Compte-rendu de réunion

Référence RéSIST/2012-03

27 mars 2012

Table des matières

1 Revue d'actualité

La réunion a commencé par une revue de l'actualité récente, compilée par M. Etienne Maynier (MDal, www.mdal.fr).
Support de la revue : www.ossir.org/resist/supports/cr/2012/2012-03-27/Revue_Actualite_Mars_2012_v1.0.pdf.

2 Méthodes de contournement de détection

La première présentation, faite par MM. Léonard Dahan et Laurent Boutet de la société Stonesoft (www.stonesoft.com), a abordé les méthodes de contournement de la détection d'attaques.
Support de la présentation : www.ossir.org/resist/supports/cr/2012/2012-03-27/Stonesoft_-_AET_OSSIR_Toulouse_2012.pdf

Ces techniques et méthodes, dont le principe est connu depuis longtemps, ont pour objectif de contourner la détection que peut faire un système de sécurité. Il s'agit d'une occultation d'attaques, mais ce ne sont pas des attaques en elles-mêmes. Les premières publications sur ces techniques remontent à 1997. Phrack a abordé le thème au tournant des années 2000. Les premières suggestions de solutions (normalisation des flux) datent de 2004.

Aujourd'hui, environ 250 techniques de contournement ont été identifiées. Chaque méthode pouvant être cumulée aux autres, comme des couches différentes d'un mille-feuilles, le nombre total de combinaisons est très élevé. Parmi les méthodes connues, on trouvera la fragmentation des paquets IP,

la segmentation TCP et les différents « jeux » que l'on peut faire avec (recouvrement de segments notamment), la fragmentation SMB, etc. Des techniques plus exotiques ont été identifiées : avec MSRPC et la notation Big Endian/Little Endian par exemple, sur les options IP, etc.

Les méthodes de normalisation, qui visent à limiter ces contournements, doivent reconstruire le flux tel qu'il sera reçu et traité par la cible. Outre que cette reconstruction dépend de la cible, cela signifie de garder en mémoire une quantité significative d'informations, sans pour autant introduire de latence insupportable.

La question se pose quant au blocage de ces techniques de contournement. Il peut être considéré comme exagéré de toutes les bloquer : certaines (voire toutes) peuvent correspondre à une réalité technique. Seule leur utilisation pour contourner des systèmes de détection est malveillante.

3 Bilan 2011 de la cybercriminalité

La seconde présentation a été faite par M. Philippe Bourgeois, du CERT-Ist (www.cert-ist.com). Cette intervention a dressé un bilan de l'année 2011 en matière d'incidents de sécurité et de cybercriminalité.

Support de la présentation : www.ossir.org/resist/supports/cr/2012/2012-03-27/CERT-IST_Bilan2011-resist-v01.pdf

La première partie de la présentation est un état des lieux sur le long terme. La conclusion en est que les menaces deviennent plus diffuses et plus spécialisées qu'auparavant. Dans les années 2000 et avant, il s'agissait surtout d'attaques massives de réseaux. Puis vinrent les attaques des postes des particuliers, et maintenant les attaques ciblant les entreprises et leurs données.

Dans les bilans des années précédentes, les attaques vers les postes de travail et les applications hors système d'exploitation étaient mises en avant. Des défenses contre ces attaques existent. Elles n'ont qu'une efficacité limitée, d'autant plus que les outils malveillants sont de plus en plus furtifs et savent encapsuler leurs échanges dans des flux valides. Les agresseurs sont clairement de plus en plus professionnels et organisés, tout comme les défenseurs.

Enfin, l'apparition de l'ultra-mobilité (*Bring Your Own Device*, notion de *Anywhere, Anytime, Anyway*) ne va pas dans le sens d'une meilleure maîtrise du système d'informations.

La seconde partie de la présentation s'est attachée à cinq axes marquants de 2011, du point de vue du CERT-Ist :

APT Les *Advanced Persistent Threats*, qui sont des attaques par infiltration et compromission des cibles, ont beaucoup fait parler d'elles en 2011. Ce type de menace n'est pas nouveau. Il semble toutefois qu'il y a eu un changement d'échelle et/ou de sensibilité des cibles. Pour le

CERT-Ist, la question n'est plus de savoir si l'on sera victime d'une telle infiltration, mais plutôt de déterminer quand, et comment la détecter au plus tôt. La réponse aux APT se situe probablement à la jonction d'une meilleure mise à jour des systèmes d'informations, de l'augmentation des capacités de détection, et de l'augmentation de la sécurité interne des SI.

Grandes infrastructures fragiles Plusieurs incidents à haut profil ont concerné de très grosses infrastructures (par leur taille ou leur importance/responsabilité vis-à-vis d'Internet), qui pourtant ont été compromises assez facilement : RSA, Diginotar, Sourceforge, kernel.org et autres. Ces attaques ont pu réussir du fait de facteurs humains, d'architectures trop fragiles, ou d'attaquants plus audacieux qu'auparavant.

SCADA Les réseaux SCADA (*Supervisory, Control And Data Acquisition*) sont des cibles réelles aujourd'hui. Stuxnet (en 2010) n'a été qu'un révélateur. Le nombre d'études et de projets de recherche lancés, ainsi que celui des vulnérabilités découvertes, n'a cessé d'augmenter.

Cyber-hacktivisme Difficile de parler de 2011 et d'ignorer Lulzsec et les Anonymous. Tout mouvement revendicatif peut, aujourd'hui, se servir des mêmes techniques. Il s'agit d'un outil de plus dans leur arsenal. Mais faut-il en avoir peur ? La réponse n'est pas tranchée. L'essentiel des cibles de 2011 étaient « faciles », avec des attaques peu sophistiquées. Il reste important de prévoir un plan de communication, au cas où une entité devienne la cible d'une telle opération.

Téléphones évolués Le nombre d'applications Android malveillantes a fortement augmenté. L'objectif actuel des ces applications reste une monétarisation rapide, par des appels ou des envois de SMS vers des numéros surtaxés. Les ordiphones étant difficiles à protéger et contenant de façon presque naturelle des données sensibles ou privées (voire les deux), ce vont être des cibles de plus en plus exploitées. L'effacement à distance des données devient alors une fonctionnalité très désirable.