Le botnet GameOver Zeus touché, mais pas coulé

C'est une première étape, mais la marche pour la fermeture du **botnet GameOver Zeus** va être longue. En fin de semaine dernière, plusieurs services de police européens et américains, y compris Europol et le FBI, ont mené **une opération coordonnée** pour mettre fin aux activités de ce botnet. Ils ont saisi des serveurs et provoqué des perturbations dans le réseau de PC zombies, mais n'ont pas réussi à le démanteler complètement.

GameOver Zeus est une souche distincte du fameux **Trojan bancaire Zeus**, même si la finalité financière est la même. Il permet le **vol d'identifiants bancaires** via du phishing et de la **fraude financière**. Selon le FBI, les pertes liées à ce réseau représente 100 millions de dollars. Le botnet a donné du fil à retordre aux chercheurs et aux autorités judiciaires, car il utilise **une architecture P2P** et dispose d'un système de commande et contrôle décentralisé. Plusieurs autres malwares et botnets mettent en œuvre cette architecture pour éviter d'être arrêtés ou contrôlés par les services de police.

Une expérience en pleine construction

La fronde menée contre GameOver Zeus a rassemblé, en plus des autorités citées précédemment, le Centre européen de lutte contre la Cybercriminalité (EC3), mais aussi plusieurs sociétés et chercheurs Shadowserver Foundation, Abuse.ch, CrowdStrike ou Microsoft. Cette démarche a tendance à se développer avec succès et permet aux différents participants d'acquérir de l'expérience dans les méthodes pour stopper et bloquer ces réseaux malveillants. En décembre dernier, la firme de Redmond, le FBI et Europol avait stoppé le botnet ZeroAccess. Mais comme pour GameOver Zeus, **le botnet n'a pas été éradiqué complètement**.

Le département de Justice américain en charge de l'affaire a expliqué qu'au cours de l'opération, les autorités ont constaté que GameOver Zeus était une des plateformes de diffusion du ramsonware, **Cryptolocker**. Ce dernier verrouille l'écran des ordinateurs et demande aux utilisateurs de payer une « rançon » pour libérer l'accès au PC. Le nombre de victimes se compte par centaine de milliers, selon l'Attorney General, **James Cole**. Aux Etats-Unis, **200 000 PC** ont été infectés en avril 2014 indique l'homme de loi. Une pratique très rémunératrice avec **27 millions de dollars** collectés par les pirates lors des 2 mois d'enquête.

Par ailleurs, le FBI a identifié **Evgeniy Mikhailovich Bogachev**, un Russe de 30 ans, comme le responsable présumé de l'opération GameOver Zeus. Il appartiendrait à un gang basée en Russie et en Ukraine. L'homme vient de rejoindre la liste des cybercriminels les plus recherchés de la planète.