Internet : De MegaUpload Ã Anonymous, 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 etÂ suite Ã la fermeture de Megaupload et Ã la rÃ©action des Anonymous, deux expertsÂ 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'hacktivisme).

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 jusquâ□□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 rÃ©pression.

Il existe des solutions de contre mesure pour ces types d'attaques qui rÃ©duisent le risque d'indisponibilitÃ© ou de fuite d'information mais celles-ci ont un certain coÃ»t.

La prise de conscience des risques n'est pas toujours prÃ©sente sein des entreprises.

- Fabrice Prugnaud, Vice PrÃ©sident EMEA de LogLogic

Les Anonymous FranÃ§ais sont actifs de diffÃ©rentes faÃ§ons et si les hackers et autres pirates peuvent se considÃ©rer comme membre du mouvement, le mouvement lui-mÃªme est trÃ¨s clair sur ces points en France.

Le blog des Anonymous FranÃ§ais rÃ©pond systÃ©matiquement quâ□□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 prÃ©sente environ 1400 membres actifs ce qui ne reprÃ©sente pas un groupe trÃ¨s largement actif.

Si lâ□□origine du mouvement est socio-Ã©conomique, il se prÃ©sente comme un robin des bois moderne qui dÃ©fend les droits des plus faibles et dÃ©nonce les abus de pouvoir des gouvernements et groupes de pouvoir institutionnels ou non. Les Anonymous franÃ§ais sont aujourdâ□□hui plus tournÃ©s vers les sectes tels que les scientologues, cible prioritaire du moment qui pourrait effectivement faire lâ□□objet dâ□□attaques dans les jours Ã venir de la part de membre connu ou non des Anonymous. Le principe mÃªme du groupe Ã©tant lâ□□anonymat, il est impossible dâ□□en dÃ©terminer le nombre. Il est Ã©vident que certaine personne se sentant plus ou moins concernÃ©e par le mouvement peuvent participer Ã des actions sans pour autant Ãªtre membre actif du rÃ©seau et ne pas Ãªtre actives pendant les mois qui suivent.

Ces attaques sont les mÃªmes que celles subies par les entreprises privÃ©es : dÃ©faÃ§age de site (changement de la page dâ□□accueil par un message diffÃ©rent sâ□□opposant Ã la marque ciblÃ©e), dÃ©nis de service (attaques multiples qui ont pour but de rendre le service inutilisable), attaques virales qui peuvent dÃ©truire certains programmes ou mÃªme intercepter des donnÃ©es.

Il existe diffÃ©rentes mÃ©thodes pour provoquer un dÃ©ni de service et de nombreux programmes sont mÃªmes disponibles sur Internet. La quasi totalitÃ© de ces programmes consiste Ã se connecter Ã un serveur et Ã congestionner celui-ci par lâ□□introduction dâ□□une erreur qui fait un effet rebond et sature les processeurs machines jusquâ□□Ã ce que la bande passante disponible soit Ã©puisÃ©e ou que le nombre de connexions demandÃ©es soit trop important pour Ãªtre rÃ©alisÃ©. La seule annonce dâ□□un dÃ©ni de service par les anonymes pourrait gÃ©nÃ©rer un deni de service si des millions dâ□□internautes se connectaient Ã un mÃªme serveur en mÃªme temps.

Les cibles des Anonymous sont illimitÃ©es et dÃ©pendent uniquement du jugement quâ□□ils portent sur la justesse sociale dâ□□une action entreprise par lâ□□Etat ou une sociÃ©tÃ©. Si les lois PIPA et SOPA aux Etats Unis et la fermeture du site Megaupload ont dÃ©clenchÃ© une sÃ©rie dâ□□attaques visant des sites de maison de production musicale et cinÃ©matographique, elles peuvent se porter partout oÃ¹ les Anonymous jugeront que la justice sociale nâ□□est pas respectÃ©e.

Ainsi les sociÃ©tÃ©s pÃ©troliÃ¨res, les banques, les fournisseurs dâ□□Ã©nergie et toutes autres institutions Ã caractÃ¨re global ou national qui influencent la vie sociale et le pouvoir dâ□□achat sont des cibles potentielles.

Le danger pour les Anonymous aujourdâ□□hui est la rÃ©cupÃ©ration de leurs motifs et

actions Ã des fins de dÃ©tournement financier Ã titre privÃ© ou mafieux. Ainsi, le vol de donnÃ©es type carte de crÃ©dit sur des sites commerciaux ne correspond pas aux motifs politiques annoncÃ©s des Anonymous. Si certaines attaques et vols de donnÃ©es bancaires subis par diffÃ©rentes sociÃ©tÃ©s ont Ã©tÃ© revendiquÃ©s par les Anonymous, il est impossible de prouver quâil sâagissait bien dâeux et ceci ne semble pas correspondre Ã leur motif premier.

Les entreprises ont Ã leur disposition un arsenal de moyen de protection technique qui doivent leur permettre de se protÃ©ger et dâanticiper de telles attaques. Ainsi le mise en place de pare-feu permet dâidentifier les adresses IP des serveurs demandant une connexion et de rejeter celles-ci. Ceci ne protÃ¨ge pas toujours dâune attaque distribuÃ©e (multiples tentatives de connexions simultanÃ©es Ã©manant de plusieurs serveurs) mais il est aussi possible dâutiliser un rÃ©seau de protection distribuÃ© (plusieurs niveaux de pare-feu et serveurs en amont) pour permettre au service de fonctionner mÃªme sâil est ralenti. Au niveau logiciels, la plupart des logiciels malveillants (malware) est connu et dispose dâune version Â« anti Â» et pour Ãªtre reconnu en amont et stopper plus ou moins bien.

Un des principes fondamentaux de la sÃ©curitÃ© informatique est la prÃ©vention des risques et les produits qualifiÃ©s de SIEM (Security information and Event Management). Ces derniers jouent un rÃ´le majeur dans lâanticipation des risques. Tous les programmes informatiques contiennent des logs ou traces en franÃ§ais. Ces traces sont Ã lâorigine utilisÃ©es pour rÃ©parer un bogue (Bug en anglais) ou disfonctionnement du logiciel. Ces traces sont lâempreinte digitale du systÃ¨me dâinformation et contiennent donc toutes les informations nÃ©cessaires Ã lâidentification des personnes et des serveurs utilisÃ©s, la rÃ©ussite ou non dâune connexion, lâidentifiant du programme et toutes les caractÃ©ristiques de temps prÃ©cises. Ainsi, si un pare-feu standard Ã©met en temps normal un nombre x de traces (appelÃ© message et mesurÃ© en volume par seconde) il est trÃ¨s facile de fixer une limite haute et basse Ã partir de laquelle une alerte peut Ãªtre lancÃ©e pour prendre une action. Une baisse consÃ©quente du volume de traces signifiera que le serveur est en panne ou va stopper Ã lâinverse une hausse consÃ©quente de ces volumes peut signifier une attaque de dÃ©ni de service.

De la mÃªme faÃ§on si une adresse IP a Ã©tÃ© identifiÃ©e comme essayant de se connecter Ã plusieurs reprises sur un serveur sans succÃ¨s, il est trÃ¨s facile de gÃ©nÃ©rer une alerte Ã lâapparition de cette adresse dans une trace et ainsi de configurer une interdiction formelle dâaccÃ¨s voir de remonter Ã la source. Dans ce but les opÃ©rateurs et fournisseurs dâaccÃ¨s internet ont des obligations de stockage de ces traces pour des pÃ©riodes qui varient selon les pays europÃ©ens. Lâensemble de ces donnÃ©es stockÃ©es permet dâeffectuer des analyses dans le temps des activitÃ©s dâun utilisateur ou dâun serveur. Ainsi, il est possible de rechercher toutes les actions passÃ©es sur plusieurs mois ou annÃ©es suite Ã la dÃ©couverte dâune seule action malveillante. Ces principes dâutilisation des traces sont utilisÃ©s dans toutes les formes de conformitÃ© auxquelles les entreprises sont contraintes depuis une dizaine dâannÃ©es, quâelles soient internes ou externes (ITIL, COBIT, ISO 27001,PCI, HIPAA ..).

Les Ã©vÃ¨nements quant Ã eux sont lâagrÃ©gation de plusieurs traces et permettent de corrÃ©ler diffÃ©rentes informations entre elles pour anticiper une menace. Ainsi, il est possible de croiser deux informations distinctes A et B qui rÃ©sultent systÃ©matiquement en un Ã©vÃ¨nement C Ã caractÃ¨re malveillant pour stopper celui-ci.

Les responsable informatiques franÃ§ais sont conscients des risques et se montrent trÃ¨s intÃ©ressÃ©s par les mÃ©thodologies du log management Ã des fins de protection mais aussi a des fins de gestion opÃ©rationnelle de leurs environnents. Lâautomatisation de la traÃ§abilitÃ© des pannes ou dÃ©fauts de fonctionnement permet dâaugmenter la productivitÃ© des Ã©quipes et dâoptimiser les ressources dans un environnement Ã©conomique difficile ou les moyens mis en place ne sont pas toujours suffisant pour faire face Ã la complexitÃ© croissante des demandes

sÃ©curitaires et opÃ©rationnelles.