Quid du niveau de fraude en ligne en février 2008 ?

Bilan du mois de février. Les sites et réseaux de '*phishing*' (ou «hameçonnage») ont dernièrement fait l'objet d'innovations, adaptations ou développements – certes mineurs, mais néanmoins nombreux.Le but de ces changements étant bien entendu d'échapper aux outils de détection et fournir une résistance supérieure aux tentatives d'analyse et de fermeture des sites malveillants.

Les réseaux de type « Botnet » et « Fast-Flux »

Dans son rapport du mois de décembre, RSA rapportait un surcroît d'activité lié à des attaques de '*phishing*' similaires à celles perpétrées par le groupe « Rock Phish » – basées sur des robots de type « Botnet « .

Le spécialiste de la sécurité estimait alors que cette tendance se poursuivrait en 2008. Une prévision qui a été vérifée puisque RSA a constaté une croissance du nombre de groupes ou réseaux de phishing exploitant des proxy Botnet et la technologie de masquage Fast-Flux.

Au cours des quatre derniers mois, RSA a identifié cinq nouveaux réseaux de hameçonnage exploitant des proxy piratés – dont certains étaient des réseaux Fast-Flux – ciblant des établissements financiers dans le monde entier. Les fraudeurs semblent utiliser désormais le tristement célèbre réseau « Storm Botnet » pour héberger leurs attaques, mais d'autres réseaux ont également été détectés. Nous nous attendons à la poursuite de cette tendance et à l'augmentation du nombre d'attaques de type Fast-Flux au cours de l'année 2008.

Des kits de phishing masqués/codés

Si les kits de phishing dissimulés (où les scripts PHP sont codés) ne sont pas une véritable nouveauté, RSA signale une recrudescence de leur utilisation lors des mois de janvier et février.

Comme la plupart des kits, ils contiennent principalement des scripts PHP. Cependant, à l'examen, le code source PHP reste masqué et inaccessible. Sans décoder le code source des scripts PHP, il est difficile de les analyser…

Ce décodage reste possible, mais exige un travail conséquent de la part des experts de la sécurité afin de pouvoir identifier, les comptes d'e-mail frauduleux, mais aussi les noms des fichiers où les habilitations sont enregistrées et les sites Web avec lesquels le kit communique – ou les véritables sites bancaires pour les attaques de type « Man-in-the-Middle ».

Utilisation de « multiples versions » de la même URL

Au cours des derniers mois, RSA a relevé un nombre croissant d'attaques utilisant des variations de la même adresse URL. En d'autres termes, les fraudeurs ne joignent pas aux e-mails une copie exacte de l'URL de phishing mais une de ses multiples variantes. En pratique, ces variantes sont très similaires et ne contiennent qu'un changement mineur (un simple chiffre ou numéro de série).

L'utilisation par les fraudeurs de plusieurs URL pour la même attaque n'est pas une nouveauté

puisque cette technique est largement utilisée pour éviter les filtres anti-spam et créer des messages de phishing « personnalisés ».

La différence minime entre ces URL permet à l'attaquant de créer des messages « personnalisés » capables de contourner les filtres anti-spam tout en conduisant la victime vers la même attaque.

Progression des attaques et première place du podium pour les USA

Le nombre de marques attaquées a augmenté en février, mais reste inférieur à certains mois record de 2007 (comme mars, juin, juillet et août). En février 2008, le centre AFCC de RSA a détecté des attaques contre pratiquement **20 établissements financiers** qui n'avaient jamais été attaqués auparavant. Cette tendance est conforme aux résultats des quatre derniers mois.

Les États-Unis occupent la première place du palmarès avec une avance significative ; Hong Kong qui était à la deuxième place en janvier avec **9 % des attaques**) chute à la sixième position alors que l'Allemagne et la Corée du Sud progressent légèrement.

Les domaines Rock Phish affectent généralement les résultats de Hong Kong mais ce territoire n'en a enregistré que très peu en février. Les Philippines, qui hébergeaient un grand nombre de domaines Rock Phish en décembre, sont absentes de la liste depuis deux mois.