Anonymat, communication, comment les Hacktivistes se protègent-ils ? (article)

- DLST Mag' - Hacktivisme -

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

Le Hacktivisme et ses outils

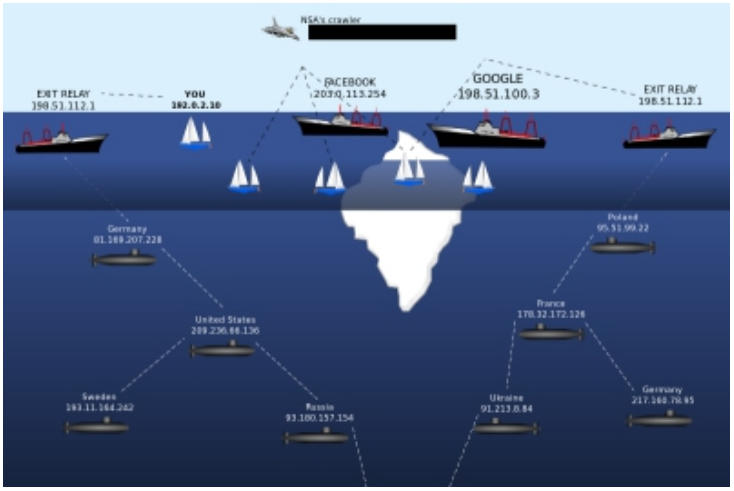
Anonymat, communication, attaques, quels outils sont-ils devenus incontournables auprès des Hacktivistes et pourquoi ?

Avec les initiatives des gouvernements, la sécurité et l'anonymat des Hacktivistes devient plus une nécessité qu'un simple enjeu. En sont d'excellents exemples ceux que nous appelons les « lanceurs d'alertes » comme Edward Snowden qui, en 2013, pour nous avoir révélé l'existence de la NSA et du PRISM, deviendra l'une des personnes les plus recherchées par les États-Unis. De tels événements révèlent bien évidemment la réelle utilité d'outils comme le Deep Web ou les VPNs pour les Hacktvistes et autres internautes utilisant le Web pour agir dans le sens contraire de la loi.

Quels sont ces outils ?

On peut compter un grand nombre d'outils utilisés par les Hacktivistes pour parfaire à leurs fins. De simples scripts d'attaque par force brute au Deep Web en passant par les réseaux anonymes et les VPNs, les Hacktivistes ont l'embarras du choix en matière de sécurité et d'efficacité. Dans la suite de cet article, nous allons établir une liste des outils les plus connus et les plus incontournables auprès des Hacktivistes.

Le Deep Web



On peut désigner un grand nombre de choses par Deep Web, sans compter le nombre de fois où ce terme est utilisé à tord. Techniquement, on entend par Deep Web l'ensemble des sites qui ne font pas partie du web surfacique (ou plus communément appelé web visible), c'est à dire du web indexé par les moteurs de recherche et auxquels il est impossible d'accéder via un hyperlien depuis d'autres site du web visible. De ce critère découlent en réalité plusieurs types de Deep Web : les sites simplement non indexés mais bien accessibles directement sans outil spécifique, les serveurs privés protégés avec par exemple des mots de passes, les réseaux anonymes (Tor, Freenet)...

Cependant, dans le cas des Hacktivistes, tous ces types de sites sont-ils réellement utiles ? Peuvent-ils s'en servir pour partager des informations ? Communiquer entre-eux ? Attaquer ?

Le projet Tor

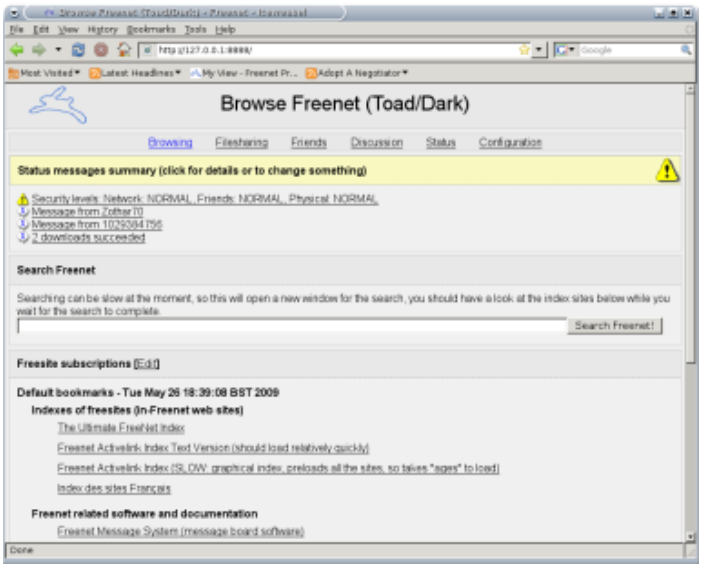
Tor, acronyme de The Onion Router, soit « le routeur oignon » en français, est un réseau anonyme mondial et décentralisé. Tor est composé d'un impressionnant nombre de routeurs appelés nSuds de l'oignon, qui transmettent de manière anonyme des flux de données à ses utilisateurs. Sur le réseau, lors de la connexion, chaque client a accès à la liste des nSuds de Tor. Le système va ainsi y choisir un chemin aléatoire (qui sera, pour des raisons de sécurité, régénéré aléatoirement au bout d un certain intervalle de temps), puis construire un « circuit » au sein duquel chaque nSud a la propriété de connaître son prédécesseur et son successeur, sans en savoir plus.

Ainsi, lors de votre navigation sur le réseau Tor, le premier nSud du circuit connaîtra votre adresse IP. Mais dès le deuxième nSud, la négociation se fera par l intermédiaire du circuit partiel déjà construit, de sorte que le deuxième nSud, par exemple, ne connaîtra finalement que l adresse IP du premier nSud (et du troisième lorsqu un troisième nSud aura été ajouté). Un tel fonctionnement assure un anonymat total pour les utilisateurs du réseau et leur permet d'échanger des informations sans que ceux qui vont les consulter, qui peuvent être, par exemple, des polices, ne puissent connaître l'identité du divulgateur. C'est tout là l'intérêt de l'utilisation de Tor pour les Hacktivistes.

Concrètement, on peut compter un grand nombre de projets Hacktivistes utilisant Tor. En est un bon exemple WikiLeaks publiant des documents confidentiels et analyses politiques et sociales dont les informations, en plus d'être accessibles sur le site WikiLeaks en web surfacique, sont aussi disponibles sur un serveur accessible uniquement par le biais de Tor afin de pouvoir être consultées de manière anonyme. WikiLeaks propose aussi un service permettant d'envoyer de documents et des informations sensibles sur WikiLeaks via Tor afin d'éviter tout risque de dévoilement d'identité.

D'autres projets du même ordre fonctionnant grâce à Tor apparaissent, de plus en plus nombreux, comme SecureDrop, un système sécurisé permettant aux Hacktivistes et aux lanceurs d'alertes de faire parvenir des informations sensibles et des documents confidentiels à des journalistes (qui pourront lestransmettrent) sans compromettre leur identité. La personne possédant l'information se connecte à un site hébergé sur Tor où il pourra envoyer les documents de manière anonyme et les « destinataires » pourront, via ce même site, récupérer ces fichiers. SecureDrop est même livré avec un système d'exploitation basé sur GNU/Linux, nommé Tails, veillant à améliorer la sécurité de l'Hacktiviste.

Le projet Freenet



Freenet est un réseau informatique anonyme visant à permettre une liberté d'expression et d'information totale grâce à la sécurité fournie par l'anonymat. Freenet permet donc à chacun de lire comme de publier du contenu en tout anonymat et toute sécurité. Il offre la plupart des services actuels d'Internet comme le courriel, le Web et la messagerie instantanée (notamment IRC). Le projet Freenet a été lancé suite à la croissance des inquiétudes concernant les dangers qui planent sur la liberté d'expression sur Internet.

Techniquement parlant, Freenet est un grand espace de stockage partagé et distribué constitué de nSuds hébergés partout dans le monde. Contrairement à un espace de stockage classique, Freenet chiffre les données et, lors des partages, chaque nSud recevant des données va les conserver en mémoire afin de pouvoir à son tour les partager à d'autres nSuds du réseau.

Freenet n'est pas constitué d'un seul outil comme Tor, en effet plusieurs applications ont été développé pour ce protocole. Ainsi on retrouve Freesites Insertion Wizard (FIW), permettant de créer un « site » sur Freenet, appelé un « freesite », Frost permettant d'échanger des fichiers de pair à pair en utilisant Freenet et Freemail permettant d'envoyer et de recevoir du courrier avec Freenet.