Botnet, des codes malveillants organiss.

A titre d'illustration, je vous propose de dcouvrir les botnets avec les travaux de David Batany. Les Botnets font partis de ce que nous pourrions appeler des architectures techniques malveillantes. En effet, un Botnet en lui mme est un code malveillant qui fonctionne dans une architecture informatique complexe avec des mcanismes de pilotage, de stockage, de rplication et d'activation spcialises. Un Botnet est peut tre considr comme un systme d'arme utilisable pour des attaques.

MITRE Attack.

Dfinition

Le terme botnet, contraction de l'anglais robot+net, se dfinit par l'ensemble des programmes, machines, serveurs connects internet ayant un ou plusieurs processus commun de communication. Plac sous le contrle d'un oprateur humain, appel botmaster, le botnet recrute des machines en exploitant les vulnrabilits, failles, infections afin d'tendre son rseau travers l'utilisation de canaux de Command and Control(C&C). Avec l'IoTInternet of Things et ses appareils connects, le rseau s'tend de plus en plus au sein de notre socit. L'actuelle faiblesse en terme de scurit lie aux objets connects reprsente une menace majeure et croissante dans notre environnement. Historique

Le concept, invent en 1988 l'universit de Oulu en Finlande, fut dvelopp l'origine pour grer les services associs au protocole IRCInternet Relay Chat, un protocole de communication textuel Le premier bot ¡GM¿ assistait ainsi l'utilisateur dans la gestion des connections IRC. Cette gestion automatise, permettant via un accs distance, de contrler et de raliser des oprations a trs vite montr un haut pouvoir malveillant. En Mai 1999, Pretty Park, un malware de forme trojan horse se propageant sur le net permettait de voler les mots de passe. Les premires drives furent notamment l'affrontement de botnet IRC (https://www.eggheads.org/Eggdrop en dcembre 1993, puis GTbot en avril 1998). Motivations lies la menace botnet itemize

- L 'aspect lucratif reprsente l'intrt majeur pour l'utilisateur de botnet. L'automatisation d'une tche contrle distance permettant de rapporter facilement des revenus (revente d'information, fraude au clic, spam), surtout si celle-ci est ralise de manire anonyme(rseau TORThe Onion Routing, un rseau d'anonymisation.
- L a motivation idologique, comme par exemple, lors du conflit entre la Georgie et la Russie en 2008 ou de nombreux sites tatiques faisant l'objet de cyberattaques massives paralysaient les infrastructures.
- L a motivation personnelle, travers la vengeance ou le chantage, est galement une finalit grce notamment au caractre anonyme de l'attaque.

Internet of Things ,
mmunication textuel .
eau d'anonymisation)