Bilan 2006

Il est de bon ton, 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 (ou comparer la réalité constatée aux prévisions qu'on avait eu l'imprudence de publier et de laisser entre les mains de quelques témoins).
A la télévision, on appelle cela un « best of », et la tentation nous a effleuré de faire un copier-coller des éditos et attaques du mois de toute l'année …
D'ailleurs c'est ce que nous avons commencé par faire, et l'exercice a révélé quelques heureuses surprises …

Avril 2004
Nous sommes d'accord, cette date ne fait pas partie de 2006. Elle l'annonçait néanmoins. 2004 fut l'année des Virus. On assista à l'infection Mydoom, puis à la « guéguerre » entre Bagle et Netsky. En Avril, un article du « Monde » rendait compte de cette effervescence (et encore, Sasser n'apparaitrait que quelques semaines plus tard) sous un titre prémonitoire : « Les créateurs de Virus informatiques deviennent des mercenaires ». La professionnalisation des créateurs de codes malveillants était sinon née, du moins identifiée.
Elle a atteint son paroxysme en 2006.
En 2006, les professionnels de l'attaque informatique :

- ne construisent plus de virus à diffusion massive,
- visent le portefeuille ou un maximum de cibles vulnérables,
- ciblent et démontent méthodiquement les environnements visés,
- lancent des attaques discrètes et violentes pour être efficaces.

La fin des Virus à diffusion massive

Janvier 2006 :
Le mois de janvier aura connu le dernier sursaut d'une époque révolue et une première attaque symptomatique des nouveaux comportements.
le ver "CME-24" (connu aussi sous les noms "Nyxem", "Kamasutra", ou "Blackworm", et décrit dans l'avis **CERT-IST/AV-2006.026**), programmé pour détruire le 3 février 2006 un grand nombre de fichiers sur les postes infectés, a connu un très large écho médiatique.
Le Cert-IST a été sollicité successivement par "Le Monde", "I-Télévision" et "France-Inter" pour commenter l'ampleur de la crise attendue. Ce ver de conception très classique s'était propagé de façon importante (plusieurs centaines de milliers de postes infectés dans le monde), mais a été très facile à stopper avec une protection anti-virale classique

Et pendant ce temps, la faille WMF (cf. avis **CERT-IST/AV-2005.485**), était exploitée avec un grand opportunisme, en particulier entre Noel et le jour de l'an, puis lors de la période des vœux de nouvel an. (Toute ressemblance avec une situation récente … ne fait que témoigner de l'absence de créativité des auteurs de codes malveillants modernes, dont on rappelle qu'ils recherchent l'efficacité, pas l'originalité,) …
Le déroulement de l'attaque (en "0-day" révélée le 28 décembre, confirmée par Microsoft le 29, montant au niveau Alerte le 2, et corrigée hors planning le 6) est

caractéristique de la brutalité et de la rapidité des attaques que l'on connaitra tout au long de l'année.

En 2006, les codes malveillants les plus utilisés seront des chevaux de Troie, envoyés par SPAM ou qui s'auto-propagent, et ont pour but la constitution de "botnet" ou la capture de données personnelles.

Mai 2006 :
Les nombreux week-ends du mois de Mai sont-ils plus propices à la réflexion, ou aux attaques ? Concernant les attaques, voyons ce que nous écrivions dans le bulletin N°104 et que nous reproduisons ci-dessous intégralement :

Les attaques du mois (Mai 2006)
Le Cert-IST a émis une alerte le samedi 20 mai, aux abonnés du service "24/7", suite à la découverte sur Internet d'attaques utilisant une ***faille*** *encore inconnue dans* ***Microsoft Word****. Cette alerte a ensuite été diffusée (le lundi) à l'ensemble des abonnés (alerte* ***CERT-IST/AL-2006.003****).*

Cette attaque nous parait tout à fait révélatrice de l'évolution des attaques sur Internet:

- La vulnérabilité a été gardée secrète. Elle n'a pas été rendue publique sur les forums de discussion, et **aucun indicateur n'a permis d'anticiper la menace**. Ainsi la chronologie traditionnelle (qui passe par les phases "révélation d'une faille", "publication de programmes de démonstration" puis "attaques") n'a pas été suivie ici, et c'est l'identification d'un virus encore inconnu se propageant sur Internet (le cheval de Troie "Ginwui" – avis **CERT-IST/AV-2006.187**) qui a permis d'identifier la vulnérabilité impactant le logiciel Word de Microsoft.
- Elle a été utilisée de façon ciblée et très limitée. L'alerte Cert-IST a été émise pour anticiper une éventuelle propagation massive de virus utilisant cette faille Word, semblable à celles qui avaient été observées pour "Bagle" (**CERT-IST/AL-2004.001**) ou "Sober" (**Virus Coord 2005-05-03**). En fait, **il n'y a pas eu de propagation massive** et visiblement la faille n'a été utilisée que dans des attaques très ciblées, au sein de certaines organisations. Il est même probable que l'exploitation de cette faille a été stoppée dès que les attaquants ont su que le virus avait été découvert par la communauté.

Des attaques ciblées ... pour de la fraude financière

Février 2006 :
Les techniques mûrissent, comme le Cert-IST en rend compte dans l'article « Les rootkits et la fraude bancaire ».
Quelques extraits significatifs :

> *« Les rootkits sont des programmes permettant de camoufler des éléments déposés par un pirate sur une machine. Ils s'orientent de plus en plus vers des activités liées à la fraude bancaire et viennent compléter dorénavant la panoplie des fonctionnalités des Malwares. »*
> *« Un exemple frappant est l'apparition en Février d'un rootkit ayant comme fonctionnalité principale (hormis sa furtivité) d'intercepter les communications web de l'utilisateur et notamment celles liées à des transactions avec des banques en ligne. »*

« Ce rootkit est détecté par les éditeurs anti-virus comme une variante du cheval de Troie "Haxdoor". »

Mars 2006 :
Après quelques tâtonnements, les cyber-délinquants identifient la bonne cible et passent à la vitesse supérieure : les nombreuses vulnérabilités identifiables dans les navigateurs génèrent une nouvelle vague d'attaques en phishing qui justifiera l'émission d'un communiqué de presse du Cert-IST lorsque trois attaques successives affecteront de grandes banques françaises.

Avril 2006 :
Dans la continuité de mars, on voit de nouvelles failles IE, (Vulnérabilité dans la **gestion des tags HTML "OBJECT" imbriqués** sous Internet Explorer - **FA-2006.060**), et pour prolonger l'analyse de la cybercriminalité, un article du bulletin (Les dessous de l'escroquerie sur Internet) détaille les schémas classiques d'escroquerie sur Internet, par compromission de serveurs web, en exploitant des vulnérabilités peu médiatisées, ou par l'envoi de programmes malveillants à l'acheteur.

Mai 2006 :
Comme déjà évoqué, le mois de mai étant propice à la réflexion, voilà ce que nous écrivions :

> *A LA UNE (Mai 2006)*
> "***Internet = Money***" *: Si l'on en croit l'évolution que nous observons pour les attaques sur Internet (voir notre rubrique "les attaques du mois"), ce slogan s'applique désormais aussi au monde des hackers. Aujourd'hui en effet, les attaques massives (comme "Blaster", "Sasser" ou "CodeRed") et gratuites (pour simplement se faire une réputation) semblent de plus en plus rares. Elles laissent par contre la place à une menace plus pernicieuse : des attaques ciblées, guidées par la recherche d'un gain financier, et ne devant pas laisser de traces. Pour les RSSI et les entreprises, cette évolution (criminalisation et professionnalisation des attaques) représente un réel danger, et elle nécessite le maintien et le renforcement des défenses en place. "Défense en profondeur", "protection du patrimoine" et "sensibilisation des acteurs" en sont, nous semble-t-il, les éléments clés.*

Une analyse méthodique des cibles

Nous signalions dès l'édito du bulletin de janvier 2006 la persistance de la vulnérabilité des Antivirus à la dissimulation des codes malveillants dans des fichiers malformés. Ainsi, plusieurs nouvelles failles étaient découvertes en janvier dans la gestion de certaines archives (ZIP, RAR et ARJ) par les anti-virus de F-Secure (avis **CERT-IST/AV-2006.033**) et de Sophos (avis **CERT-IST/AV-2006.043**). Elles permettaient à un fichier d'archive spécifique de contourner le moteur d'analyse de ces anti-virus, et, dans le cas de F-Secure, de prendre le contrôle des postes utilisant une version vulnérable de l'anti-virus. Ces failles font partie d'**une série de vulnérabilités génériques affectant les logiciels anti-virus**, que le Cert-IST avait commencé à suivre dans son "hub de gestion de crise" à l'automne 2005, et qui feront l'objet de diverses présentations publiques, dont une au Forum Cert-IST 2006.

Ce type de « vulnérabilité générique affectant une famille de logiciels » est également une tendance de 2006, dont on va avoir une illustration en février, et qui sera ensuite expliquée par l'analyse du « fuzzing ».

Février 2006 :
Les utilisateurs de **MacOS X** sont la cible du mois … Les vers "**Leap**" (**CME-4**) et "**Inqtana**" ont eu un impact médiatique important sachant que c'étaient les premiers vers significatifs circulant sur ces plates-formes. De même, la vulnérabilité découverte dans le navigateur **Apple Safari** (**CERT-IST/AV-2006.084**) **et Apple Mail** a attiré fortement l'attention car elle impacte tous les systèmes MacOS X par défaut et pas seulement ces deux logiciels. Elle a donc fait l'objet d'un **Danger Potentiel** , puis d'un suivi dans le hub de crise, qui a permis de détailler les impacts et l'origine de la faille :
Elle exploite le fait que MacOS X associe à chaque fichier des "méta-data" qui décrivent le contenu du fichier (par exemple : type du fichier, application à utiliser pour l'ouvrir, etc...). Le 2 mars, Apple émettait un avis de sécurité (Security Update 2006-001 - #303382) corrigeant un ensemble de vulnérabilités dont celles-ci.
L'ensemble des vulnérabilités corrigées est décrit dans l'avis **CERT-IST/AV-2006.091**.

Mars 2006 :
Les failles les plus notables affectent les navigateurs, ainsi que leur plug-in pour Windows Media Player. La vulnérabilité n'est pas l'apanage des plug-in puisque le lecteur lui-même est vulnérable à une deuxième attaque (**CERT-IST/AV-2006.072**).

Juin 2006 :
La recherche (et la publication) de failles inconnues finit par se faire en pleine lumière, c'est le MoBB de HD Moore… Celui-ci a publié en juin, dans le cadre d'une opération baptisée le "**MoBB**" ("the Month of Browser Bugs"), 31 "bugs" concernant les navigateurs web (un par jour). De là à penser que la succession d'attaques en "zéro-days" qui impactent toute l'année les outils de la suite "**Office**" de Microsoft est due à des recherches similaires …

L'une des suites les plus emblématiques de "MoBB" sera l'alerte **CERT-IST/AL-2006.006**, ("**Exploitation de la faille 'WebViewFolderIcon' dans Microsoft Windows**"), émise le 02/10/2006, après confirmation d'une utilisation active de cette faille sur Internet.

Octobre 2006 :
Le Cert-IST émet ce mois là **huit avis Cert-IST concernant les anti-virus**. Comme nous l'évoquions en juin 2006 lors du Forum 2006 du Cert-IST, il y a visiblement un intérêt intense (et une utilisation systématique des outils de « fuzzing » déjà évoqués … ?) des chercheurs de failles pour l'analyse des anti-virus. En octobre 2006 la plupart des produits phare du marché étaient touchés :

- McAfee (**CERT-IST/AV-2006.400**),
- TrendMicro (**CERT-IST/AV-2006.401**),
- Kaspersky (**CERT-IST/AV-2006.435**),
- ClamAV (**CERT-IST/AV-2006.440**),
- Symantec (**CERT-IST/AV-2006.406**, **CERT-IST/AV-2006.437**, **CERT-IST/AV-2006.441**),
- et Sophos (**CERT-IST/AV-2006.448**).

Novembre 2006 :
Mac OS X (Apple) est de nouveau sous les feux de l'actualité. Si d'un côté Apple a corrigé 31 failles (cf. l'avis **CERT-IST/AV-2006.496**), de l'autre 10 nouvelles failles sont révélées dans le cadre du "**MoKB**" ("Month Of the Kernel Bug").

Décembre 2006 :
Le mois de décembre aurait dû être le mois des failles **Oracle**, dans une opération baptisée the "Week of Oracle Database Bugs" – "WoODB". Mais la société Argeniss a finalement renoncé.

Des attaques plus discrètes (et ciblées) mais très violentes contre Microsoft

Revenons sur l'environnement Microsoft, qui a bien entendu eu sa part d'intérêt de la communauté des chercheurs de failles, et a souvent fait l'objet d'attaques un peu ciblées, très rapides, et finalement assez opportunistes.
Tout comme pour l'attaque WMF en "0-day" de Janvier 2006, ces attaques se produiront souvent en l'absence de tout correctif, voire juste après la publication des correctifs mensuels, bousculant les plannings Microsoft.

Mars 2006 :
Le navigateur **Microsoft Internet Explorer** a été la cible de plusieurs attaques, y compris en "0-day", qui ont donné lieu à deux messages dans la liste de diffusion "Vuln-Coord" (**Vuln Coord 2006-03-22** et **Vuln Coord 2006-03-23**). Suite à la publication d'un programme d'exploitation pour l'une d'entre elles (vulnérabilité "createTextRange()"), le Cert-IST a émis le Danger Potentiel **CERT-IST/DG-2006.003**, et en toute fin de mois l'alerte **CERT-IST/AL-2006.002** (multiplication des programmes d'exploitation et campagne de spam). Microsoft a réagi en publiant un avis de sécurité proposant des solutions de contournement (hors cadre officiel de ses publications), qui a fait l'objet de l'avis **CERT-IST/AV-2006.119**.
De même, et comme cela se produira à plusieurs reprises en 2006 lorsque Microsoft met trop longtemps au gré des experts (plus d'une semaine …) à proposer un correctif, la société eEye publiera un patch non-officiel, que le Cert-IST testera sans toutefois en recommander le déploiement.

Juin 2006 :
Microsoft a publié ce mois -ci 12 bulletins de sécurité. Dans les jours suivants, se sont ajoutées 3 failles "Excel" (ou Office en général) et 2 failles "Internet Explorer" .

Ces exploitations en 0-day étant heureusement assez rapidement détectées, elles sont aussi vite abandonnées par les hackers, et l'on ne dépassera pas le niveau du Danger Potentiel.
Le scénario commun à ces événements, (qui la plupart du temps visent à installer des chevaux de Troie sur le poste des victimes dans un but d'espionnage industriel), reste invariant :
les attaquants utilisent des failles encore inconnues pour réaliser des virus nouveaux qu'ils envoient à un nombre limité de victimes (pour éviter que ces nouveaux virus ne soient repérés par les éditeurs anti-virus). Une fois le virus capturé, les attaquants abandonnent la faille utilisée par le virus (puisque cette faille est maintenant connue) et construisent un autre virus utilisant une nouvelle faille inconnue.

Ce type d'attaques va dans la deuxième moitié de l'année se multiplier et s'intensifier.

Aout 2006 :
A noter pour l'anecdote une vulnérabilité Microsoft introduite dans un correctif de sécurité (**MS06-042**) et touchant le navigateur web **Internet Explorer** (CERT-IST/AV-2006.342).

Mais la principale attaque du mois d'août aura été celle liée à la publication de la vulnérabilité du **service "Serveur"** des systèmes Microsoft Windows (CERT-IST/AV-2006.315 - **MS06-040**). Dès l'apparition des premiers codes d'exploitation (3 jours après la diffusion de l'avis de sécurité de Microsoft), le Cert-IST a émis un "**DanGer potentiel**" CERT-IST/DG-2006.006) pour avertir sa communauté des risques liés à ce problème.
Comme on pouvait s'y attendre, au cours du long week-end du 15 août, et plus précisément le dimanche 13, les premiers éléments d'attaque sur Internet ont été signalés. A travers son service de veille 7/7, le Cert-IST a émis une **Alerte** vers les abonnés de ce service. Cette alerte a été ensuite transmise à l'ensemble des adhérents le 16 août au matin (**CERT-IST/AL-2006.004**).
L'activité autour de cette vulnérabilité a ensuite évoluée tout au long du mois. Des variantes de vers connus comme "Gaobot" (CERT-IST/AV-2004.094) ont intégré ce nouveau vecteur d'attaque.
Vous pouvez retrouver toutes ces informations dans le "**Hub De gestion de Crise**" (HDC) "MS06-040 Netapi".

Septembre 2006 :
Le mois de septembre a également été caractérisé par de nombreuses exploitations de vulnérabilités Microsoft.
Tout d'abord, il y a eu l'apparition d'un cheval de Troie exploitant une vulnérabilité de type "0-Day" dans le traitement de texte **Word 2000** (CVE-2006-4534). Un "Hub De gestion de Crise" et un avis de sécurité (CERT-IST/AV-2006.364) ont alors été créés à cet effet. Il est à noter que pendant plusieurs jours **aucun correctif officiel de Microsoft n'a été publié**.
Ensuite, une nouvelle faille de type "0-Day" a été découverte dans la partie logicielle des environnements Microsoft chargée d'interpréter les images vectorielles (**VML**) (CVE-2006-4868). L'exploitation de cette vulnérabilité a été rapidement constatée sur Internet (**CERT-IST/DG-2006.008** - **CERT-IST/AL-2006.005**). Un "Hub De gestion de Crise" (https://wws.cert-ist.com/fra/hub/mswindowsvml/) a alors été créé pour suivre l'évolution de ce problème. Microsoft a fourni un correctif hors-planning pour cette vulnérabilité (**CERT-IST/AV-2006.391**).
Pour finir, une nouvelle vulnérabilité de type "0-Day" a été découverte dans le logiciel **PowerPoint** (CVE-2006-4694) et a été rapidement exploitée par des chevaux de Troie. Le "Hub De gestion de Crise" concernant "PowerPoint" (https://wws.cert-ist.com/fra/hub/powerpoint07_06/) permet de suivre l'évolution de cette vulnérabilité. De nouveau, pendant plusieurs jours aucun correctif officiel n'a été publié.

Octobre 2006 :
L'événement majeur d'Octobre fut l'alerte **CERT-IST/AL-2006.006**, ("**Exploitation de la faille 'WebViewFolderIcon' dans Microsoft Windows**"), émise le 02/10/2006, après confirmation d'une utilisation active de cette faille sur Internet.
La vulnérabilité "WebViewFolderIcon" (CVE-2006-3730, avis **CERT-IST/AV-2006.396**) :

- avait été révélée en juillet dans le cadre du "MoBB" ("Month of the Browser Bug"),
- avait donné lieu fin septembre à un premier programme d'exploitation (cf. notre information du 28/09/2006 dans la liste "[Vuln-coord]"),
- a finalement été corrigée par Microsoft le 10/10/2006 dans son bulletin mensuel "MS06-057".

Ce type de calendrier, s'il en était encore besoin, démontre largement l'intérêt du Hub de Gestion de Crises et de son blog pour suivre l'historique et l'évolution d'une menace.

Novembre 2006 :
« La faille Microsoft du mois » était en novembre la MS06-070 :
Dès la publication le 14/11/2006 des bulletins de sécurité de Microsoft pour le mois de novembre, la faille "MS06-070" (cf. l'avis **CERT-IST/AV-2006.478** : "Vulnérabilité du service Workstation sur Microsoft Windows") est apparue comme très dangereuse. Elle permet en effet la prise de contrôle à distance des plates-formes Windows vulnérables, et elle est "wormable" (i.e. qu'un ver peut être développé grâce à cette faille) sur les systèmes Windows 2000. La note CVSS de 10 (note de dangerosité maximale avec le modèle CVSS) a d'ailleurs été attribuée par NVD à cette faille (c'est la première fois qu'une note aussi élevée est attribuée à une faille). Le 16/11/2006 le Cert-IST a émis le **DanGer potentiel CERT-IST/DG-2006.009** pour cette faille, suite à la publication d'un premier programme d'exploitation. Cette montée de la menace a par ailleurs été confirmée par Microsoft qui a émis le lendemain un "Security Advisory" sur le sujet. Il n'y a pas eu par la suite d'attaques d'une ampleur significative au moyen de cette faille (et en particulier, pas de ver).

Les environnements multimédia et Wireless : la prochaine cible ?

Si la vulnérabilité liée aux nouvelles technologies est un sujet de conférence souvent alléchant, cette année elles ont plus fait l'objet de recherches et de publications que d'exploitations réellement dangereuses.

Ces différents thèmes ont été l'objet de nombreux articles-bulletins.

Février 2006 :
La problématique de l'outil "**Google Desktop Search**".

Mars 2006 :
Le bulletin de mars est l'occasion de suivre l'évolution du domaine, avec les articles "**Virus RFID**" et "**Nouveaux vecteurs de codes malveillants**" (smartphones).

Aout 2006 :
Les spécialistes, en particulier lors des conférences "**Black Hat**" et "**DefCon**" ont investigué des aspects plus originaux que les "classiques" vulnérabilités/avis Microsoft. Les présentations qui ont retenu notre attention étaient toutes liées à des aspects multimédia ou Wireless :

- La première concerne le **contournement des gardes-barrières Cisco** à travers de flux SIP (signalisation de la voix sur IP).

- La seconde décrit, quant à elle, l'attaque de PC via une **vulnérabilité dans les pilotes ("drivers") Wifi**.
- Enfin la troisième montre qu'un **terminal BlackBerry compromis** peut servir à un pirate pour rentrer dans le SI de l'entreprise.

Au-delà de l'effet médiatique déclenché par ces présentations, l'analyse à froid, en particulier au travers de deux articles "Vulnérabilité des pilotes WIFI" et "Attaque "BBproxy" contre les terminaux BlackBerry" du bulletin d'Aout, a montré leurs limites.

Conclusion

Au travers de ce bilan sur l'année 2006, on voit que **la menace pour les entreprises a changé**. Les années 2001 à 2005 ont 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 parait désormais révolu. **Aujourd'hui il n'y a plus d'attaque massive et bruyante**.

Au premier abord la vie des RSSI est donc plus tranquille, mais ces apparences sont 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 le risque d'une fraude financière ou d'une compromission de données est bien plus important qu'il y a cinq ans. Certe, dans le même temps le niveau de défense des entreprises s'est accru, mais aujourd'hui s'il reste le moindre point faible dans la cuirasse, il y a fort à parier qu'il y aura quelqu'un capable de l'identifier et de l'exploiter.
Pour nous la menace est donc devenue plus pernicieuse : beaucoup plus discrète, et beaucoup plus puissante.

Pour faire face à cette nouvelle menace il est nécessaire de continuer à développer au sein des organisations deux axes de défense :

- **Le traitement systématique des correctifs de sécurité**. La chaine qui va de la veille sur les failles jusqu'à la mise à jour de l'ensemble du parc lorsqu'un correctif (ou un palliatif) est disponible doit être la plus robuste et la plus systématique possible. Dans ce domaine, et comme nous l'avons évoqué lors de notre Forum 2006, la mise en place d'outils de "workflow" nous semble la solution la plus appropriée.
- **La protection des informations critiques de l'entreprise**. La professionnalisation des attaques (le renforcement des motivations mercantiles) veut dire pour l'entreprise un renforcement du risque de type "espionnage industriel". En effet, si des faiblesses existent dans le système d'information d'une entreprise, alors ces faiblesses seront maintenant utilisées pour voler (discrètement) de l'information à l'entreprise. Pour minimiser ce risque, outre le traitement systématique des failles, il faut donc aussi travailler à renforcer la protection des informations sensibles.

Bien sûr, la capacité de réaction en temps réel face à une crise (capacité qui a été imposée aux entreprises à l'occasion des "grandes" attaques des années 2001 à 2005) doit en parallèle continuer à être cultivée, ne serait-que pour être capable de traiter une attaque ciblée ...