Phishing : des kits « prêts à l'emploi » font exploser les statistiques

La semaine dernière, l'équipe de recherche IBM X-Force a identifié pas moins de 114.013 nouveaux sites de phishing. Dans leur grande majorité, ces sites ont été découverts par un nouveau procédé d'analyse qui détecte les kits de phishing prêts à l'emploi qu'ils utilisent.

Car dans **99,8%** de ces nouveaux sites proviennent de kits de phishing disponibles en ligne.

Seulement **158** (0,2%) de ces sites ne semblaient pas suivre une stratégie de déploiement automatique pour leurs attaques de phishing.

En poussant plus loin ses recherches, l'équipe IBM X-Force a également constaté que ces sites reposants sur des kits de phishing prêts à l'emploi renvoyaient vers **111 domaines Web**, ce qui correspond à une moyenne de 1.000 sites hébergés par domaine Web malicieux.

Près d'un tiers des domaines associés aux sites basés sur des kits (33%) appartiennent à la catégorie ccTLD (country code Top Level Domains) de Hong Kong (.HK), puis à celle de Taiwan (.tw) avec 14% et enfin de la Chine (.cn) avec 8%.

Quid des kits de phishing?

Ces derniers dérivent d'un kit de développement de virus très populaire à la fin des années 90.

Ce kit, intitulé **DIY** permet à des non-techniciens de concevoir et de déployer rapidement de nombreux sites de phishing disposant chacun de nombreux domaines DNS virtuels, à partir d'un seul ordinateur (PC, portable, serveur, etc…).

Très légers et pouvant être déployés facilement au travers de robots espions, ces kits permettent de piéger les usagers de centaines de sites de banque en ligne à travers le monde en prenant le contrôle d'une seule machine.

Dans deux nouveaux billets disponibles sur son blog, Gunter Ollmann, Directeur des stratégies de sécurité pour IBM Internet Security Systems tire toutes les conséquences de ces chiffres.

– Article 1.

– Article 2.

Le blog de l'équipe de surveillance du réseau IBM ISS est accessible à cette adresse.