2.500 sociétés dans le monde affectées par le botnet Kneber

Le réseau botnet baptisé Kneber vient d'être mis à jour. A en croire la société NetWitness, il aurait même réussi à infecter les postes de 2.500 sociétés. Au total, **75.000 postes auraient ainsi été compromis à travers le monde.**

Le botnet en question est **une variante de Zeus**, le réseau d'ordinateurs zombies qui avait réussi à toucher le Cloud d'Amazon. Par ce biais, des *hackers*se sont introduits en décembre dernier sans permission et ont pu installer leurs propres commandes de contrôle de l'infrastructure en ligne. Le logiciel pirate Zeus était alors au centre des attentions. Pour information, le *botnet*Zeus sert principalement à dérober des mots de passe et autres identifiants, pouvant générer plusieurs millions de dollars de revenus, notamment dans le cadre d'opération à la fraude bancaire.

Cette fois la déclinaison de ce *botnet*ressemble à un dossier caché de 75 Go utilisé, encore une fois, à des fins de **vol de mots de passe et des comptes bancaires.** Pour autant, les responsables qui ont mis le doigt sur le botnet estiment qu'il tenterait de dérober d'autres informations que celles purement bancaires. Selon le *Wall Street journal* de grandes sociétés auraient été touchées par ce *botnet*. **Juniper, Paramount tout comme Merck et Cardinal Health** figureraient au menu des victimes.

Quant au moyen de sa propagation, les experts en sécurité estiment que certains systèmes auraient été infectés par la **méthode du drive-by-download,** à défaut d'être clairement visées par le botnet. De même, Alex Cox, expert de NetWitness informe que la moitié des machines touchées par **Kneber** le sont aussi par le **ver nommé Waledac**. Un fait plutôt étrange considérant le*modus operandi* traditionnel des réseaux botnets.

Une analyse des adresses IP, des domaines et des informations d'enregistrement montre alors que les **serveurs utilisés par Kneber** se trouvent dispersés à travers le monde. Si nombre d'entre eux semblent se situer en Chine, d'autres se trouveraient en Ukraine, en Corée, au Panama et aux Etats-Unis.

Malgré les fermetures consécutives de certains serveurs accusés d'abriter ces réseaux *botnets*, Kneber est la preuve que **la toile zombie s'est retissée**. Plutôt rapidement…