Bilan Cert-IST 2008 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 2008 de façon à mettre en évidence les tendances sur l'évolution des attaques et des menaces. Ce bilan présente une synthèse des informations fournies aux adhérents du Cert-IST au fil des mois via les bulletins du Cert-IST, que nous revisitons à cette occasion.

Quelques chiffres

En 2008 le Cert-IST a publié 563 nouveaux avis de sécurité et a suivi leur évolution au travers de 1330 mises à jour (dont 82 mises à jour majeures). La production brute d'avis est donc légèrement en retrait par rapport à l'année 2007 (595 avis) tout en étant supérieure aux années précédentes (546 avis en 2006, 485 en 2005, etc.).

Sur ces 563 vulnérabilités, 13 ont évolué vers des situations à fort risque et ont fait l'objet d'un suivi spécifique au travers du "Hub de gestion de Crise" du Cert-IST. Au final, le Cert-IST a émis 2 alertes pour des situations de risque maximum nécessitant un traitement immédiat au sein de notre communauté :

- L'alerte **CERT-IST/AL-2008.001** en juillet pour la vulnérabilité DNS
- L'alerte **CERT-IST/AL-2008.002** en novembre pour le ver Conficker (Downadup)

Globalement, le Cert-IST suivi actuellement les vulnérabilités concernant 739 produits et 6194 versions de produits (chiffres à ajuster).

Les principaux faits marquants

Rappelons tout d'abord les tendances les plus marquantes de cette année 2008 :

- **Attaques du poste de travail par des sites web compromis**. Le début de l'année a clairement montré une recrudescence des attaques visant l'internaute. Plus que le navigateur web ou le système d'exploitation, ce sont avant tout des vulnérabilités découvertes dans des logiciels tiers (QuickTime, Acrobat Reader, Real Media, Flash) qui sont utilisés pour compromettre le poste de l'utilisateur lors de sa navigation sur Internet. De plus l'internaute se fait le plus souvent attaquer lorsqu'il visite des sites web anodins qui ont été eux-mêmes compromis et qui propagent sans le savoir ces attaques.
- **Compromissions massives et organisées**. Le deuxième événement fort de cette année 2008 sur le front des attaques est l'utilisation systématique de vulnérabilités de façon massive et organisée : l'attaquant utilise ici la même vulnérabilité dans un déploiement rapide et sur une grande échelle, ce qui provoque des vagues d'attaques. Ainsi, au cours des 2 premiers trimestres des vagues d'attaques par "Injection SQL " ont permis à des attaquants de déposer des codes malicieux silencieusement en quelques heures sur des milliers de sites web, permettant ensuite d'infecter les ordinateurs de victimes visitant ces sites.
- **La faille DNS : un cas historique**. Il s'agit d'une faille hors norme par sa gravité (elle permet à un pirate de détourner vers lui tout le trafic réseau destiné à un serveur donné), par son ampleur (la grande majorité des installations DNS étaient vulnérables) et par son mode de divulgation (la vulnérabilité a été gardée secrète plusieurs mois puis divulguée partiellement pour laisser le temps aux organismes de déployer les correctifs, ce qui a généré un emballement médiatique). Il s'agit sans aucun doute de LA faille de l'année 2008.
- **Conficker (Downadup) : le retour du ver**. La fin de l'année 2008 (et le début de 2009) a été marqué par le ver Conficker aussi connu sous le nom de "Downadup". Ce ver utilise une

vulnérabilité découverte fin octobre dans le service "serveur" de Windows et a connu une propagation large et rapide, ce qui peut rappeler les crises virales vues en 2004 (Sasser).

En plus de ces événements incontournables qui ont constitué l'actualité des attaques 2008, plusieurs autres faits ont ponctué cette même année :

- Des failles préoccupantes, mais à l'impact encore limité. La faiblesse des **clés OpenSSL des systèmes Debian et de leurs dérivés**, la vulnérabilité **TCP DOS** ou encore les **collisions MD5** dans les certificats X509 sont trois exemples de failles préoccupantes révélées en 2008. Elles touchent toutes des éléments fondamentaux pour la sécurité sur Internet. Lorsqu'une vulnérabilité de ce type est découverte les conséquences potentielles sont graves. Il est intéressant de noter ici que 2008 a été particulièrement riche en termes de publications, et sur des sujets très divers (voir aussi les articles publiés en 2008 par le Cert-IST sur des sujets comme "Cold boot attack", ou "Ghost in the Browser").
- Les cybercriminels sont de plus en plus actifs (voir par exemple notre article " Le marché lucratif des faux antivirus") mais la réaction des autorités devient aussi plus déterminée (voir par exemple notre article " La lutte contre les ISP complaisants s'intensifie").

2) L'actualité des attaques et des vulnérabilités au fil des mois

Ce chapitre présente les attaques et les vulnérabilités les plus marquantes qui se sont produites mois par mois en 2008.

2.1) Attaques du poste de travail via des sites web compromis – Janvier/Février/Mars 2008

L'**attaque des postes de travail des internautes au travers de leur navigateur web** a été une des préoccupations majeures de 2008. En effet, s'il n'est pas nouveau qu'un utilisateur puisse être infecté lorsqu'il visite un site web malicieux, il est par contre préoccupant de voir le nombre de sites apparemment inoffensifs qui propagent désormais à leur insu ces attaques, la sophistication de ces attaques, et la vitesse avec laquelle les nouvelles vulnérabilités sont intégrées aux panoplies de l'attaquant.

Ces attaques utilisent le plus souvent des sites web qui ont été compromis. La nature de la menace a donc évolué. Certaines attaques de serveurs web sont désormais réalisées, non pas pour ce que ces serveurs sont ou ce qu'ils contiennent, mais pour en faire des vecteurs de rebond pour atteindre les postes de travail. Le danger n'est plus que l'internaute aille sur des sites inconnus :

- Un site de confiance peut être « infectant » s'il a lui-même été infecté (extension du périmètre « à risque »).
- Les sites dont nous avons la responsabilité peuvent être eux même « infectants » (implication de notre responsabilité dans des attaques visant des tiers).

Ces attaques du poste de travail visent désormais de plus en plus les logiciels tiers qui équipent le poste de l'internaute (typiquement les logiciels d'extension ou les plugins complémentaires couramment installés comme : QuickTime, Acrobat Reader ou Real Media) plutôt que le système d'exploitation lui-même, voire le navigateur web. Cette évolution constitue aussi un nouveau défi pour le maintien à jour du parc informatique car si les mécanismes de mise à jour du système d'exploitation ont fait des progrès significatifs ces dernières années, la mise à jour des logiciels tiers reste aujourd'hui souvent difficile.

Comme nous l'expliquions de façon détaillée en janvier dans **le Hub de Crise ouvert sur ce sujet**, il y a aujourd'hui plus que jamais un grand risque à naviguer sur le web en utilisant un ordinateur qui n'est pas totalement à jour en termes de correctifs de sécurité.

Au cours du premier trimestre le Cert-IST a émis 5 "Dangers Potentiels" (DG), messages de pré-alertes qui avertissent nos membres d'attaques qui pourraient les toucher prochainement. Ces DG traduisent bien le phénomène d'attaque des postes, via la navigation sur des sites réputées de confiance qui nous mentionnions ci-dessus en, synthèse :

- Les DG **CERT-IST/DG-2008.001** **CERT-IST/DG-2008.002** et **CERT-IST/DG-2008.004** informent notre communauté de vulnérabilités dans les logiciels RealPlayer, QuickTime et PDF. Il s'agit donc typiquement du phénomène d'attaque des postes de travail via les outils tiers.
- Les DG **CERT-IST/DG-2008.003** et **CERT-IST/DG-2008.005** alertent sur le phénomène parallèle au premier : l'infection massive de sites web. Sur chacun des sites infectés le pirate dépose un code d'attaque qui utilise les nouvelles vulnérabilités visant les postes de travail. En infectant de multiples sites le pirate augmente la probabilité qu'un utilisateur visite un site piégé et se fasse infecter.

Revue de détail des attaques

Note : Le texte ci-dessous a été mis en italique pour indiquer qu'en lecture rapide le lecteur pourra sauter cette section.

Les attaques du mois de Janvier

Le Cert-IST a émis au cours du mois de janvier 3 "Dangers Potentiels" :

- ***CERT-IST/DG-2008.001*** *(07/01/2008) : Activités malveillantes autour de vulnérabilités de RealPlayer*
- ***CERT-IST/DG-2008.002*** *(11/01/2008) : Nouvelle vulnérabilité RTSP critique dans QuickTime d'Apple*
- ***CERT-IST/DG-2008.003*** *(17/01/2008) : Infections massives de sites web*

Les deux premiers concernent des vulnérabilités dans des lecteurs multimédia ("RealPlayer" pour la première et "QuickTime" pour la seconde) et sont assez semblables d'un point de vue externe, car ces vulnérabilités :

- *sont activables au travers du navigateur web.*
- *sont dues à des débordements de pile dans des applications qui n'utilisent pas le mécanisme de protection contre les débordements de pile (DEP) de Microsoft Windows (mécanisme dont bénéficie désormais la plupart des applications de Windows XP-SP2, Windows 2003-SP1 et Windows Vista).*

Pour ce type de vulnérabilités, l'évolution de la menace est classique :

- *Découverte de la vulnérabilité (ou publication d'un programme de démonstration montrant son existence et son exploitabilité),*
- *Puis apparition d'un (ou plusieurs) programmes d'attaques utilisant cette vulnérabilité.*

A ce stade, le Cert-IST émet un "Danger Potentiel" pour avertir sa communauté que des attaques sont désormais possibles. Chacune de ces menaces est suivie dans un "Hub de Crise" dédié :

- *Hub de crise sur la menace "RealPlayer 01/08"*
- *Hub de crise sur la menace "QuickTime RTSP"*

*Le troisième "Danger Potentiel" (**CERT-IST/DG-2008.003**) concerne le fait qu'en janvier deux vagues de compromissions massives de sites web ont été observées.*

Les attaques du mois de Février

*Le Cert-IST a émis le 11 février le "Danger Potentiel" **CERT-IST/DG-2008.004** (Propagation de fichiers PDF malicieux - CVE-2007-5659) parce qu'une vague d'attaques au moyen de fichiers PDF malveillants avait été identifiée sur Internet. Cet évènement a été signalé initialement le samedi 9 février aux abonnés bénéficiant du service de veille 7/7.*
Du fait de l'exemplarité de cette attaque, nous lui avons consacré un article.

Les attaques du mois de Mars

*Le Cert-IST a émis le 17 mars le "Danger Potentiel" **CERT-IST/DG-2008.005** ("Multiples attaques massives de sites web") parce que deux vagues d'attaques avaient été observées sur Internet et avaient infecté un grand nombre de sites web. Les sites infectés ont été modifiés de façon à attaquer ensuite les visiteurs.*
*Pour suivre l'évolution de cette menace, le Cert-IST a actualisé le Hub de Crise **"Infection Web"**, initialement créé le 17 janvier en même temps que le "Danger Potentiel" **CERT-IST/DG-2008.003** (Infections massives de sites web). La technique d'attaque utilisée pour la seconde vague est des plus originale (car nouvelle), puisqu'elle consiste à injecter des données malicieuses dans les caches des moteurs de recherche des sites web infectés.*

2.2) Des stratégies de compromission massives et organisées - Avril/Mai/Juin 2008

Les vagues d'infections massives de site web qui ont été vues dès janvier 2008 (cf. **CERT-IST/DG-2008.003**) vont se poursuivre tout au long du second trimestre. La tactique des attaquants est claire : à chaque fois qu'une nouvelle vulnérabilité est découverte il faut l'intégrer le plus vite possible à la panoplie des attaques et la déployer sur un maximum de sites web compromis. En 2008 la technique de compromission la plus populaire a été l'attaque des serveurs web par " injection SQL". Les serveurs les plus visés ont été les serveurs Microsoft IIS utilisant une base de données SQL-Server. Un article publié en juin 2008 par le Cert-IST (intitulé "Les attaques par injections SQL de ces derniers mois") s'attache à expliquer les techniques employées pour mettre en œuvre ces attaques.

Pour réaliser ces vagues de compromissions, il faut que l'attaquant soit organisé et capable de maîtriser des activités aussi diverses que :

- La recherche de vulnérabilité,
- Le développement de programmes d'attaques,
- Le déploiement massif de ces attaques,
- Le regroupement des postes infectés en botnets.

Comme déjà mentionné en 2007, on voit clairement ici l'industrialisation des procédés utilisés par la cybercriminalité.

Au-delà des infections massives de sites web par injections SQL (ce qui est une nouveauté de 2008) on retrouve également au cours de ce second trimestre, des phénomènes déjà vu les années précédentes :

- Le malware "**StormWorm**" (qui existe depuis janvier 2007, et dont nous avons retracé l'activité dans un article du bulletin de janvier 2008) continue de faire parler de lui. Sa dernière mouture se présente sous forme d'un e-mail à propos du 1er avril et invite le lecteur à se rendre sur un site web pour y voir un "poisson d'avril". Bien évidemment ce site web est piégé. Cet évènement a été signalé à notre communauté par le message **VirusCoord-2008.001** de la liste de diffusion ad-hoc. Le botnet "**Kraken**" (réincarnation 2008 de "Bobax", l'un des plus anciens botnet de spam) a fait également parler de lui au second trimestre 2008.
- En juin, nous avons signalé dans les bulletins de veille média du 09/06/2008 et du 10/06/2008, **le retour du malware "GPCode"**. Ce virus, également connu sous le nom "PGPcoder", date déjà de 2005 (cf. cet article). Sa particularité est de chiffrer les documents trouvés sur le poste qu'il infecte. Il

demande ensuite une rançon à ses victimes en échange de la clé qui permettra de déchiffrer ces fichiers. Ce type de malware est désormais communément désigné sous le terme anglais de "ransomware".

Revue de détail des attaques

Dans ce chapitre nous détaillons mois par mois les différentes attaques survenues au second trimestre 2008.

Les attaques du mois d'Avril

Le mois d'avril a été dense en ce qui concerne les attaques, avec 4 messages sur notre liste de diffusion "Vuln-Coord". Il n'y a pas eu par contre de "Danger Potentiel" ce qui signifie que les menaces rapportées ont eu surtout un retentissement médiatique et n'ont pas justifié de montée de crise. Avril a en réalité constitué une répétition condensée des évènements de janvier, février et mars 2008 : attaques web, fichiers PDF malveillants, mais a été également l'occasion de marquer une certaine progression dans les attaques automatisées des serveurs.

*C'est le 8 avril que le Cert-IST a émis le premier message VulnCoord pour informer ses membres de l'émergence d'une nouvelle menace : **Kraken**. A l'image de StormWorm, Kraken est un botnet qui se répand principalement via des campagnes de messages de spam.*
*Trois jours plus tard, nous rapportions qu'un programme presque fonctionnel exploitait une vulnérabilité dans l'API GDI de Microsoft (vulnérabilité **MS08-021**), et se répandait sur des sites Web malveillants.*
Enfin, le 25 avril, nous émettions 2 messages "Vuln-Coord" sur les menaces suivantes :

- *VulnCoord-2008.010 : une reprise et une amplification du nombre d'**attaques par injections SQL** visant des serveurs utilisant ASP et une base de donnée Microsoft SQL (300 000 sites compromis).*
- *VulnCoord-2008.011 : une augmentation du nombre de messages de Spam contenant des fichiers **PDF malveillants** exploitant une vulnérabilité (CVE-2008-0655) corrigée depuis 2 mois dans Adobe Reader.*

Les attaques du mois de Mai

Le mois de mai confirme bien la tendance constatée en avril, c'est-à-dire la recrudescence d'attaques par injection SQL. Le 9 mai, 4000 nouveaux sites ont été infectés par ces attaques, ce qui nous a poussé à mettre à jour le hub de crise "Infections web".

Le 28 mai, nous avons émis le "Danger Potentiel" **CERT-IST/DG-2008.006** "Vulnérabilité 0-day dans *Adobe Flash Player" suite à la découverte par Symantec de fichiers FLASH malveillants exploitant une vulnérabilité non divulguée (0-day) contre la dernière version d'Adobe Flash Player. Compte tenu du peu d'information initiale (faille 0-day) et de l'ampleur des sites web impactés (plusieurs milliers de sites concernés), le Cert-IST a décidé d'ouvrir un hub de crise afin de suivre l'évolution des attaques massives liées à cette "nouvelle" vulnérabilité (Vulnérabilité 0-day dans Adobe Flash Player).*

Les attaque du mois de Juin

*Dans la continuité des mois précédents, on signale de nouvelles **infections de sites web au moyen d'attaques par "Injection SQL",** d'ampleur cependant plus faible que celles rapportées lors des vagues d'attaques précédentes. On notera dans ce domaine :*

- *Les recommandations publiées par Microsoft pour éliminer ce type de vulnérabilité sur les serveurs IIS (cf. notre message "VulnCoord-2008.018" à ce sujet).*
- *L'analyse technique publiée par le SANS à propos du code SQL injecté.*

2.3) La faille DNS : un cas historique - Juillet/Août/Septembre 2008

La Faille DNS

L'événement marquant de l'été, et probablement de l'année, est la vulnérabilité découverte dans le protocole DNS (Domain Name System) par l'expert en sécurité Dan Kaminsky, qui devait la divulguer à l'occasion de la conférence Black Hat de Las Vegas. La manière dont la communication sur cette vulnérabilité a été gérée constitue une première dans le domaine d'Internet et de la sécurité informatique. Un article du bulletin de juillet vous en explique les raisons.

Conscient de la criticité de cette faille, le Cert-IST a très tôt suivi cette vulnérabilité dans l'avis de sécurité CERT-IST/AV-2008.310 puis dans le "Danger Potentiel" CERT-IST/DG-2008.007, et enfin au travers de son hub de crise "Vulnérabilité DNS".

Faille DNS : un cas historique

Cette faille constitue un cas "hors-norme" et encore controversé en matière de "divulgation responsable". Plusieurs facteurs font que cette menace revêt une importance particulière.

- Tout d'abord, les impacts et conséquences de cette faille sont graves puisque cette dernière permet à un attaquant de détourner tout le trafic des utilisateurs d'un serveur DNS vulnérable vers des sites malveillants (corruption de cache DNS).
- Ensuite, elle impacte l'immense majorité des serveurs et clients DNS connectés à Internet dans le monde, ce qui rend l'application des correctifs difficile,
- Elle touche un très grand nombre d'acteurs de l'Internet ; les équipementiers réseaux, les ISP, les régulateurs des noms de domaines (registry, registrar), les administrateurs DNS, les développeurs, sans oublier les utilisateurs.
- Enfin, cette faille intéresse les cybercriminels parce qu'elle permet de rediriger des internautes vers de faux sites web. De multiples scenarii d'attaque sont possibles, et en particulier celui du phishing.

Une gestion inhabituelle

Les détails techniques de cette vulnérabilité, découverte en février 2008, ont été maintenus secrets de longs mois. Un groupe de personnes, constitué du découvreur, de membres de l'US-CERT et des différents éditeurs de services DNS, ont travaillé ensemble afin de décider de la meilleure façon de gérer et corriger cette faille, puis de la rendre publique.
La date du 8 juillet 2008 a ainsi été retenue pour la publication concertée des correctifs, tout en souhaitant garder secrets les détails techniques. C'est justement ce point, le "secret", qui a suscité la curiosité des chercheurs en sécurité, qui se sont empressés d'investiguer et analyser le problème. Dans le même temps, la crédibilité de la découverte Dan Kaminsky était mise en doute. A trop vouloir se justifier et insister sur la gravité de la vulnérabilité au cours d'échanges informels, il a probablement diffusé involontairement des informations techniques précieuses. Le 22 juillet, les détails techniques de la faille étaient finalement connus.
Dès lors, tout est allé très vite. Des programmes d'exploitation ont été publiés le 24 juillet et les premières attaques ont été signalées le 29 juillet.

Etat de déploiement des correctifs

Nous écrivions en juillet : « A présent, la difficulté réside dans l'application universelle des correctifs ; la menace demeurera en effet présente tant qu'un seul serveur DNS restera vulnérable ». Le 8 juillet, environ 85% des serveurs étaient vulnérables (source "DoxPara Research"). Le 25 juillet, soit 13 jours après, ce chiffre était estimé à 52% par DoxPara, et à 66% par le CERT autrichien (http://www.cert.at/static/cert.at-0802-DNS-patchanalysis.pdf). Cette progression est significative, mais elle montre aussi qu'il restait encore de nombreux serveurs DNS vulnérables (plus de la moitié au moins).

En juillet, tous les détails techniques n'avaient pas été dévoilés, en l'attente du 7 août, où Dan Kaminsky a dévoilé les arcanes de la vulnérabilité, lors de la conférence BlackHat (http://www.blackhat.com).
Une chose est certaine, c'est que tout ne s'est pas passé comme "prévu" (http://www.doxpara.com/?p=1162). Reste à analyser les erreurs commises et à s'interroger sur les nombreux problèmes soulevés par la découverte puis la publication responsable pour ce type de vulnérabilité. L'un des problèmes majeurs étant la difficulté d'appliquer des correctifs sur une aussi grande échelle (problème déjà connu mais accentué dans le cadre du DNS) et aussi rapidement.

Pour plus d'information

- Hub de gestion de crise "Faille DNS" : https://wws.cert-ist.com/fra/hub/failledns
- Site officiel de Dan Kaminsky : http://www.doxpara.com/

Les autres attaques d'août à septembre 2008

Cyber attaque en Géorgie

Selon la presse, des cyber-attaques attribuées à la Russie ont touché en août les sites gouvernementaux de Géorgie. Les discussions entre les CERT via le FIRST confirment effectivement l'existence d'attaques DDOS, en particulier à partir du 14 août, sans pouvoir cependant les lier à la Russie. Marcus H. Sachs, directeur de l'ISC du SANS et expert en cyber-sécurité auprès du gouvernement américain, a publié sur l'ISC une analyse intéressante de ce phénomène.

Attaques des infrastructures SSH ?

Il est bien connu que les serveurs SSH accessibles depuis Internet font régulièrement l'objet d'attaques de type "force brute" (attaques des mots de passe par dictionnaire).

Le 14 mai, le Cert-IST avait émis le message "Vuln-Coord" **VulnCoord-2008.013** "Vulnérabilité des clés OpenSSL dans Linux Debian et dérivés" concernant une vulnérabilité fortement médiatisée dans le monde des distributions basées sur Debian (Debian, Ubuntu, Knoppix, etc.). Cette vulnérabilité, due à un défaut dans le générateur de pseudos-aléas, affecte directement le package "OpenSSL" et indirectement tous les produits dérivés ou basés sur des clés SSL (OpenSSH, OpenVPN, HTTPS, etc.). Un correctif permet maintenant de détecter les clés vulnérables et force leur mise à jour sur ces distributions.

L'actualité d'août peut faire penser que des attaques plus sophistiquées sont en cours contre ces infrastructures, nous vous avons signalé :

- Tout d'abord via le message **VulnCoord-2008.026**, que des pirates s'étaient introduits sur les serveurs des infrastructures de Red Hat et de Fedora.

- Et d'autre part via le message **VulnCoord-2008.027**, que l'US-CERT avait identifié des attaques visant les serveurs SSH sur Linux et dont l'objectif semble être de voler les clés SSH stockées sur ces serveurs (rootkit "Phalanx2").

Campagnes virales de type "botnet Storm" propagées via du Spam

En août, plusieurs campagnes de SPAM de grande ampleur visant à infecter le poste de l'internaute, ont été remarquées et signalées dans le message **VirusCoord-2008.002.** Elles portent le nom de "Jeux Olympiques", "Top News CNN" ou "Airline Ticket email" et ont toutes pour but d'attirer les curieux vers un site web qui infectera le PC avec un botnet de du type de "Storm" (cf. l'actualité d'avril).

2.4) Vulnérabilités préoccupantes, mais impact encore limité - Octobre/Novembre/Décembre

Hormis l'arrivée du ver Conficker, qui mérite à lui seul un chapitre (cf. § 2.5), les mois d'octobre à décembre n'ont pas vraiment apporté d'événements marquants en termes d'attaques.

Par contre, plusieurs vulnérabilités (détaillées ci-après) ont été fortement médiatisées. Bien que soulevant des problèmes sérieux, ces vulnérabilités n'ont pas (encore) eu d'impacts significatifs sur les infrastructures et n'ont par conséquent pas donné lieu à l'émission d'alertes ou de dangers potentiels Cert-IST vers nos membres.

Vulnérabilité "ClickJacking" (hub de crise "clickjacking")

La vulnérabilité dite de "ClickJacking" a été présentée fin septembre à l'occasion de la conférence OWASP (Open Web Application Security Project) à New-York. Cette attaque exploitant une vulnérabilité dans les contenus dynamiques de pages DHML (Dynamic HTML) permet d'amener un utilisateur à cliquer sur des liens dangereux à son insu. Le Cert-IST a envoyé le message Vuln-Coord-2008_030 pour prévenir sa communauté, et a suivi cette vulnérabilité dans la liste des "Failles en cours d'investigation" (cf. FA-2008_0181).

Faille DOS TCP (VulnCoord-2008.031)

Fin septembre, deux experts en sécurité finlandais ont annoncé avoir découvert une vulnérabilité impactant toutes les implémentations des piles TCP/IP, et provoquant un déni de service. Après avoir annoncé la publication de certains détails de la faille à l'occasion de la conférence T2 qui se tenait le 17 octobre 2008 dernier en Finlande, les deux protagonistes se sont rétractés considérant que ces détails ne devraient être révélés qu'une fois les correctifs constructeurs publiés. Seule une démonstration de l'exploitation de la vulnérabilité aurait été présentée lors de cette conférence, et elle provoquerait un déni de service de n'importe quel équipement implémentant une pile TCP/IP vulnérable.
Pour le moment aucune information technique n'a filtré. Les détails seront probablement connus courant 2009. Cette vulnérabilité fait l'objet d'un suivi dans la rubrique "Failles en cours d'investigation" (cf. FA-2008.0184) et dans le hub de crise "Vulnérabilité DOS dans TCP annoncée pour la conférence T2 2008".

"Token kidnapping" : Exploitation d'une vulnérabilité Windows via IIS et SQL Server (VulnCoord-2008.032)

Ce message "Vuln-Coord" a été émis suite à la publication sur Internet d'un programme d'exploitation permettant d'attaquer les systèmes Windows via les serveurs Microsoft IIS et SQL Server (attaque "Token Kidnapping").

Par contre, deux vulnérabilités nous ont semblé plus préoccupantes et ont donné lieu à émission de Dangers Potentiels afin que notre communauté puisse se préparer à de possibles attaques. A ce jour, ces attaques n'ont connu aucune ampleur significative justifiant l'émission d'alertes.

Vulnérabilité dans le démon sadmind sous Solaris (hub de crise "sadmin")

Mi-octobre une vulnérabilité a été découverte dans le produit "Sun Solstice AdminSuite" impactant les systèmes Solaris 8 et 9. En l'absence de correctif de la part de l'éditeur et compte tenu de la criticité de cette vulnérabilité (prise de contrôle totale à distance), nous avons suivi celle-ci dans la faille en cours d'investigation "**FA-2008.0194** et informé notre communauté de la publication de programmes d'exploitation dans le "Danger Potentiel" (**CERT-IST/DG-2008.008**).

Vulnérabilité 0-day XML dans Internet Explorer (hub de crise " IE XML 0day")

Cette vulnérabilité 0-day dans le traitement de certaines données XML par Internet Explorer, a été révélée le lendemain du Patch Tuesday de décembre. Elle a fait l'objet du Danger Potentiel CERT-IST/DG-2008.011 dès le 10 décembre et du hub de gestion de crise "IE XML 0day". Un avis de sécurité a également été rédigé (CERT-IST/AV-2008.538) proposant dans un premier temps des mesures palliatives. Microsoft a réagi le 17 décembre en publiant à nouveau un bulletin de sécurité hors cycle (MS08-078), fournissant des correctifs pour cette vulnérabilité.

2.5) Conficker (Downadup) : le retour du ver

Le fait le plus marquant du dernier trimestre 2008 est l'arrivée du ver Conficker (aussi appelé "Downadup"). Il s'agit du premier ver qui touche de façon aussi significative notre communauté depuis 2004 (année du ver "Sasser"). Nous retraçons ci-après le traitement que le Cert-IST a fait face à cette menace. Mais globalement nous pouvons en retenir que

- La menace a bien été anticipée. Dès le 23 octobre (date de l'annonce par Microsoft de cette vulnérabilité dans le bulletin MS08-067), il a été clairement été identifié qu'un ver pourrait apparaître. Les publications régulières du Cert-IST (un avis relatif à la vulnérabilité, trois avis relatifs aux malwares l'exploitant, deux "Dangers Potentiels", et enfin une alerte) ont permis à nos adhérents d'être tenus au courant tout au long de l'évolution de cette menace.
- Depuis 2004 aucun ver d'une ampleur significative n'avait été observé. Nous nous posions même la question de savoir s'il y aurait encore des vers (cf. notre bilan 2007) puisque ce mode de propagation massif et bruyant n'est pas forcement intéressant pour les cybercriminels qui aspirent désormais à plus de furtivité.
- Certains de nos membres ont été exposés à cette menace et un traitement rigoureux et systématique leur a permis de la contenir. Bien que les foyers d'infection de Conficker soient restés isolés et limités, il n'a pas encore été possible de déterminer systématiquement le vecteur déclencheur de ces infections. Ces vecteurs semblent potentiellement nombreux, citons en particulier les clés USB, postes nomades, canaux VPN, et les mails de spam. Pour ce type de menace, il semble inévitable que des foyers se déclenchent, malgré des mécanismes de protection tels que des antivirus, des protections périmétriques et des filtrages réseaux. Un aspect fondamental pour maîtriser la menace (en attendant que les correctifs soient appliqués sur l'ensemble des parcs)

est donc de savoir détecter au plus tôt les foyers infectieux dans l'entreprise, de les isoler puis de les traiter rapidement.

Revue de détail de la chronologie

Octobre : Bulletin de sécurité Microsoft MS08-067 "hors cycle" (VulnCoord-2008.034)

L'un des faits marquants de ce mois d'octobre est la publication d'un bulletin sécurité Microsoft (MS08-067) en dehors des dates de publications habituelles. La raison de cette publication est la découverte d'une faille majeure dans le service "Serveur" des systèmes Microsoft Windows. Plusieurs programmes d'exploitation de cette vulnérabilité sont apparus sur Internet, allant du programme de type "Proof-Of-Concept", au programme téléchargeant des malwares dérobant des informations sur un poste infecté (ex. GimmiV).
*Cette vulnérabilité a fait l'objet de l'avis de sécurité CERT-IST/AV-2008.460 et du "Danger Potentiel" **CERT-IST/DG-2008.009**. L'évolution de la menace liée à cette vulnérabilité a été suivie dans le hub de crise "Vulnérabilité critique dans le traitement des requêtes RPC sous Windows (MS08-067)".*

Novembre : Les codes malveillants se multiplient et Conficker arrive

L'évènement majeur du mois de novembre a surtout été le maintien d'une forte activité autour de la vulnérabilité MS08-067 du service "Serveur" des systèmes Windows.
Non seulement les codes malveillants se sont fortement multipliés, mais surtout une augmentation de leur efficacité s'est accrue. Ceci nous a notamment poussé à émettre, en plus des nombreux billets ayant alimenté le hub de crise "Vulnérabilité critique dans le traitement des requêtes RPC sous Windows (MS08-067)":

- *L'avis de sécurité CERT-IST/AV-2008.467 et le "Danger Potentiel" CERT-IST/DG-2008.010 relatifs aux virus "Kerbot" et "Wecorl".*
- *L'avis de sécurité CERT-IST/AV-2008.504 relatif au ver "Conficker" (aussi connu sous le nom de "Downadup").*
- *L'alerte CERT-IST/AL-2008.002 suite à de nombreux rapports d'infections par le ver "Conficker" dans le monde, mais également dans notre communauté.*

Décembre 2008 et janvier 2009 : Les infections Conficker se sont multipliées

*En décembre puis en janvier 2009 les cas d'infections Conficker se sont multipliés. La presse spécialisée a d'ailleurs largement diffusé cette information mi-janvier 2009 comme nous en faisions état dans nos bulletins de veille média (cf. **vmedia-2009.01.14**, **vmedia-2009.01.15**, **vmedia-2009.01.19**, **vmedia-2009.01.20**). Notre communauté a bien sûr également été touchée, mais les infections sont restées localisées, et donc plus facilement maîtrisables. Afin de permettre un échange accru entre ses adhérents sur cette menace, le Cert-IST a mis en place une liste de discussion dédiée à ce sujet (liste ms08-067).*

3) Conclusion

On le voit au travers de ce bilan, l'année 2008 a été riche en événements.
Tout comme en 2007 la professionnalisation des attaques est flagrante : le niveau de technicité des codes malveillants, la multiplicité des aspects maitrisés et la coordination globale au niveau des attaques ne peut en effet qu'être le résultat d'une activité très structurée.

Mais si l'on veut résumer cette année en termes de tendances, on peut qualifier l'année 2008 comme une année de "durcissement" :

- Les attaquants semblent de plus en plus forts. Les techniques d'attaques, la vitesse des cycles de vies et l'action coordonnées ont sans aucun doute progressé en 2008.
- D'un autre côté la défense a aussi progressé. En termes de technique d'abord. Par exemple un outil comme le MSRT de Microsoft (Malicious Software Removal Tool) est devenu un véritable "killer de botnet". La défense a progressé aussi en termes d'organisation; des initiatives comme ShadowServer (qui travaille à répertorier et démanteler les botnets) ou des actions comme l'arrêt brutal d'activités illicites (voir notre article "La lutte contre les ISP complaisants s'intensifie" à propos des l'hébergeurs McColo et Atrivo publié dans le bulletin mensuel du Cert-IST) sont révélatrices d'une progression et d'un durcissement de la défense.

Pour les entreprises ce durcissement des attaques implique que les défenses en place soient solides et étanches. Il faut aujourd'hui avoir des mécanisme efficaces et réactifs pour l'applications des correctifs, des mécanismes de défense en profondeurs, et des procédures rigoureuses pour faire face efficacement aux situations de crise.