Le kit d'attaque Zeus libéré sur le web

Devoteam nous informe que les sources de Zeus sont désormais accessibles en ligne. Tout comme son mode d'emploi (le *User guide*). Repérées hier soir, *« je pense que, depuis, l'accès aux fichiers sources a terriblement été facilité. »*, soutient **Olivier Caleff**, directeur technique pour la SSII, prestataire CERT depuis 2010, et grand spécialiste de l'outil malveillant qu'il suit à la loupe depuis 3 ans. On peut en effet trouver une version estampillée ZeuS 2.0.8.9.7z de 6 Mo sur Megaupload, notamment.

Rappelons que Zeus est une boîte à outils constitutée de serveur et modules clients pour mettre en oeuvre des attaques informatiques avec une tendance à la spécialisation en *phishing*. *« Zeus est livré avec un listing de licences élaborées comme la possibilité de louer un réseau de botnets »*, soutient le responsable technique. Une solution d'informatique répartie qui n'a rien à envier au modèle du cloud computing. En résumé, Zeus est une boîte à outils complète pour mener à bien des attaques informatiques qui se négociait **jusqu'à 100.000 dollars** même si les tarifs semblait s'être stabilisé autour des 1500 à 2000 dollars.

Qu'est-ce qui a donc poussé son (ou ses) auteur(s) à mettre les sources de cette solution à disposition de tout le monde? Difficile à dire en l'absence du témoignage de l'intéressé. *« Il y a eu une sorte de **convergence entre Zeus et SpyEye** [un autre couteau suisse du pirate apparu en 2010, NDLR] qui a commencé à la fin de l'été 2010*, explique Olivier Caleffe. *Ce qui nous a donné l'impression que l'auteur laissait un peu tomber Zeus et le rendait moins visible au profit de SpyEye. »* Selon l'expert, les sources de Zeus, vieillissantes, pourraient alors servir de vitrine technologique à SpyEye sur le refrain : *« Regardez ce qu'on a été capable de faire avec Zeus, imaginez tout ce que vous pourrez faire avec SpyEye »*.

Une autre interprétation laisse la place à l'idée que le sources désormais publiques vont donner naissance à **une myriade de variantes** afin d'augmenter la pression sur les établissements visés, les prestataires CERT et les éditeurs d'antivirus. Pas de panique pour autant. D'abord parce que les éditeurs de sécurité profiteront des sources pour mieux étudier le comportement du kit d'attaque et intégrer sa signature à leurs bases antivirales.

Ensuite, les prestataires sont désormais informés et vont pouvoir d'autant mieux alerter leurs clients. *« Personnellement, **je pense qu'il faut sensibiliser clients et utilisateurs** en prévenant d'un risque accru de phishing »*, prévient le spécialiste sécurité même si *« chacun applique sa stratégie selon sa propre culture »*. D'autant que les responsables disposent d'un peu de temps. *« Entre deux et six mois »*, estime Olivier Caleff. Car si ajouter des plugins personnalisés à Zeus est accessible à n'importe quel développeur un peu doué en peu de temps, monter l'organisation pour réussir une campagne de phishing demande du temps. *« Il ne suffit pas d'avoir un kit, il faut avoir une organisation*, insiste l'expert de Devoteam. *C'est-à-dire des machines compromises, un réseau de personnes pour récupérer les informations de compte, pour transferer l'argent, etc. On a à faire face à une industrie pas à des étudiants dans leur cave, ce qui ne les empêche d'ailleurs pas de s'amuser avec Zeus. »*

S'il n'y a donc pas de quoi paniquer avant de voir apparaître les premières variantes de Zeus, il convient néanmoins de **redoubler de vigilance**. D'abord face à SpyEye qui a visiblement intégré les technologies de Zeus, probablement de manière améliorée. Ensuite, *« on commence à voir du Zeus, ou son équivalent, qui attaque les téléphones portables et tablettes, notamment en provenance de Chine ou d'Espagne, et crée des réseaux de smartphones zombies*, prévient Olivier Caleff. *On voit bien que le monde*

du PC est l'informatique de papa, ***le piratage de demain se tourne vers la mobilité****.* » Nous voilà prévenus.