoin de sécurité des installations industrielles incontournable. Si les frontières de l'entreprise bougent sur le front de l'Internet, elles bougent aussi de l'intérieur et les entreprises doivent désormais également prendre en compte la sécurité de leurs installations industrielles.

## 3.2 Les réseaux sociaux

En 2009, le phénomène des réseaux sociaux s'est renforcé sur Internet : FaceBook a continué à s'ancrer dans les usages du grand public en gagnant une population de plus en plus large. Twitter a lui connu un véritable "boom" en 2009. On pourra noter enfin que 2009 a été l'année du déclin de "Second Life", jeu précurseur des réseaux sociaux… Bien que d'usage marginal au sein des

entreprises, les réseaux sociaux représentent un phénomène à surveiller puisque la frontière entre le monde professionnel et la sphère personnelle devient de plus en plus ténue.

C'est pourquoi le Cert-IST suit activement l'activité "sécurité" de ces réseaux. Voici à titre d'exemple des extraits du bulletin mensuel Cert-IST reflétant cette actualité.

Dans la rubrique des attaques du mois de notre bulletin d'avril 2009 nous disions :

> *De façon moins significative pour notre communauté, on peut noter également qu'au cours du mois d'avril les **attaques autour de Facebook et Twitter** (les deux outils préférés des internautes "branchés") se sont multipliées. Dans le cas de Facebook il s'agit d'attaques de phishing (faux e-mail cherchant à attirer les utilisateurs de Facebook vers des sites malveillants). Pour Twitter, il s'agit du premier ver qui s'est répandu sur Twitter (voir notre bulletin de veille media vmedia-2009.04.14)*

Et en août 2009 nous écrivions en "Une" :

> Le succès de Twitter est étonnant *: sorti de l'ombre en 2008, ce service de "micro-blogging" a littéralement explosé depuis et il est devenu aujourd'hui presque systématique de voir sur les blogs conventionnels la petite icône Twitter (à coté de celle de Facebook …) qui propose de suivre l'auteur du blog sur Twitter.*
>
> *Il est difficile de mesurer s'il s'agit d'une simple mode ou si cette vague Twitter perdurera. En tout cas, il est sûr que Twitter intéresse aussi les hackers qui n'ont pas été longs à utiliser eux aussi ce nouveau média et à tirer partie de certaines faiblesses (que Twitter tente de combler). Spam, virus, phishing et botnets ont donc envahi Twitter. Par exemple le déni de service subit par Twitter le 6 août pourrait être dû à un spam massif.*

## 3.3 Plus d'attaques visant les smart-phones ?

En 2009, plusieurs attaques ont concerné les téléphones dits "intelligents" (smart-phones). Notamment on notera :

- En janvier : L'attaque "**Curse of silence**", permettait à un message SMS spécifiquement formaté de bloquer le service de réception des SMS des téléphones Symbian S60. Nous avons émis à propos de cette actualité le message **VulnCoord-2009.001**.
- En février : Le malware **YXES** (aussi appelé « Sexy Space ») a visé les mobiles Symbian alors qu'il avait été signé électroniquement par erreur par Symbian comme une application "saine".
- En juillet : Lors la conférence **Blackhat**, Charlie Miller présentait une faille permettant de prendre le contrôle d'un iPhone via l'envoi d'un simple SMS
- En novembre, **le ver Ikee** se propageait sur les iPhone qui avaient été débridés ("jail-breakés").

On voit au travers cette actualité que la sécurité des smart-phones est clairement un sujet qui intéresse les chercheurs de failles. Cependant ces attaques restent expérimentales et sont plus du domaine de l'exploration des possibilités techniques de cet environnement que de véritables codes malveillants.

Le marché du smart-phones est en pleine expansion. Les terminaux Blackberry et iPhone se multiplient dans les entreprises et l'utilisation de cette informatique mobile s'ancre dans les usages. Elle participe donc elle aussi à l'évolution des frontières du S.I. que nous évoquions précédemment. Si les attaques concernant cette technologie restent aujourd'hui marginales le risque potentiel que représentent les terminaux mobiles pour l'entreprise est donc bien réel. Il est donc nécessaire de suivre attentivement l'évolution de ce domaine.

# 4) Les grandes campagnes de correction

La dernière tendance qu'il nous parait intéressant de relever dans ce bilan annuel est l'effort fait par les constructeurs pour mieux prendre en compte les failles de sécurité découvertes dans leurs produits. Il s'agit du travail réalisé par les équipes PSIRT (Product Security Incident Response Team) qui ont pour responsabilité de prendre en compte et mettre au point les réponses des constructeurs lorsque des vulnérabilités sont découvertes. Dans ce domaine, l'année 2009 nous semble une année de progrès et de murissement des équipes.

## 4.1 De plus en plus de constructeurs structurent leur effort

Tout d'abord, de plus en plus de constructeurs adoptent le principe de publication de correctifs de sécurité à intervalles réguliers :

- Microsoft une fois par mois (le 2eme mardi de chaque mois),
- Oracle une fois par trimestre (le mardi le plus proche du 15 des mois de janvier, avril, juillet et octobre),
- Cisco IOS deux fois par an (le 4eme mercredi des mois de mars et septembre),
- Adobe Reader et Acrobat une fois par trimestre, le même jour que les avis Microsoft.

Cette structuration temporelle de l'activité de publication de correctifs n'est pas forcement la panacée. Elle peut avoir en particulier l'inconvénient de retarder la diffusion d'un correctif (par exemple lorsque le constructeur informe que la vulnérabilité actuellement exploité sur Internet sera corrigée … lors du prochain patch trimestriel !) ou de provoquer des avalanches de corrections en début de trimestre (comme par exemple en octobre 2009 : 34 vulnérabilités corrigées par Microsoft, 38 vulnérabilités par Oracle et 29 vulnérabilités par Adobe). Globalement elle nous semble tout de même révélatrice d'une plus grande maturé dans les processus de correction car, d'un point de vue externe, le processus de correction passe d'un état "ad-hoc" (les vulnérabilités sont corrigées lorsqu'elles apparaissent avec un processus spécifique à chaque fois) à une activité planifiée (utilisant des processus qui semblent plus industrialisés).

## 4.2 Les grandes campagnes de correction de 2009

Cette structuration débouche sur les processus de corrections élaborés permettant de résoudre des problèmes complexes de façon structurée. La vulnérabilité DNS de l'été 2008 avait été un exemple de résolution de faille complexe. En 2009 nous avons vu deux autres exemples de "grandes campagnes de correction" :

- La correction de la vulnérabilité dans le composant ATL (Active Template Library) de Microsoft. Il s'agit ici du cas d'une vulnérabilité affectant de multiples produits d'un même constructeur.
- La correction de la vulnérabilité TCP-DOS (CVE-2008-4609) coordonnée par le CERT-FI. Dans ce cas la vulnérabilité est multi-constructeur et nécessite une coordination des différents acteurs.

- **Vulnérabilité du composant ATL de Microsoft**

Cette vulnérabilité concerne la librairie ATL fournie par Microsoft. Elle touche potentiellement tous les composants qui ont été développés en utilisant cette librairie (typiquement des contrôles ActiveX), ce qui inclus de nombreux produits tiers. La correction de la vulnérabilité a été complexe parce qu'elle touche un grand nombre de composants. Microsoft a publié pas moins de 6 bulletins de sécurité, diffusées de juillet à octobre 2009, pour corriger ce problème.

Voici une synthèse des avis Cert-IST (et bulletin Microsoft correspondant) qui ont été publiés sur ce problème :

- **CERT-IST/AV-2009.288 -** Vulnérabilité dans le contrôle ActiveX Microsoft Video (**MS09-032**)
- **CERT-IST/AV-2009.326 -** Multiples vulnérabilités dans Microsoft Internet Explorer (**MS09-034**)
- **CERT-IST/AV-2009.327 -** Vulnérabilités "Microsoft ATL" dans de multiples produits (**MS09-035**)
- **CERT-IST/AV-2009.354 -** Vulnérabilités "Microsoft ATL" dans les composants standards de Windows (**MS09-037**)
- **CERT-IST/AV-2009.466 -** Vulnérabilité "Microsoft ATL" dans certains ActiveX de Windows (**MS09-055**)
- **CERT-IST/AV-2009.468 -** Vulnérabilités "Microsoft ATL" dans des ActiveX de Microsoft Office et Visio Viewer (**MS09-060**)

Il ne s'agit pas de corrections successives dues à des erreurs dans les corrections précédentes mais de la prise en compte progressive de tous les éléments impactés : correction du premier composant publiquement connu pour être vulnérable (**MS09-032**), puis renforcement des défenses intégrées dans Internet Explorer (**MS09-034**), puis renforcement de la suite de développement "VisualStudio" (**MS09-035**), etc…

- **Vulnérabilité TCP-DOS (CVE-2008-4609)**

Il s'agit ici du cas d'une vulnérabilité dans le protocole TCP qui permet à un attaquant distant de bloquer un service TCP (par exemple un serveur web) en saturant ses ressources (attaque en déni de service). Cette vulnérabilité a été initialement annoncée en octobre 2008, sans qu'aucun détail technique ne soit alors révélé. Le CERT de Finlande (CERT-FI) a ensuite eu la responsabilité d'orchestrer le travail de coordination entre les découvreurs et les constructeurs impactés (38 constructeurs ont travaillé activement à la prise en compte de cette vulnérabilité). En septembre 2009, les principaux constructeurs impactés ont finalement publié de façon concertée les correctifs pour cette vulnérabilité et le CERT-FI publiait une description technique de la vulnérabilité.

Voici la "Une" que nous avions consacrée dans notre bulletin mensuel à propos de cette conclusion.

> *Enfin ! C'est après presqu'un an, que « sans tambour ni trompette », les correctifs pour la fameuse vulnérabilité "TCP DoS" (CVE-2008-4609) ont commencé à être diffusés. Le 8 septembre dernier, le CERT Finlandais (CERT-FI), coordinateur de la « divulgation responsable » de cette vulnérabilité, publiait finalement les détails de cette faille, permettant l'arrêt brutal d'un équipement vulnérable à l'aide de paquets TCP spécifiquement formatés. Pour rappel, celle-ci avait été révélée par deux experts en sécurité (Jack Louis et Robert Lee) le 1er octobre 2008, et présentée lors de la conférence T2 à Helsinki le 17 octobre 2008. Impactant de nombreux éditeurs dont Cisco, Microsoft et bien d'autres, il aura donc fallu presqu'un an pour que ces derniers produisent enfin des correctifs pour leurs produits.*
> *Cependant, du fait de la complexité pour corriger cette vulnérabilité, tous les éditeurs n'ont pas encore fourni de correctifs. Notamment, Microsoft a annoncé qu'il ne corrigerait pas celle-ci pour les systèmes Windows 2000 SP4 dont le support étendu officiel se termine le 13 juillet 2010. Pour plus de détails sur cette vulnérabilité, reportez-vous au Hub de Crise [TCP DOS] que le Cert-IST a ouvert en octobre 2008 (il retrace l'historique), et à l'avis CERT-IST/AVIS-2009.409.*

## 4.3 Une prise en compte rapide des vulnérabilités est indispensable

Un dernier exemple (ou plutôt contre exemple) vaut la peine d'être noté pour ce qui concerne la prise en compte des vulnérabilités par les équipes PSIRT. Il s'agit de la vulnérabilité Java qui a impacté Mac OS/X (de Apple) en mai 2009.

Une faille vieille de presqu'un an a en effet ressurgi en mai 2009, une fois n'est pas coutume, dans le monde "protégé" des Macintosh. Des programmes d'exploitation visant Mac OS/X ont à ce moment là été diffusés sur Internet. Ils utilisaient une faille majeure dans l'environnement Java, découverte en août 2008, et corrigée par l'éditeur Sun en décembre dernier. Seule la firme à la "Pomme" (qui reconditionne le composant Java pour ses systèmes) n'avait pas encore intégré les correctifs liés à celle-ci pour ses systèmes Mac OS X. Apple a finalement publié les correctifs pour Mac OS X le15 juin 2009.

Voilà ce que nous disions de cette vulnérabilité dans notre bulletin mensuel :

> *Le 25 mai dernier, nous avons émis le Danger Potentiel **CERT-IST/DG-2009.007** suite à la publication de programmes exploitant une vulnérabilité dans l'environnement Java JRE, susceptible d'être utilisée par des sites web malveillants pour compromettre des systèmes Mac OS X. Bien que le premier programme soit un programme de démonstration de type "Proof-Of-Concept (PoC), le second est un programme d'exploitation fonctionnel utilisé lors du concours "Pwn2own" à la conférence CanSecWest 2009, en mars 2009. Cette vulnérabilité (CVE-2008-5353), corrigée dans les systèmes autres que Mac OS X depuis décembre 2008 (cf. avis Multiples vulnérabilités dans les environnements JRE de Sun) n'a jamais été corrigée par l'éditeur Apple. Rappelons que celle-ci permet à une page web malicieuse d'exécuter des commandes arbitraires sur le poste d'une victime navigant sur cette page avec les privilèges de l'utilisateur. L'éditeur n'a toujours pas publié de correctif officiel pour cette vulnérabilité. Cette vulnérabilité est suivie par le Cert-IST dans le hub de crise "[Mac OS X Java] Vulnérabilité Java sous Mac OS X (CVE-2008-5353)".*

# 5) Conclusion

L'année 2009 a été, par rapport à 2008, une année de continuité : les grandes tendances de 2008 se sont confirmées et affinées en 2009.

Tout d'abord, tout **comme en 2008, les attaques 2009 visent avant tout le poste de travail de l'utilisateur. Mais ces attaques sont devenues plus discrètes et moins massives qu'elles n'ont été en 2008**. Par exemple il n'y a pas eu en 2009 de phénomène similaire aux grandes vagues d'attaque en SQL-Injection qui avaient été vues au printemps 2008. La menace est globalement toujours aussi forte (le nombre d'avis émis par le Cert-IST en 2009 reste globalement stable d'année en année) mais les attaques sont aujourd'hui plus discrètes.
Pour les entreprises, ce constat doit être analysé avec soin, car s'il semble aujourd'hui que le risque d'attaque massive diminue, le risque d'attaque ciblée lui augmente constamment. L'affaire Aurora (nom de l'attaque qui a touché Google et d'autres entreprises américaine fin 2009 et début 2010) expose en plein jour, ce risque d'attaque ciblée, à caractère de d'espionnage industriel, qui croit de façon permanente depuis au moins 2005.
Dans notre "Une" du bulletin Cert-IST de juillet 2005 nous disions:

> *Le **risque d'espionnage industriel** à l'aide de chevaux de Troie spécialisés, que nous avons évoqué à la "Une" du bulletin précédent, semble se concrétiser. En effet, après la mise en garde du NISCC, l'US-CERT (le CERT du gouvernement des Etats-Unis) puis le CIAC (le CERT du Department of Energy des Etats-Unis) ont à leur tour émis ce mois-ci des alertes sur ce type d'attaques ciblées. Il nous semble donc souhaitable que chaque entreprise, si elle ne l'a pas déjà fait, analyse l'exposition de son Système d'Information à cette menace. Les moyens de protection applicables ici ne sont pas spécifiques au domaine informatique et reposent sur deux éléments clés : la sensibilisation des utilisateurs et la protection systématique des informations "société".*

Ce risque montant est désormais une préoccupation majeure des RSSI. Il traduit en fait un changement de profil de l'attaquant. La lutte informatique n'a plus aujourd'hui pour objectif de simplement repousser les "hackers" qui tenteraient de percer les défenses informatiques de

l'entreprise. Elle doit aujourd'hui combattre le "cyber-crime", c'est-à-dire les attaques organisées qui utilisent toutes les formes de faiblesses informatiques (failles techniques, manipulation de l'information, ingénierie sociale, etc…) pour mener à bien une attaque motivée. Pour ces attaquants l'informatique est un outil, et comme cet outil a pris une place prédominante dans la société, il devient un vecteur incontournable pour les attaques.
Nota: Le Cert-IST n'est bien sûr pas le seul à faire ce constat. On pourra par exemple trouver des analyses similaires auprès d'organismes comme ShadowServer ("Cyber Espionage: Death by 1000 Cuts") ou Deloitte ("Cyber crime: a clear and present danger").

Ce constat renforce une autre observation que nous faisons depuis plusieurs années et qui ne s'est pas démentie en 2009 : **la professionnalisation des acteurs**, aussi bien des attaquants que défenseurs. En 2008, nous avions noté que les attaques étaient plus structurées et plus professionnelles qu'avant, mais que les réactions des entités qui luttent contre ces attaques s'étaient montrées plus efficaces et plus déterminés. En 2009, certains constructeurs nous ont montrés également que leur capacité de réaction pour traiter les vulnérabilités découvertes dans leurs produits s'était renforcée. Les grandes campagnes de correction que nous avons vues en 2009 (et que nous avons analysées au chapitre 4) ne sont pas médiatiques et peu d'organismes de veille à notre connaissance en ont parlés. Elles sont pour nous révélatrices d'un gain en maturité des défenseurs et d'une capacité de réaction qui va croissante. Elles apportent également aux entreprises la possibilité d'une meilleure gestion de leur cycle de "patch management". Par exemple la publication à intervalle régulier (et préprogrammé) de correctifs de sécurité par les constructeurs permet à l'entreprise de prévoir le cycle de déploiement des correctifs de sécurité et de ne déclencher des déploiements "hors cycle" que face à des événements exceptionnels.

Globalement pour l'entreprise, le paysage actuel sur le front des attaques se compose de plusieurs phénomènes :

- **Un bruit de fond récurrent de menaces traditionnelles qui inclut par exemple les virus, les spam et le phishing.** L'entreprise n'est pas spécialement visée par ces attaques mais elle y est confrontée parce que cette menace est omniprésente sur Internet.
- **Quelques attaques opportunistes** qui peuvent parfois percer ses premières défenses parce qu'une nouvelle vulnérabilité découverte a été exploitée massivement (attaque en "0-day" ou ver se propageant sur Internet). Nous qualifions d'opportunistes ces attaques parce que soit elles ne visaient pas spécialement l'entreprise (l'attaquant recherchait des sites où la vulnérable X ou Y était présente mais ne visait pas particulièrement l'entreprise) soit elle n'attaque pas en profondeur le S.I. de l'entreprise (l'attaquant s'arrête à sa première cible sans profiter de son avantage pour percer en profondeur les défenses).
- Et aussi des **attaques ciblées** menées par des attaquants professionnels et construite spécifiquement pour tirer partie des faiblesses identifiées pour l'entreprise visée.

Dans une attaque ciblée, le maillon humain est souvent le plus faible (le plus difficile à "sécuriser" ?) et il n'est donc pas étonnant que les attaques visant le poste de travail soient les plus courantes désormais. Les attaques PDF ont en particulier connues une croissance importante en 2009. On peut prévoir sans risque de se tromper qu'en 2010 PDF sera un vecteur majeur d'infection.

# Fin du document