Bilan Cert-IST 2007 des failles et attaques

Avant Propos

Le Cert-IST a pris l'habitude, lors des changements d'années, de présenter un « retour sur » l'année écoulée, pour se rappeler les grands moments, dégager des tendances, et parfois se hasarder à quelques prévisions.
En 2006 nous avons pour la première fois publié un Top 20, qui grâce au principe de notre hub de crise, reposait sur les principales menaces signalées au fil de l'eau. De même, la « nouvelle » formule du bulletin mensuel du Cert-IST, avec la une et les attaques du mois, permet également de signaler tous les mois les évènements et réfléchir aux évolutions.

Le bilan annuel est donc de plus en plus l'occasion de réexaminer les attaques qui ont attiré notre attention, pour en dégager l'évolution sur l'année.
Comme nous l'avons déjà dit, c'est également l'occasion du jeu de la prospective (et de comparer la réalité constatée avec les prévisions que nous avons eu l'imprudence de publier et de laisser entre les mains de quelques témoins).

Rappel 2006

La conclusion sur l'année 2006 était que la menace pour les entreprises avait changé. Les années 2001 à 2005 avaient été celles des attaques virales massives qui paralysent les réseaux d'entreprises (avec par exemple : Nimda et CodeRed en 2001, Slammer en 2003, Sasser en 2004, et Zotob en 2005). Ce temps nous paraissait, début 2007, révolu : « Aujourd'hui il n'y a plus d'attaque massive et bruyante ».

Au premier abord, la vie des RSSI était donc plus tranquille, mais ces apparences étaient trompeuses. « Au cours de ces années, l'expertise des attaquants (et le nombre de personnes capables de devenir attaquants) se sont développés, la recherche de faille s'est automatisée et systématisée (au moyen d'outils telles que les "fuzzers") et la menace technique pour les systèmes d'information est de nos jours bien plus grande que ce qu'elle était il y a cinq ans ».
Pour nous la menace était devenue plus pernicieuse : beaucoup plus discrète, et beaucoup plus puissante.

Tendances 2007

Nous pouvons d'ores et déjà annoncer la confirmation et l'amplification de cette tendance sur 2007, avec une étape supplémentaire dans la professionnalisation :

- la professionnalisation des outils et codes malveillants qui se traduit par leur sophistication de plus en plus grande (mpack, stormworm/zhelatin …)
- la professionnalisation des agresseurs, avec au-delà de la criminalisation de l'escroquerie électronique (phishing et autres « xxx-ing », comme disait un invité prestigieux du Forum 2007), les premières attaques massives de caractère cyber-terroriste. On a beaucoup parlé des offensives des « hackers chinois », pour nous, le véritable événement sur lequel nous disposons de données factuelles a été l'offensive en DDOS contre les infrastructures de l'Estonie.

L'année 2007 a donc été marquée par une progression d'attaques dirigées, rarement massives, souvent ciblées et en tout cas de plus en plus sophistiquées.
Les véritables menaces ont le plus souvent été des 0-day, comme si les processus de "patch management" de plus en plus efficaces (que ce soit au sein des entreprises ou du grand public) rendaient les attaques post-avis moins intéressantes.
La sortie extrêmement médiatisée de l'iphone fin 2007 a suscité quelque intérêt de la part de la communauté des hackers, et il est possible que ce type de "smartphone" multimédia communiquant intègre rapidement le palmarès 2008.
Plus généralement, les attaques visant le « multimedia » (de la VoIP à la vidéo en passant par l'IM) bien que présentes en 2007 (cf les vers exploitant youtube, quicktime ou skype) n'ont toujours pas pris l'ampleur que nous envisagions dans les précédents bilans.

Encore une fois, on retiendra de l'année 2007 non pas des attaques contre des nouveaux moyens de communication, mais surtout le phénomène « Storm Worm ». Ce fait marquant de l'année aura démarré de manière presque anodine en janvier, par des spams relatifs aux tempêtes en mer du nord (d'où son nom).
Il a connu un premier palier technique majeur en avril, avec des variantes qui commençaient à attirer l'attention de par leur sophistication, tout en ayant une propagation ne justifiant pas véritablement une alerte.

On peut considérer que « Storm Worm » est l'aboutissement d'une série de travaux sur lesquels nous avons attiré votre attention lors du Forum Cert-IST 2006. Ainsi il consacre la fusion des attaques : association de la propagation d'un spam et/ou d'un cheval de Troie, infection par la navigation web, puis sur le poste infecté, techniques de furtivité, de rootkit, de défense active, et constitution d'un botnet.
Ce botnet est de plus difficile à détecter et éradiquer, en particulier sur une infrastructure opérateur/grand public, car il utilise (au lieu d'un classique serveur IRC) un modèle P2P totalement décentralisé (utilisation du protocole "Overnet" qui est la forme la plus aboutie de système P2P décentralisé). D'une part il se fond dans le trafic P2P habituel (typiquement eMule) d'autre part, il est très difficile de lui associer une signature réseau (pas de ports fixes, trafic UDP, etc…) sans recourir à des solutions complémentaires telles que le DPI (Deep Packet Inspection).

Un autre phénomène important de 2007 a été (surtout depuis septembre) une augmentation importante du spam. Plusieurs de nos adhérents nous ont signalé ce phénomène, l'augmentation a été tellement subite que certains sites se sont demandés s'ils subissaient des attaques (de type "mail bombing"). Ce phénomène étant apparu au travers de demandes de support sur incident, il n'en a pas été fait mention dans nos bulletins pour des raisons de confidentialité aujourd'hui caduques.

Conclusion et prospective 2008

Il nous apparaît aujourd'hui que 2008 ne connaitra une recrudescence d'attaques sur des nouveaux moyens de communication que si ceux-ci commencent à intéresser les cybercriminels en bande organisée. Sinon 2008 connaitra son lot habituel de vulnérabilités et 0-day plus prosaïques, de chevaux de Troie plutôt que de virus etc …Par contre, l'expérience Storm Worm a montré que ces attaques « classiques » seront de plus en plus sophistiquées et efficaces, et que les RSSI qui baisseraient leur garde (ces attaques étant désormais plus discrètes) risquent de devoir faire appel à des structures aussi organisées que les assaillants pour répondre aux attaques en 2008.
Une telle situation mettrait bien évidemment en valeur les compétences dans la gestion de crise du Cert-IST, si ce n'est qu'il est préférable, pour nous aussi, de faire de la prévention plutôt que de la réaction …

Chronologie des principales failles et attaques 2007

Pour illustrer et étayer notre analyse, replongeons nous dans les failles et attaques de 2007, et commençons par ce que la presse appelle un « marronnier », la question « qui de Windows, Macintosh, Firefox ou Linux a été l'environnement le plus vulnérable ?

1er trimestre : Apple, Arcserve, Ver Solaris … et quand même Microsoft

Et bien une fois n'est pas coutume (encore que, diront les véritables experts), janvier 2007 aura commencé par de nombreux "0day" **Apple** révélés et publiés dans le cadre du "MoAB" ("Month Of Apple Bug") ainsi que des vulnérabilités exploitées dans la solution de sauvegarde **"BrightStor ARCServe Backup"** (**DG-2007.001**). En effet, de nombreux programmes d'exploitation ont été diffusés permettant de prendre le contrôle à distance des plates-formes Windows hébergeant cette solution. Dans ce cadre, nous avons émis successivement sur ce problème un message dans la liste "Vuln-coord", un avis de sécurité (**AV-2007.025**), et finalement une pré-alerte (**DG-2007.001**).

La vulnérabilité exploitée dans la solution "**BrightStor ARCServe Backup for Laptops & Desktops**" publiée en février concerne un produit logiciel distinct du précédent, dédié aux stations de travail et ordinateurs portables.
Les vulnérabilités de type "0day " concernant le monde Apple qui ont été révélées chaque jour durant le mois de janvier ont fait l'objet d'avis de sécurité (**AV-2007.002**, **AV-2007.018**).

La fin du mois février a été marquée par l'apparition d'un **ver sous Unix** (**CERT-IST/AL-2007.003**). Ce phénomène exceptionnel est dû en grande partie à la simplicité d'exploitation de la vulnérabilité utilisée. En effet, cette faille présente dans le démon "**telnetd**" des systèmes **Solaris 10 (et 11)** est facilement "scriptable" (elle peut être automatisée dans un fichier de commandes) et le ver qui est apparu est en fait un simple "shell-script" (fichier de commandes Unix). La propagation de ce ver a été limitée grâce au filtrage quasi-général de ce protocole à l'entrée des réseaux d'entreprise. Néanmoins, ce ver a été constaté en **France** par le Cert-IST.
Le Hub De Crise intitulé "**0-day Solaris 10**" (https://wws.cert-ist.com/fra/hub/0daysolaris10/) a permis de suivre l'évolution de cette menace.

Il y aura toutefois de nombreuses attaques en "0day" [découvertes] dans **Microsoft Office** (CVE-2007-0515 et CVE-2007-0671) en plus de celles affectant des failles déjà identifiées en décembre 2006 (CVE-2006-5994, CVE-2006-6456, CVE-2006-6561). **Il y avait donc en janvier 5 failles non corrigées** par Microsoft concernant la suite "Office". Ces vulnérabilités furent suivies dans le "Hub de crise" du Cert-IST sous l'intitulé "**0-day Word 12/06**" et ont fait l'objet d'une pré-alerte Cert-IST (**DG-2007.002**).

Les documents Microsoft Office ont continué en février à constituer une menace significative. Sur la fin de l'année 2006, les vulnérabilités liées aux **outils bureautiques de Microsoft** (Word, Excel, PowerPoint) avaient commencé à prendre le pas sur les vulnérabilités Windows ou IE. Et bien que Microsoft publie régulièrement des correctifs pour les vulnérabilités connues, de nouvelles vulnérabilités apparaissent dans le même temps. Ainsi en février, juste après la publication par Microsoft des correctifs pour ses outils bureautiques (**CERT-IST/AV-2007.070**, **CERT-IST/AV-2007.071**), une nouvelle faille sous Word 2000 a été publiée. Cette dernière a été suivie dans le Hub De Crise intitulé "**0-day Word 02/07**" (https://wws.cert-ist.com/fra/hub/0-dayword02_07/).

Alors que le mois de mars a semblé dans l'ensemble très calme au niveau des failles Microsoft (pas d'avis de sécurité lors du "patch Tuesday" ce qui est fort rare), la fin de mois a vu culminer la tendance des attaques en 0-day… En effet il a fallu attendre l'avant dernier jour du mois pour voir de nouveau une attaque **"0-day" via une nouvelle vulnérabilité dans la gestion des fichiers "ANI" ("ANImated cursors") de Windows** (cf. Danger : **CERT-IST/DG-2007.004**). Cette faille sans correctif initialement, est présente dans les plates-formes Windows 2000, XP, 2003 et même Vista… (cf. Avis : **CERT-IST/AV-2007.140**). Même si pour être exploitée elle nécessite une interaction de la part de l'utilisateur (au travers d'un lien web, fichier ou e-mail malicieux), de nombreux codes malicieux ont vu le jour très rapidement tels que les vers chinois et divers variantes "**Fubalca**" ou "**Anito**" (cf. Avis **CERT-IST/AV-2007.141**).
Cette faille ayant un fort potentiel, Microsoft a publié, hors calendrier, un correctif le mardi 4 avril 2007. Le Hub De Crise intitulé "**0day ANI Windows**" a permis de suivre cette menace.

Mentionnons pour boucler le 1er trimestre en mars une autre vulnérabilité découverte dans le service "Mediasvr.exe" du logiciel de sauvegarde "**CA BrightStor ARCserve Backup**" versions r11.5 et antérieures qui permet à un attaquant distant de prendre le contrôle du système vulnérable (Avis **CERT-IST/AV-2007.143** et hub de crise "**ARCServe 03/07**"). Cette vulnérabilité a fait l'objet d'un 0-day.

2ème trimestre : sophistication (storm worm, mpack) et cyber-terrorisme (Estonie)

La vulnérabilité DNS des serveurs Microsoft Windows 2000 et 2003, pour laquelle un correctif a été publié le 8 mai, est la vulnérabilité majeure du mois d'avril (Avis CERT-IST/AV-2007.165 et Danger CERT-IST/DG-2007.005). Il s'agit de la première faille "serveur" depuis longtemps (les autres failles Microsoft survenues les mois précédents étaient des failles impactant plutôt les postes clients). Elle a donc suscité une mobilisation des responsables des infrastructures informatiques, mais aussi de l'ensemble de la communauté SSI. Par exemple, chose sans précédent à notre connaissance, des scans ont été réalisés pour identifier les machines vulnérables et pour en prévenir les propriétaires. Cette vulnérabilité a été suivie par le Cert-IST dans le Hub De Crise intitulé "Windows DNS RPC".

Le mois d'avril a aussi vu la première propagation signalée du ver "**Zhelatin.CQ**" (connu aussi sous les noms "Glowa", "Nuwar", "Mixor", "Peacomm") et sa variante "**Storm Worm**" (connue aussi sous les noms suivants "Peacomm!zip", "NUWAR.ZIP", "NUWAR.AOP").
« Ces vers informatiques se propagent à travers des e-mails en anglais contenant une pièce jointe malveillante (fichier ".exe" pour "Zhelatin.CQ" ou un fichier "zip" chiffré pour "Storm Worm"). Une fois présents sur le système, ils installent un "rootkit" pour dissimuler leur activité, tentent de désactiver les logiciels de sécurité (anti-virus, garde-barrière personnel) et construisent un réseau "Peer-To-Peer" (P2P). Ces vers sont décrits dans l'avis CERT-IST/AV-2007.151 et la propagation de "Storm Worm" a fait l'objet d'un message Virus-Coord. »
Nous avons cité in extenso le commentaire réalisé en direct sur cette attaque.
Nous verrons plus loin que ce phénomène, d'une sophistication aussi élevée que sa propagation a paru faible au début, sera l'un des grands faits et tendances de l'année : une attaque pernicieuse, d'une grande puissance (certains membres de la communauté du Cert-IST en sentiront les effets sans jamais être mis en difficulté) mais qui ne sera jamais suffisamment massive pour faire l'objet d'une alerte.

Le mois de mai 2007 a été calme en termes de vulnérabilités. Il aura surtout **été marqué par une** attaque de grande envergure**, utilisant des techniques par saturation (déni de service distribué - "DDoS"), contre de nombreux sites web situés en Estonie.**
Face à cette attaque ayant vraisemblablement **un caractère politique** caché, les autorités internationales ont souhaité coordonner les efforts afin de faire cesser cette attaque et d'identifier les techniques/systèmes utilisés par ces auteurs. La communauté internationale et Européenne des Certs a été mise à la disposition des Autorités Estoniennes. Les actions, par exemple de mener des investigations sur la base d'adresses IP ayant participé à cette attaque (et étant localisées en France, pour ce qui concernait le Cert-IST), ont été coordonnées par le Cert de l'OTAN, le NATO Computer Incident Response Capability - Coordination Center **(http://www.ncirc.nato.int/index.htm).** Il a été remarqué que la plupart des machines mises en cause étaient des PC domestiques hébergés chez des fournisseurs d'accès grand public. Les fournisseurs d'accès ont été alors contactés.

A noter que cette analyse / retour d'expérience jouera un rôle non négligeable dans la prudence dont le Cert-IST ou certains de ses homologues feront preuve pour commenter des attaques mettant en cause la nationalité des agresseurs, en particulier le « feuilleton » des hackers chinois.

En juin encore, il n'y a pas de crise significative, en termes d'attaques ou de menaces pour notre communauté.
Cependant, dans le même temps, des incidents ciblés de plus en plus professionnels ont aussi été découverts. La tendance se confirme donc et s'accentue : attaques ciblées, technicité accrue et professionnalisation.

La dimension multinationale est également désormais omniprésente : les outils d'attaques sont développés en un point du globe, puis utilisés pour attaquer des cibles dans un autre pays, en utilisant éventuellement des serveurs tiers compromis situés encore ailleurs.

L'analyse de ces phénomènes, et les moyens pour y répondre, sont donc au cœur de nos préoccupations, comme le montrent les sujets traités lors de notre Forum annuel (consacré à la coopération multinationale) qui s'est déroulé le 7 juin 2007, ou à la conférence du FIRST qui a réuni les CERT du monde entier à Séville du 17 au 22 juin dernier.

Pour illustrer la tendance, le Cert-IST signalait en juin une industrialisation de certains outils de piratage ciblant les postes des utilisateurs au travers de leurs navigations web. Il a été en effet constaté qu'un outil payant d'attaque, proposé par des hackers russes, et nommé "**MPack**", a été utilisé à grande échelle en Europe (plus de 10 000 sites web compromis). Un message dans la liste "Vuln-Coord" ("Sites web compromis et logiciel "MPack"/Hacked web sites and "MPack" software") a été émis à ce sujet. Nous l'avons complété par une analyse technique de cette attaque dans un des articles bulletin ("MPack" ou la commercialisation d'un outil de hacking").

Cet outil est un logiciel PHP s'exécutant sur un serveur web via des sites web compromis sur lesquels une redirection web vers le serveur "MPack" est ajoutée au travers d'une directive IFRAME insérée dans les pages web. Dès lors, en fonction du client web (IE, Firefox, ...) et du système d'exploitation (Windows, Linux, ...) utilisés par la victime lors de sa navigation sur un site web ainsi compromis, la solution "MPack" attaque cette dernière avec des programmes d'exploitation adéquats sélectionnés dans sa base de données.

Ainsi, une fois qu'une porte d'entrée sur le poste de la victime a été découverte, l'outil "MPack" installe sur le système divers outils malveillants (virus, chevaux de Troie, "keyloggers", "bots"). Dans le cas qui nous intéresse, le cheval de Troie "Torpig" (souche datant de 2005) a été couramment rencontré par les victimes. Ce cheval de Troie a pour principale fonction de voler les identifiants bancaires sur le poste infecté.

A la fin du mois, cette technique d'attaque a été déclinée au travers d'e-mails de spam anglais ("*You've received a greeting ecard from a partner!*" ou autre) contenant des liens (URL) vers des serveurs "MPack".

Il a été également remarqué l'apparition d'un "malware" très élaboré, nommé "**ArpIframe**", qui permet d'effectuer des attaques de type "Man-In-The-Middle" vis-à-vis des connexions web (HTTP) des utilisateurs situés sur le même brin réseau que le PC infecté. Ce "malware" qui pourrait lui aussi être couplé à un outil comme "MPack" a également fait l'objet d'un article sur "ArpIframe" .

3ème trimestre : « URI handling », storm worm, quicktime, un concentré de 2007 …?

Le "marché" des failles de sécurité évolue. D'un côté tous les éditeurs ont une politique de publication rodée, et pourtant certaines failles sont de plus en plus tenues secrètes. Quand on sait qu'une faille peut valoir 24 000 dollars vendue à une société connue, on imagine bien que la même faille vaudra encore plus cher sur le « marché noir ». A ce prix là, il est peu probable qu'une telle faille apparaisse sur un forum public...
Globalement, il y a donc plus de failles … dont on parle de moins en moins ouvertement tant qu'elles n'ont pas été reconnues par l'éditeur. Cette évolution constitue pour les CERT un défi permanent : il faut en effet être attentif à toutes les failles, et savoir détecter au plus tôt les situations qui pourraient dégénérer en crise.

Le Cert-IST a émis en juillet un "**Danger Potentiel**" (**CERT-IST/DG-2007.006** du 27/07/2007, actualisé le 30 puis le 31/07/2007), suite à la découverte d'une **vulnérabilité 0-day dans Firefox 2.x**. Les informations techniques publiées le 27/07/2007 sur Internet rendaient en effet triviale l'écriture d'une page web malicieuse visant à infecter les utilisateurs de Firefox visitant le site web malicieux depuis un poste Windows XP « vulnérable », c'est-à-dire qu'il faut naviguer avec Firefox, à partir d'un PC sur lequel Internet Explorer 7 est également installé (c'est un pré-requis pour la réussite de l'attaque, mais une configuration courante).
A notre connaissance, il n'a pas été observé en juillet d'attaque d'ampleur significative utilisant cette faille. Le 31/07/2007, un correctif est disponible pour Firefox 2.x (cf. l'avis **CERT-IST/AV-2007.353**).

Dans le domaine des virus, nous avons observé début juillet une augmentation importante d'**e-mails malicieux** invitant les destinataires à se rendre sur un site web pour télécharger (ou visualiser) une **carte de vœux ("Greeting Card")**. Ces attaques (baptisées "Storm Worm" par certaines sources, du nom du virus véhiculé par les e-mails) ont fait l'objet de l'annonce "**VirusCoord-2007.006**" dans notre liste "Virus-coord". C'était la deuxième signalisation du phénomène Storm Worm sur l'année.

Storm Worm sera encore l'une des « stars » du mois d'Août :
La fin du mois d'août 2007 a été marquée par la vague toujours soutenue d'e-mails de Spam, phénomène appelé "**Storm Worm**", qui a été détecté par les infrastructures de surveillance durant tout cet été.

"Storm Worm" est la dénomination générique d'une activité malveillante basée sur l'ingénierie sociale, se propageant sous forme d'un e-mail de Spam invitant le destinataire à se rendre sur un site web pour télécharger (ou visualiser) une photo, carte de vœux, une vidéo, cliquer sur une URL et entrainant par la suite la compromission du poste de la victime (téléchargement de fichiers malveillants de type cheval de Troie ou utilisation d'une faille de sécurité cf. **SANS**).

Nous vous avons fait part d'exemples d'ingénierie sociale utilisée dans le message **Virus et "Greeting Cards"** posté début juillet dans la liste "Virus-Coord". Ce phénomène s'est poursuivi les semaines suivantes sous différentes formes (liens "YouTube" cf. **SANS**) signalées dans le message **Multiplication des Spams malveillants ("Storm Worm" ou "Zhelatin")**.

Une vague de scan ciblée suivie de tentatives d'attaques ont également été détectées fin août 2007 sur tous les continents. Ces attaques concernaient la solution antivirale **"ServerProtect" de TrendMicro**. L'éditeur **a confirmé**, après quelques hésitations sur la vulnérabilité exploitée, la présence d'attaques liées à une ancienne vulnérabilité (**CERT-IST/AV-2007.089**) datant du mois de février 2007.

A cet effet, le Cert-IST a ouvert le suivi de la menace intitulée "**Trend TCP 6158**" dans son "Hub de Gestion De Crise" afin de suivre l'évolution de ce problème.
Mi-septembre, le CERT Renater a mentionné dans ses statistiques hebdomadaires (**2007/STAT036**) que des scans sur le port TCP 5168 avaient été relevés dans sa communauté. Ces scans laissaient présager des attaques sur ce type d'équipement vulnérable.

Le mois de septembre a été marqué par une vulnérabilité critique dans le lecteur multimédia **QuickTime** d'Apple. Des programmes de démonstration ont été largement diffusés sur Internet et testés par le Cert-IST. Face à cette menace, le Cert-IST a ouvert un "Hub de Crise" intitulé "**QuickTime QTL**" pour suivre l'évolution de cette vulnérabilité. Apple a corrigé cette vulnérabilité début octobre.

Notons également le début d'une rumeur persistante sur une faille dans le **lecteur PDF** (**VulnCoord-2007.022**).

Enfin, après les annonces de différents gouvernements contre des **attaques cybernétiques semblant provenir de la Chine**, le "Department of Homeland Security" US (DHS) a confirmé au bout de plusieurs mois qu'il avait subi en avril 2007 une telle attaque. Le DHS a déclenché une **polémique** en mettant en cause ses prestataires et les moyens qu'ils avaient déployés. C'est l'occasion de rappeler l'importance de la prise en compte de ce type de menace (espionnage industriel ou stratégique), mais aussi l'importance de la séparation des rôles entre les fonctions d'exploitation et de contrôle.

Il est également à noter la propagation toujours constante en septembre des vers de type "**Storm Worm**" (ou "**Zhelatin**") sur Internet. Cette constance est due à l'apparition régulière de nouvelles variantes qui prennent comme thèmes des faits d'actualité. Un message dans la liste "Virus-Coord" (**VirusCoord-2007.007** - Multiplication des Spams malveillants ("Storm Worm" ou "Zhelatin")) a été diffusé en début de mois pour maintenir le niveau de vigilance dans la communauté IST.

Quatrième trimestre : des attaques toujours plus pernicieuses / indirectes

Le mois d'octobre a été marqué par la médiatisation d'un problème générique impactant la **gestion des URI** par les systèmes Microsoft Windows lorsque la version 7 d'Internet Explorer est installée. Cette menace été regroupée dans le Hub de Crise intitulé "**URI Handling/IE7**". Il est à noter que cette vulnérabilité n'est pas exploitable directement sur le système, mais peut être mise en œuvre au travers d'applications tierces gérant des URI (Firefox, Adobe Acrobat, Outlook, Skype, …). Ainsi plusieurs avis de sécurité ont été émis par le Cert-IST (**CERT-IST/AV-2007.353** pour Firefox, **CERT-IST/AV-2007.459** pour Acrobat) concernant dans un premier temps ces applications. De même, la facilité d'exploitation de ce problème via le logiciel Acrobat a entraîné la publication par le Cert-IST d'un DanGer potentiel (**CERT-IST/DG-2007.008**) et l'ouverture d'un Hub de Crise "**URI handling/PDF**". Un Hub de Crise avait déjà été ouvert à ce propos pendant l'été concernant le navigateur Firefox ("**Firefox %00 URI**"). De son côté, Microsoft a également réagi face à la dangerosité de cette vulnérabilité pour travailler actuellement sur l'élaboration d'un correctif (Avis **943521**).

La vulnérabilité facilement exploitable au travers de l'application Acrobat (**CERT-IST/AV-2007.459**) a rapidement donné lieu à des programmes d'exploitation et à la diffusion au travers de messages de Spam de fichiers PDF malveillants ("**Pidief**", "**AdobeReader.K**"). Néanmoins, la manipulation de certains fichiers PDF entraînait le téléchargement d'un cheval de Troie détecté de manière générique par les anti-virus à jour (cf. Hub de Crise "**URI handling/PDF**").

Le monde Apple a été également touché en octobre par un nouveau cheval de Troie "**DNS changer**" qui a été diffusé sur Internet (SANS - http://isc.sans.org/diary.html?storyid=3595). Ce cheval de Troie se présente sous la forme d'un codec (fichier ".dmg") et est recensé sur des sites à caractère pornographique. Une fois téléchargé et exécuté par la victime (le mot de passe administrateur est néanmoins demandé lors de l'installation), ce cheval de Troie change les paramètres DNS du système Mac OS X. Cette modification détourne ainsi les requêtes DNS de l'utilisateur vers un serveur de noms malveillant en vue d'attaques de type "pharming"/"phishing". Le cheval de Troie communique également des informations sur le système de la victime à un serveur externe.
Bien que le phénomène soit connu et reste pour l'instant encore marginal par rapport au monde Microsoft, ce malware était assez représentatif, pas son mode d'action de la professionnalisation et sophistication croissante des vecteurs d'attaques déjà relevée.

Nous avons signalé au premier trimestre le glissement des vulnérabilités et des attaques affectant les logiciels « système » (Windows et IE) vers les logiciels applicatifs (Word, Excel …). Le Cert-IST observe en novembre une deuxième évolution de cette tendance à propos des vulnérabilités découvertes. En effet, si le nombre de vulnérabilités critiques impactant directement les systèmes d'exploitation et les navigateurs web semble toujours en léger recul, on voit par contre une augmentation des vulnérabilités qui impactent des logiciels "standards" pouvant être appelés depuis un navigateur web. Le dernier exemple est le cas de la vulnérabilité du lecteur multimédia QuickTime (avis **CERT-IST/AV-2007.536** et Hub de Crise "**QuickTime RTSP**"), mais on pourrait citer aussi des vulnérabilités découvertes au quatrième trimestre sur les lecteurs Acrobat Reader, Real Player, Windows Media Player, ...
Tout se passe comme s'il était devenu trop difficile de trouver (ou d'exploiter) des failles dans les systèmes d'exploitation Windows, Internet Explorer et Firefox, et qu'à défaut, certains chercheurs de failles se tournent maintenant vers d'autres produits moins explorés jusqu'à présent.

Le 26/11/2007, le Cert-IST a donc ouvert un Hub de Crise sur la vulnérabilité "**QuickTime RTSP**" (avis de sécurité **CERT-IST/AV-2007.536**). Le 30/11/2007, le Danger Potentiel **CERT-IST/DG-2007.009** ("Vulnérabilité RTSP critique dans QuickTime d'Apple") a été émis suite à une multiplication des programmes d'exploitation rendus publics sur cette faille. Sans rapport d'attaques de grande ampleur utilisant cette faille, le Cert-IST n'a pas eu à déclencher une alerte, cependant la situation est restée préoccupante. En particulier des attaques ponctuelles semblent exister.

Parmi les attaques du mois de novembre, nous avons aussi relevé une étude, menée par l'éditeur "Sunbelt Software", indiquant que près de **40 000 sites web indexés par le moteur de recherche Google contenaient des "malwares"** destinés à compromettre les postes des internautes. Il semble s'agir d'une attaque délibérée visant à utiliser Google pour attirer les internautes vers des sites malveillants. Ces sites se font indexer sur des thèmes très divers qui n'ont aucun lien avec leur contenu, mais dont la popularité peut attirer un nombre important de victimes. Il est à noter que Google n'est pas le seul moteur de recherche victime de ce phénomène car les moteurs Yahoo et Microsoft Live sont également touchés.