

Internet : De MegaUpload Ã Anonymus, avis d'experts !

SÃ©curitÃ©

PostÃ© par : JulieM

PubliÃ©e le : 31/1/2012 13:30:00

En raison de lâ€™actualitÃ© forte sur le marchÃ© de la sÃ©curitÃ© informatique etÃ suite Ã la fermeture de Megaupload et Ã la rÃ©action des Anonymous, deux expertsÃ du marchÃ© de la sÃ©curitÃ© : **Guillaume Vassault-HouliÃ¨re**, Directeur Technique et OpÃ©rationnel de Hack in Paris et **Fabrice Prugnaud**, Vice PrÃ©sident EMEA de LogLogic, nous font part de leur rÃ©action..

- Guillaume Vassault-HouliÃ¨re, Directeur Technique et OpÃ©rationnel de Hack in Paris

Le but d'un Anonymous est d'Ãªtre anonyme donc potentiellement on ne sait rien d'eux. On sait globalement que les Anonymous franÃ§ais sont rattachÃ©s avec conviction aux Anonymous internationaux et qu'ils suivent les directives ou les actions du groupe.

La cible essentielle des Anonymous franÃ§ais est le site d'hadopi (hadopi.fr) mais comme expliquÃ© prÃ©cÃ©demment, ils suivent le mouvement international dont les cibles sont plutÃ´t situÃ©es Ã l'Ã©tranger, comme la derniÃ¨re opÃ©ration en date : "opmegaupload". L'opÃ©ration "opmegaupload" prend pour cible le FBI, universal music, hadopi, le site du ministÃ¨re de la justice amÃ©ricain etc. Plus globalement, toutes les cibles ayant un rapport direct ou indirect avec l'application du texte de loi SOPA, PIPA aux Etats-Unis et plus gÃ©nÃ©ralement le traitÃ© (ou l'accord commercial) ACTA au niveau international.



Les Anonymous ont peu, voire trÃ¨s peu de compÃ©tence technique. Ils utilisent le plus souvent des logiciels clÃ© en mains (loic ...) pour rendre indisponible le site de leur cible, on appelle cela des attaques de DDOS (distributed denial of service). Pour les plus avertis d'entre eux, ils effectuent des intrusions plus techniques afin de voler des donnÃ©es pour les rendre ou non publiques puis ils "defacent" leur cible pour revendiquer leur passage (defacer : supprimer la page d'accueil d'un site et la remplacer avec un slogan de propagande pour signer l'acte d'hacktivism).

Toutes les institutions qui Ã leurs convenances appliquent de faÃ§on directe ou indirecte la censure sur internet ou un non respect des libertÃ©s individuelles.

Il est souvent trÃ¨s difficile de remonter jusqu'Ã l'attaquant lorsqu'il est compÃ©tent. Dans notre cas, la grande majoritÃ© est identifiable et ne se cache que derriÃ¨re des pseudos sur

internet mais la masse rend plus complexe la répression.

Il existe des solutions de contre mesure pour ces types d'attaques qui réduisent le risque d'indisponibilité ou de fuite d'information mais celles-ci ont un certain coût.

La prise de conscience des risques n'est pas toujours présente sein des entreprises.

- Fabrice Prugnaud, Vice Président EMEA de LogLogic

Les Anonymous Français sont actifs de différentes façons et si les hackers et autres pirates peuvent se considérer comme membre du mouvement, le mouvement lui-même est très clair sur ces points en France.

Le blog des Anonymous Français répond systématiquement qu'il ne peut cautionner de telles attaques et que chaque individu est responsable de ses actes et ne peut revendiquer ses actions de piratages informatiques sous le nom des Anonymous. Le site présente environ 1400 membres actifs ce qui ne représente pas un groupe très largement actif.

Si l'origine du mouvement est socio-économique, il se présente comme un robin des bois moderne qui défend les droits des plus faibles et dénonce les abus de pouvoir des gouvernements et groupes de pouvoir institutionnels ou non. Les Anonymous français sont aujourd'hui plus tournés vers les sectes tels que les scientologues, cible prioritaire du moment qui pourrait effectivement faire l'objet d'attaques dans les jours à venir de la part de membre connu ou non des Anonymous. Le principe même du groupe étant l'anonymat, il est impossible d'en déterminer le nombre. Il est évident que certaine personne se sentant plus ou moins concernée par le mouvement peuvent participer à des actions sans pour autant être membre actif du réseau et ne pas être actives pendant les mois qui suivent.

Ces attaques sont les mêmes que celles subies par les entreprises privées : défaçage de site (changement de la page d'accueil par un message différent s'opposant à la marque ciblée), dénis de service (attaques multiples qui ont pour but de rendre le service inutilisable), attaques virales qui peuvent détruire certains programmes ou même intercepter des données.

Il existe différentes méthodes pour provoquer un déni de service et de nombreux programmes sont mêmes disponibles sur Internet. La quasi totalité de ces programmes consiste à se connecter à un serveur et à congestionner celui-ci par l'introduction d'une erreur qui fait un effet rebond et sature les processeurs machines jusqu'à ce que la bande passante disponible soit épuisée ou que le nombre de connexions demandées soit trop important pour être réalisées. La seule annonce d'un déni de service par les anonymes pourrait générer un déni de service si des millions d'internautes se connectaient à un même serveur en même temps.

Les cibles des Anonymous sont illimitées et dépendent uniquement du jugement qu'ils portent sur la justesse sociale d'une action entreprise par l'Etat ou une société. Si les lois PIPA et SOPA aux Etats Unis et la fermeture du site Megaupload ont déclenché une série d'attaques visant des sites de maison de production musicale et cinématographique, elles peuvent se porter partout où les Anonymous jugeront que la justice sociale n'est pas respectée.

Ainsi les sociétés publiques, les banques, les fournisseurs d'énergie et toutes autres institutions caractéristique global ou national qui influencent la vie sociale et le pouvoir d'achat sont des cibles potentielles.

Le danger pour les Anonymous aujourd'hui est la récupération de leurs motifs et

actions des fins de détournement financier titre privé ou mafieux. Ainsi, le vol de données type carte de crédit sur des sites commerciaux ne correspond pas aux motifs politiques annoncés des Anonymous. Si certaines attaques et vols de données bancaires subis par différentes sociétés ont été revendiqués par les Anonymous, il est impossible de prouver qu'il s'agissait bien d'eux et ceci ne semble pas correspondre à leur motif premier.

Les entreprises ont à leur disposition un arsenal de moyen de protection technique qui doivent leur permettre de se protéger et d'anticiper de telles attaques. Ainsi la mise en place de pare-feu permet d'identifier les adresses IP des serveurs demandant une connexion et de rejeter celles-ci. Ceci ne protège pas toujours d'une attaque distribuée (multiples tentatives de connexions simultanées émanant de plusieurs serveurs) mais il est aussi possible d'utiliser un réseau de protection distribuée (plusieurs niveaux de pare-feu et serveurs en amont) pour permettre au service de fonctionner même s'il est ralenti. Au niveau logiciels, la plupart des logiciels malveillants (malware) est connu et dispose d'une version « anti » et pour être reconnu en amont et stopper plus ou moins bien.

Un des principes fondamentaux de la sécurité informatique est la prévention des risques et les produits qualifiés de SIEM (Security information and Event Management). Ces derniers jouent un rôle majeur dans l'anticipation des risques. Tous les programmes informatiques contiennent des logs ou traces en français. Ces traces sont à l'origine utilisées pour résoudre un bogue (Bug en anglais) ou dysfonctionnement du logiciel. Ces traces sont l'empreinte digitale du système d'information et contiennent donc toutes les informations nécessaires à l'identification des personnes et des serveurs utilisés, la source ou non d'une connexion, l'identifiant du programme et toutes les caractéristiques de temps prises. Ainsi, si un pare-feu standard émet en temps normal un nombre x de traces (appelé message et mesuré en volume par seconde) il est très facile de fixer une limite haute et basse à partir de laquelle une alerte peut être lancée pour prendre une action. Une baisse consécutive du volume de traces signifiera que le serveur est en panne ou va stopper à l'inverse une hausse consécutive de ces volumes peut signifier une attaque de DDoS de service.

De la même façon si une adresse IP a été identifiée comme essayant de se connecter à plusieurs reprises sur un serveur sans succès, il est très facile de générer une alerte à l'apparition de cette adresse dans une trace et ainsi de configurer une interdiction formelle d'accès voir de remonter à la source. Dans ce but les opérateurs et fournisseurs d'accès internet ont des obligations de stockage de ces traces pour des périodes qui varient selon les pays européens. L'ensemble de ces données stockées permet d'effectuer des analyses dans le temps des activités d'un utilisateur ou d'un serveur. Ainsi, il est possible de rechercher toutes les actions passées sur plusieurs mois ou années suite à la découverte d'une seule action malveillante. Ces principes d'utilisation des traces sont utilisés dans toutes les formes de conformité auxquelles les entreprises sont contraintes depuis une dizaine d'années, qu'elles soient internes ou externes (ITIL, COBIT, ISO 27001, PCI, HIPAA ..).

Les événements quant à eux sont l'agrégation de plusieurs traces et permettent de corréler différentes informations entre elles pour anticiper une menace. Ainsi, il est possible de croiser deux informations distinctes A et B qui résultent systématiquement en un événement C à caractère malveillant pour stopper celui-ci.

Les responsables informatiques français sont conscients des risques et se montrent très intéressés par les méthodologies du log management des fins de protection mais aussi à des fins de gestion opérationnelle de leurs environnements. L'automatisation de la traçabilité des pannes ou défauts de fonctionnement permet d'augmenter la productivité des équipes et d'optimiser les ressources dans un environnement économique difficile ou les moyens mis en place ne sont pas toujours suffisants pour faire face à la complexité croissante des demandes

sÃ©curitaires et opÃ©rationnelles.