Les Botnets

Un Botnet est un ensemble de machines infectées par un malware controlé par un pirate ou un groupe de pirates. Le nombre de machines faisant partie d'un Botnet peut varier entre quelques centaines et quelques millions...

Une fois la machine infectée, le malware reste inactif transformant son hôte en une "machine zombie". L'objectif du Botmaster (pirate qui contrôle le malware) est de collecter le maximum de machines zombies qui seront utilisées par la suite pour réaliser des attaques DDos (Distributed Denial of Service).

Comme tout logiciel malveillant, le malware affecte les performances de la machine victime tout en surchargeant la connexion internet et en bloquant la mise à jour du système d'exploitation. Il est important de rappeler que ces signes peuvent être différents selon le type du malware affectant la machine.

Les mécanismes de propagation

Les téléchargements "Drive-By"

Le Botmaster utilise le télécharment "Drive-By" pour télécharger le malware sur la machine de la victime et ce, via un site préalablement infecté par le pirate.

Les E-mails infectés

Les campagnes de mailing douteuses continuent à être utilisées par les pirates pour piéger le maximum de machines. En effet, l'objetif principal du Botmaster est de collecter le maximum de victimes.

Comment se protéger des Botnets ?

Gardez vos logiciels à jour !

Un malware exploite une faille de sécurité logicielle affectant l'une des composantes de votre système d'information (système d'exploitation, antivirus, etc...) et ces failles passent, généralement, inaperçues aux yeux des utilisateurs simples. Il est donc crucial de planifier et mettre en place une stratégie de mise à jour de votre architecture logicielle afin de minimiser les risques face aux botnets.

Sensibilisez vos employés !

Les malwares exploitent une faille humaine pour infecter les machines de vos employés et les botmasters exploitent leur manque de connaissances pour les piéger. En effet, il suffit d'un click pour transformer votre machine en un "Zombie", il est donc recommandé de sensibiliser et former vos employés et d'instaurer une politique de sécurité rigoureuse pour minimiser les failles dans votre système d'information.

Sauvegardez vos données sensibles !

Il est important de planifier la sauvegarde de vos données critiques périodiquement afin de reduire l'impact d'une éventuelle attaque.

tunCERT Tunisian Computer Emergency Response Team
الوكالة الوطنية للسلامة المعلوماتية Agence Nationale de la Sécurité Informatique