Bilan 2008 du CERT-IST sur les failles et attaques
Philippe BOURGEOIS, CERT-IST

M. Bourgeois a présenté le bilan de l'année écoulée concernant les failles et attaques. Pour le CERT-IST, 2008 a vu quatre phénomènes majeurs :

1. La compromission massive de postes de travail via des sites web eux-mêmes infectés.
   Il y a une grande probabilité d'infection si l'on navigue avec un ordinateur qui ne serait pas à jour – y compris lorsque la navigation se restreint à des « grands » sites, sans fréquenter le côté obscur ou simplement gris de l'Internet.
   Ces sites relais font, pour la plupart, du transport involontaire des infections, suite à leur compromission silencieuse. Le site renverra de façon cachée (via des <IFRAME> ou <SCRIPT>) vers des sites « sous-contrôle », lesquels lanceront de nombreuses attaques vers le poste de travail. Ces attaques sont le plus souvent dirigées vers des outils tiers (greffons PDF, Flash, Quicktime, etc.) plutôt que vers le système d'exploitation ou le navigateur.
2. Des compromissions massives et très organisées.
   Le CERT-IST a observé une augmentation de la sophistication des attaques, ainsi qu'une organisation très efficace des attaquants (chercheurs de vulnérabilités, développeurs de programmes d'attaque, outils de déploiement massif et très rapide, syndication des victimes en botnets, etc.). Conficker est l'exemple le plus visible de cette sophistication.
   La capacité des attaquants à infecter des systèmes parfois très en amont des victimes (par exemple une régie publicitaire, via les agences produisant les animations Flash, afin d'attaquer in fine les internautes) montre aussi leur capacité d'organisation et d'anticipation.
3. « La » faille DNS.
   Il s'agit, pour le CERT IST, d'une faille hors normes du fait de l'impact potentiel de la vulnérabilité et de l'organisation qui a été nécessaire pour préparer puis diffuser les correctifs. Cette faille a mis en lumière toutes les interrogations quant à la gestion, au niveau mondial, d'une prochaine situation du même type.
   En outre, la controverse qui ne manquera pas d'arriver, relative à la diffusion de l'information (garder le secret ou non, organiser la définition des correctifs, etc.) constitue un écueil majeur dans la gestion de telles situations.
4. Conficker.
   Il s'agit du premier « grand » ver depuis Sasser (2004). Il repose sur la vulnérabilité traitée par le correctif MS08-67, et utilise (dans ses différentes versions) de multiples vecteurs de propagation. Il est intéressant de noter que, dès sa version B, Conficker a intégré l'algorithme de hachage MD6, qui n'est pourtant qu'au stade de candidat pour le remplacement de SHA-2. Preuve de la réactivité des attaquants, un correctif a été intégré très rapidement après que les auteurs de MD6 ont signalé une faiblesse de leur algorithme.
   Par ses modes de propagation très variés, Conficker pose la problématique des « micro-infections » au sein d'une communauté bien protégée, et donc amène la réflexion sur le terrain de la détection, quarantaine et décontamination d'infections ponctuelles.

M. Bourgeois a évoqué d'autres événements significatifs de l'année 2008 (par exemple : OpenSSL Debian, les collisions MD5 et les certificats numériques, le « TCP DOS » qui pourrait – ou pas – être un problème de même ampleur que la faille DNS...).

Si 2008 a vu une augmentation de la « puissance » des attaques, la collectivité et les autorités n'en ont pas été de reste. Il suffit de citer McColo et Atrivo, ainsi que la désaccréditation de Registrars un peu trop myopes quant à leurs clients, pour s'en convaincre. Il existe donc une tendance forte à l'organisation et à la structuration des défenses, à un niveau trans-entreprises, voire trans-national.

La mise en place de défenses solides et aussi étanches que possibles est une nécessité, mais qui ne peut s'affranchir de procédures particulièrement rigoureuses (gestion des correctifs et des menaces, réactions en cas de crise, etc.)

Le DNS comme outil de défense
Fabrice PRIGENT, Université de Toulouse 1

M. Fabrice Prigent a présenté un outil qu'il a développé afin de se servir des requêtes envoyées aux solveurs DNS de l'Université de Toulouse 1 comme symptômes d'infections virales. Cet outil était initialement destiné à détecter les postes infectés par Conficker, mais a aussi servi à relever des infections plus mineures.

M. Prigent a débuté sa présentation par un bref rappel des « différentes » utilisations du DNS aujourd'hui. Cet outil est en effet très robuste, omniprésent dès lors que l'on se connecte à un réseau (ou presque), et peut donc servir au-delà de sa fonction primaire de résolution de noms. SPF, DK/DKIM, les RBL (généralistes ou sur des outils spécialisés) sont déjà des outils se servant du DNS pour remplir leurs missions. Cependant, de l'avis de M. Prigent, il est possible de faire mieux, ou plus, ou au moins différent.

Avant Conficker, l'utilisation du DNS pour la lutte contre les infections se ramenait à l'identification de domaines « infectieux », la résolution desquels était modifiée par un solveur DNS afin de renvoyer le poste infecté vers un système sous contrôle disposant d'outils de décontamination, ou au minimum d'empêcher la connexion vers le domaine aggressif. Il est à noter que les virus sont déjà utilisateurs de ce principe, lorsqu'ils modifient le fichier HOSTS local afin de renvoyer 127.0.0.1 (usuellement) comme adresse des serveurs de mise à jour des bases de signatures d'un certain nombre d'outils anti-viraux.

Avec Conficker A et B, une défense simple

- par blocage, au niveau d'un solveur DNS, des domaines infectieux,
- par pré-réservation des domaines utilisables par le virus,
- couplée à un blocage de certaines URL « significatives » (points de rendez-vous des systèmes infectés) par les relais de navigation

se révélaient suffisantes.

L'apparition de Conficker C, qui utilise notamment des routines de détection de réponses « pathologiques » venant de solveurs DNS, rend une défense statique très difficile si ce n'est impossible. Les relais de navigation ne peuvent plus non plus bloquer les requêtes HTTP vers les points de rendez-vous, qui n'ont plus de caractère spécifique (http://adresse-ip). Il faut donc passer à un mode de défense différent, ce sur quoi M. Prigent a travaillé.

L'idée est de journaliser les requêtes envoyées à un solveur (ou ensemble de solveurs) DNS, et de traiter en temps réel ces requêtes. Le couple [domaine demandé, IP client] est stocké dans une base de données. Après une période d'apprentissage, la détection se fait lorsqu'arrive une demande de résolution d'un domaine qui n'a encore jamais été vu ou, plus exactement, lorsque le nombre de domaines « nouveaux » demandés par un même client dépasse un certain seuil.

Pour minimiser les faux positifs, il a fallu progressivement

- adapter le mécanisme de pondération a été adapté (ignorer les serveurs, détection au-delà de 100 domaines « nouveaux » demandés par un même client, note augmentée si le domaine n'a pas de serveur de noms, etc.), et
- incorporer diverses listes noires (domaines Conficker – 1.5 million de noms, domaines associés à des malwares, etc.).

Ces outils ont permis, outre la détection de postes infectés par Conficker, de relever (de façon plus anecdotique) des postes victimes d'autres outils agressifs.

En conclusion, M. Prigent signale l'évidence : il faut empêcher toute résolution de noms qui ne se ferait pas sur les solveurs de l'entité à protéger. Cela signifie un filtrage/blocage des requêtes DNS sortantes – un point qui devrait être déjà en place partout...