Selon FireEye, 184 pays sont déjà engagés dans la cyberguerre

Dans une étude à paraitre lundi, l'éditeur de sécurité FireEye met en évidence une forme de généralisation et de banalisation des cyber-attaques et des attaques persistantes (**APT** pour Advanced Persistent Threat) visant à s'installer dans les systèmes d'information de l'entreprise sur la durée pour soutirer de l'information. Tant au niveau des Etats, prompts à se lancer dans la cyberguerre, qu'au niveau des entreprises.

« *Les gouvernements se sont engouffrés dans ce nouvel espace de guerre* », note **Denis Gadonnet**, le directeur Europe du Sud de cet éditeur américain. Selon l'étude, 184 pays ont été impliqués en 2012 dans des formes de cyberguerre, soit comme cibles, soit comme assaillants supposés. Il y a deux ans, seuls 130 états étaient engagés sur ce nouveau théâtre d'opérations.

Reste que cette comptabilité est très difficile à tenir, remarque FireEye, puisque, pour contourner des législations restrictives notamment, certains pays passent par des Etats tiers, où des groupes de hackers se vendant au plus offrant mènent des attaques en leur nom. Une forme de collusion entre Etats et cybercriminels donc.

La Chine ou le « carpet bombing »

D'après FireEye, les pays les plus prolifiques en matière d'attaques sont les Etats-Unis, la Corée (Nord et Sud), la Chine, la Russie, l'Ukraine et l'Allemagne.

Au-delà de ces Etats, l'éditeur identifie des comportements différents et des typologies d'attaques spécifiques en fonction de la zone d'où provient l'opération. « *La Chine se caractérise par du spear-fishing (technique consistant à tromper certains employés d'une organisation avec des e-mails ciblés et infectés, NDLR) à grande échelle, tandis que la Russie emploie des méthodes plus sophistiquées, de l'usurpation d'identités ou des techniques permettant à un malware de se mettre en sommeil s'il détecte une analyse visant à le détruire. De leur côté, les Etats-Unis ont recours à des attaques très sophistiquées, et extrêmement bien financées* », reprend le dirigeant.

La place de la **Chine** sur cet échiquier mondial de la cyber-terreur reste centrale. Selon FireEye, 89 % des bouts de code relatifs à des attaques d'origine inconnue proviennent de l'Empire du Milieu, les malwares chinois étant souvent ré-exploités par d'autres.

« *Les hackers chinois, qui sont organisés sur un modèle très pyramidal avec une équipe de direction très pointue et des soldats plus novices, mettent au point des attaques persistantes qui cherchent à pénétrer une organisation par n'importe quel biais*, note Denis Gadonnet. *Rappelons que l'attaque RSA est arrivée par le service RH.* » FireEye a identifié environ 200 groupuscules de hackers chinois plus ou moins liés à l'Armée populaire de l'Empire du Milieu.

Et ces campagnes de spear-fishing seraient très efficaces, selon FireEye. L'éditeur estime qu'une campagne de 3 e-mails a 50 % chances de réussir (autrement dit qu'un des trois employés ciblés se laisse abuser). Une proportion qui monte à 80 % si les assaillants mènent une deuxième campagne

de 3 e-mails.

Un malware toutes les 3 minutes

Rappelons que FireEye surfe sur les limites des défenses actuelles, reposant pour l'essentiel sur des signatures de malwares. Un procédé inopérant contre des exploits zero-day (non patchés par les éditeurs et non intégrés par les éditeurs de sécurité). « *Les entreprises ont bâti une nouvelle ligne Maginot* », ironise **Paul Davis**, le vice-président en charge des activités en Europe de FireEye.

« *Nous proposons la création d'environnements virtuels dans lequel nous laissons se dérouler l'attaque avant de détruire les machines virtuelles (VM) infectées* », précise Denis Gadonnet. L'éditeur revendique un million de VM déployées auprès de ses clients dans le monde entier. A noter que la société américaine, qui vient d'entrer en bourse après avoir été financé par le fonds de la CIA In-Q-Tel, se rapproche de **Cassidian**, la branche sécurité d'EADS, ce dernier étant appelé à servir de proxy pour l'Europe à l'éditeur. Une façon de contourner les réserves des entreprises après l'affaire Prism.

Depuis le début de 2013, l'éditeur affirme avoir détecté 23 millions d'activités de malware chez l'ensemble de ses clients. Une entreprise ou un gouvernement est ainsi ciblé par un malware toutes les 3 minutes. FireEye explique que, depuis janvier, 9 attaques zero-day réellement dangereuses ont été lancées, 7 étant détectées par sa technologie.

Comme l'explique **Greg Day**, le directeur technique pour l'Europe, « *le danger pour les entreprises consiste à regarder la sécurité uniquement sous l'angle des chiffres, et de se concentrer sur le nombre d'attaques bloquées. Or, plus une attaque est unique, plus elle est dangereuse et va s'installer pour longtemps dans les systèmes d'information. La sécurité ne consiste pas à gérer des volumes d'alertes, mais à recontextualiser les événements à la lumière de l'activité de l'organisation.* »

D'autant que les techniques d'APT (Advanced Persistent Threat) se démocratisent : 66 % des attaques détectées par FireEye en août n'ont visées leur cible qu'une seule fois. « *Or, moins une attaque est massive, plus elle est difficile à détecter* », prévient Greg Day.

Voir aussi
Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales