Sécurité : cybercriminalité, cyberattaques, cybervictimes

Quelles sont les principales menaces qui pèsent sur les réseaux ? D'où viennent-elles ? Combien de sites web distribuent des menaces ? Le **McAfee Threats Report** répond à ces questions.

Personne n'est à l'abri d'une menace. D'abord parce qu'il suffit de surfer sur le web pour s'exposer. Ensuite parce que nos messageries s'emplissent de spam forcément douteux – environ 2,5 messages spammés pour un message légitime – dont une 'petite' partie échappe aux protections déployées par les internautes, les entreprises, les opérateurs… Et les auteurs de ces menaces savent aujourd'hui détourner notre attention pour mieux nous piéger !

De victime à mafieux… non consenti

Victimes d'une attaque, combien d'entreprises sont capables d'en identifier l'origine et les responsables ? Si elles sont de plus en plus nombreuses à se poser la question, là aussi la complexité des menaces ne permet quasiment pas d'y répondre. En effet, ni la localisation ni l'adresse IP repérées ne permettent d'établir l'identité de l'auteur d'une menace.

Car il y a en réalité deux réseaux, celui de l'entreprise, menacé par celui des cyberpirates mafieux. Au départ, il y a deux ordinateurs : le premier est celui de l'internaute menacé, le second est celui à partir duquel se propage la menace qui cible le premier. Là où l'affaire se corse, c'est que lorsque l'ordinateur attaqué cède à la menace, il devient lui-même compromis. Conséquence, *« un ordinateur compromis peut devenir proxy pour le spam, les réseaux de robots, le déni de service et bien d'autres types d'activités malveillantes »*, constate le rapport d'analyse du réseau McAfee Global Threat Intelligence.

Les menaces du réseau, leurs origines, leurs victimes

Les réseaux sont principalement victimes de quatre types de menaces. Les appels de procédure à distance représentent plus d'un quart des menaces. Les injections de code SQL suivent de très près. Le navigateur a ravi la troisième place à l'exécution forcée de scripts sur les sites web (cross-site scripting). À elles quatre ces menaces occupent environ 80 % du terrain des cyberattaques.

Les États-Unis sont à la fois le premier pays source des menaces, parfois très largement, et le premier pays victime. D'autres contrées se distinguent également, mais dans une moindre mesure. Le Royaume-Uni et le Vénézuéla côtoient les US sur les auteurs d'injection de code SQL. Taïwan et la Malaisie en victimes des exécutions forcées de scripts…

Les réseaux de robots

Les réseaux sont de plus en plus victimes des botnets, les ordinateurs compromis qui s'accumulent, généralement à l'insu de l'utilisateur, pour servir de base de lancement d'attaques comme du

spam. Le principal d'entre eux, environ 70 % des botnets selon McAfee, se nomme Mariposa. Ce réseau de robots, qui agit par paquets de sondes UDP, vient rappeler que de plus en plus de menaces sont mafieuses, à caractère financier visant à extorquer l'internaute inconscient. Mariposa vole les informations bancaires, en particulier les identifiants des cartes de crédit. Suivent parmi les principaux réseaux de robots Pushdo, déni de service via l'exploitation de failles ; les balayages de canaux IRC ; Spybot ; et Ainslot.B Traffic. Et près de la moitié des nouveaux serveurs de contrôle de réseaux de robots sont hébergés aux États-Unis.

De la réputation des sites web

« Un site servant à des attaques par phishing ou hébergeant des logiciels malveillants ou des programmes potentiellement indésirables sera catalogué comme site malveillant. » Un secteur où un sous-domaine, une adresse IP ou une URL spécifiques qualifient un site web et participent à sa réputation. Qu'un code douteux soit détecté et le site bascule sur la liste des sites malveillants. Au cours du premier trimestre 2012, les McAfee Labs en ont détecté en moyenne 9000 par jour, dont approximativement 4200 distribuent des logiciels malveillants et des programmes potentiellement indésirables ; 2200 nouvelles URL de phishing – les sites abritant des menaces de phishing sont plus nombreux que ceux hébergeant uniquement des téléchargements malveillants ou du spam – ; le reste étant des URL de spam.

De plus en plus d'internautes sont dirigés vers ces sites malveillants. Un client de McAfee sur six, les cinq autres clients ne consultaient pas de sites à risque (le rapport était de 1 sur 7 au dernier trimestre 2011 !). *« Ce chiffre est demeuré constant tout au long du trimestre et témoigne du succès rencontré par les cybercriminels qui tentent de rediriger les utilisateurs vers des sites malveillants »*. Le nombre de sites web hébergeant des téléchargements malveillants ou des exploits de navigateur continue d'augmenter. Sans surprise la majorité des nouveaux sites malveillants sont situés aux États-Unis. En revanche, *« l'examen des classements par région révèle qu'aucune zone de l'Internet planétaire n'est à l'abri des risques »*.