Extrait du Internet : Culture et Communication

http://filipe.f.ferreira.free.fr/dlst

Les moyens employés par les Hactivistes

- DLST Mag' - Hacktivisme -

Date de mise en ligne : mardi 17 d¥mbre 2013

Copyright © Internet : Culture et Communication

Les hacktivistes peuvent agir, communiqué et être soutenu.

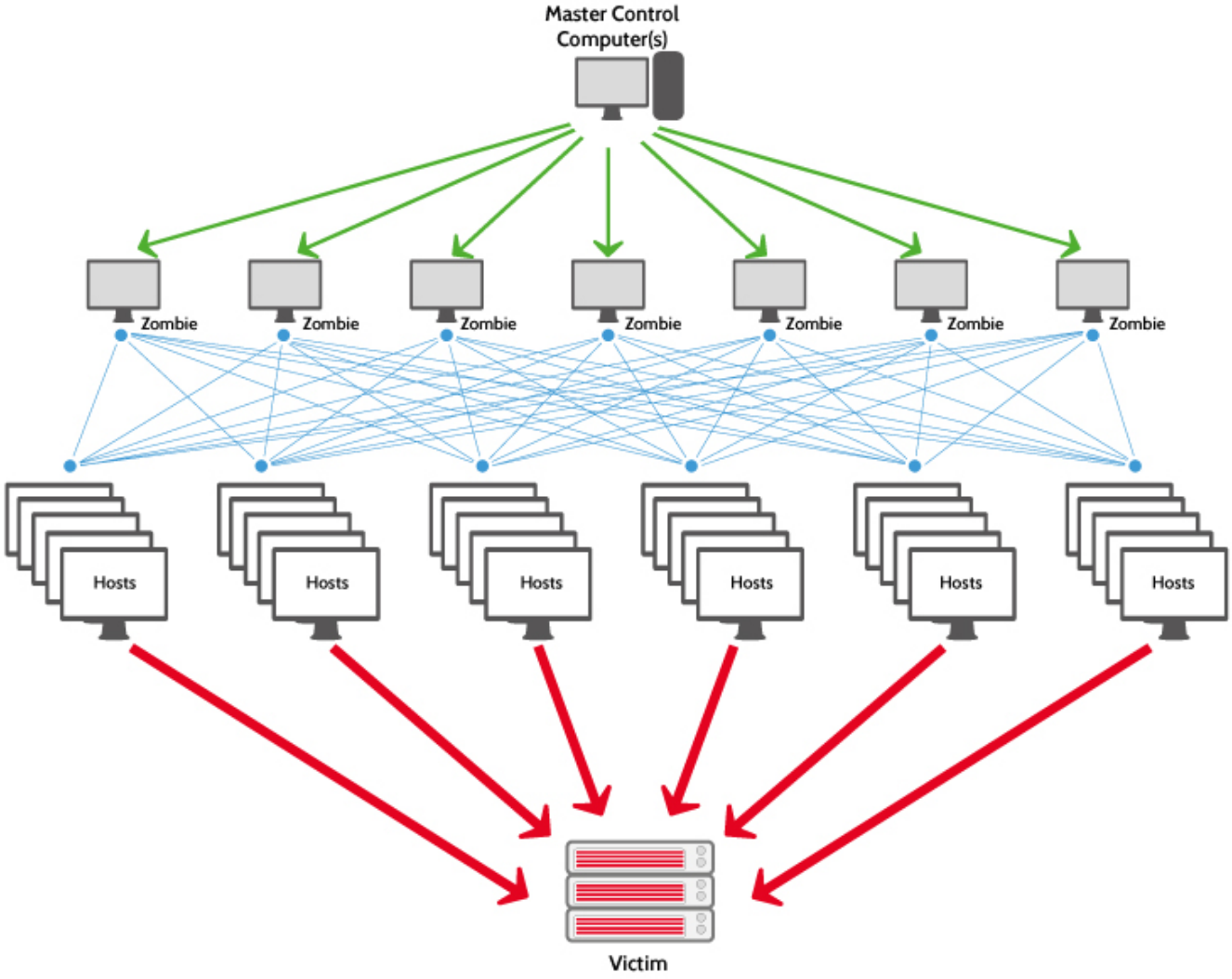
Les hacktivistes et leurs moyens d'actions

Les hacktivistes sont des activistes (ils cherchent a faire passer un bon message mais d'une mauvaise manière) cependant leurs moyens d'action sont directement liés au TIC.

Une des méthodes les plus connues est le Distributed Denial of Service dit DDoS. Cette méthode consiste a simplement « bombarder » de requête inutiles un serveur afin de saturé sa connexion internet. Ainsi deux cas de figure peuvent survenir : la machine a un puissance trop faible par rapport a ce qu'il lui est demander de traiter et son processeur va être utilisé a 100 % et donc dégager énormément de chaleur ce qui va conduire a une extinction préventive automatique du serveur ou (cas très rare) la machine ne dispose dispose pas de cette sécurité et va grillée. Le second cas est que la machine est suffisamment puissante pour encaisser la charge cependant sa connexion internet n'étant pas illimitée, toute tentative de connexion entraînera un délai de chargement conséquent ou une non réponse du serveur : un TimeOut.

Comment un hacktiviste peut-il lancer une telle attaque ? En effet aujourd'hui une requête de connexion a un serveur ne pèse que quelques octets or nos connexions sont capable de monter jusqu'à plusieurs mégaoctets/seconde et les serveurs peuvent disposer de plusieurs gigaoctets/seconde. Pour cela un hactivistes ou plus souvent un groupe de hactiviste disposent de ce qu'on appele un BotNet. Ce terme décrit en fait un réseau de d'« ordinateur zombie » que le hactiviste peut contrôler en leur ordonnant d'attaquer une adresse précise (la cible). Ces botnets disposent en générale de plusieurs milliers de pc zombie. Ces réseaux sont développés via la création d'un cheval de Troie : Une victime exécute le virus (en croyant récupéré autre chose) et le virus va alors ce dissimulé et agira en tache de fond dès qu'il detectera un ordre sur un serveur maitre. Ce moyen est egalement utilisé par les hackers pour faire de l'argent.

Copyright © Internet : Culture et Communication

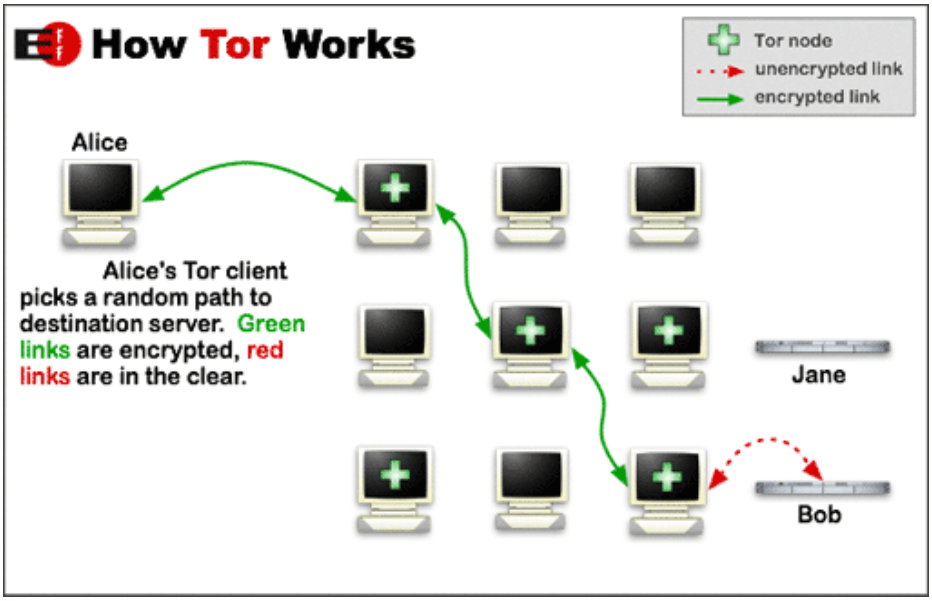


Fonctionnement d'un botnet (© OVH) Une autre méthode, moins courante, est le piratage d'un site internet disposant d'une certaine popularités, donc consulté par un grand nombre de personnes, afin d'afficher un autre message. Ceci ce fait généralement par des injection de code via des failles XSS ou CSRF (voir) présente sur un site. Cependant, ces failles sont plus ou moins critiques car elle peuvent aller d'un simple accès au flux d'actualité d'un site jusqu'au contrôle totale de la machine distante et selon la sécurisation de cette dernière cela peut aller jusqu'au contrôle du réseau de machine intégrale du-dit site. Cette méthode peut être utilisé a des fin pas seulement marketting mais également au dérobement d'information sensible permettant de justifier la cause de ces hactivistes.

Enfin une dernière méthode, qui est moins virtuelle, consiste a utilisé une personne disposant d'un accès étendu a l'organisation interne d'une entité cible d'un groupe d'hacktivistes. On peut notemment cité le cas d'Edward Snowden ou de Bradley Mannings sur lesquels nous reviendrons plus tard.

Les hacktivistes et leurs moyens de communication

Pour communiqués un hacktiviste ou un groupe d'hacktivistes peut s'y prendre de plusieurs manière : La méthode numéro 1 est de produire un coup d'éclat médiatique, qui va attiré la presse vers lui (l'affaire Snowden encore une fois est un bon exemple). Ensuite, un groupe peux communiqué via les réseaux sociaux (Facebook ou Twitter) Twitter étant très utilisé par Anonymous notemment. Enfin ils peuvent communiqué entre eux de manière sécurisé via le deepweb.



Fonctionnement du réseau TOR (Licence CC)

Le réseau Tor est très utilisés car chaque requête des utilisateurs du réseaux est transmis par l'intermediaire d'un autre utilisateur qui va son tour la transmettre et ainsi de suite plusieurs dizaine de fois, ainsi l'information est sécurisée.

Pour plus d'information sur TOR rendez vous ici

Les hacktivistes et leurs soutiens



Anonymous (Licence CC) Les hacktivistes peuvent disposé de moyens de soutiens des plus inattendu, car aujourd'hui il y a deux cas majeurs connus : Le premier est Julian Assange, cette est a l'origine du site WikiLeaks qui a fait fuiter des milliers de cables diplomatique relatifs au Etats Unis. Quelques semaines plus tard une plainte pour viol arrivait de Suède, il s'est donc enfui et a finalement était coincé par la Grande Bretagne. Son procès devait l'extrader vers la Suède ou il a fait appel et a saisi la cour des droits de l'homme de l'UE puis quelques jours avant le verdict qui semblait clairement en sa défaveur il est aller se réfugier dans l'ambassade d'Equateur pour demander

l'asile politique qu'il a obtenu malgré les menaces de pression de l'Angleterre qui envisageait un assaut contre l'ambassade. Le deuxième cas, qui est même dès plus surprenant est celui d'Edward Snowden qui travaillait comme Administrateur système pour la CIA et la NSA a mis au jours un dès plus gros scandale de surveillance mondiale généralisée via l'aide de société privé comme Google, Facebook ou Microsoft. Celui ci a envisagé les même solution que Assange, il a d'abord fuis de Hawai vers Hong Kong puis finalement vers la Russie où son passeport a était invalidé par les Américain, il a finalement obtenu un asile temporaire de 1 an en russie.

Copyright © Internet : Culture et Communication