Des attaques informatiques de plus en plus ciblées en 2010

« Cinq tendances se dégagent, globalement en phase avec ce que l'on commençait à voir il y 18 mois pour la grande majorité des éléments », se félicite **Laurent Heslault**, directeur technologies de sécurité chez Symantec France, à l'occasion de la présentation du 16e ISTR (*Internet Threat and Security Report*), qui recense les menaces informatiques de 2010.

Un rapport construit à partir des données relevées sur le réseau Global Intelligence Network de l'éditeur et composé de quelques 240.000 'capteurs' répartis dans 200 pays dans le monde. Des capteurs qui ont piégé plus de **100.000 vulnérabilités logicielles** de 14.000 éditeurs, 5 millions de comptes spam et permet de filtrer 8 milliards d'e-mail et quelques 1 milliard de requêtes web quotidiennement. De quoi *« nous donner une vision assez claire de ce que se passe sur Internet à l'instant T »*, relève Laurent Heslault.

Cinq grandes tendances en matière d'insécurité informatique se sont dégagées en 2010. A commencer par les attaques de plus en plus ciblées, *« voire micro distribuées »*, selon le responsable sécurité. En témoigne les activités des maliciels Hydraq (un ver aux allures d'espion déjà très actif en 2009) et le très populaire Stuxnet visant à perturber les centrifugeuses nucléaires Siemens.

Le vol d'informations coûte 2,2 millions d'euros en France

Ces attaques ciblées se spécialisent également dans le vol d'information. Les récentes attaques de la Commission européenne et de son Parlement, qui s'ajoutent à celles de Bercy, en témoignent. Aux Etats-Unis, ce ne sont pas moins de **260.000 identités ainsi exposées** par brèches pour un coût moyen par pertes de données de 7,2 millions de dollars. Un chiffre bien supérieur aux 2,2 millions d'euros constatés en France où, néanmoins, la déclaration des pertes de données n'est toujours pas obligatoire et, donc, les frais de 'réparations' évitent les poursuites éventuelles et autres actions de groupes fort onéreuses en frais judiciaires. Il n'en reste pas moins que la tendance serait à la hausse de 16 %.

Autre tendance forte, l'**utilisation des réseaux sociaux** pour mener des attaques. Soit en exploitant les informations que les membres publient sur eux-mêmes (et qui va permettre de constituer une identité numérique en vue de son usurpation, soit livrer quelques indices pour déceler les mots de passe) ou directement comme vecteur de propagation d'un *malware*. Dans ce cadre, les réseaux sociaux sont en train de remplacer les campagnes de spam dont les 250 milliards d'envois quotidiens ont été divisé par dix depuis août 2010. La raison est simple : l'e-mail est en perte de vitesse. *« Les plus jeunes utilisent peu, voire pas du tout, le courriel au profit des messageries instantanées, réseaux sociaux et solutions mobiles »*, justifie Laurent Heslault.

D'où l'intérêt grandissant des cybercriminel pour les terminaux mobiles, smartphones au premier plan, et qui constitue l'une des grandes tendances des menaces numériques. Certes, pour l'heure, Symantec n'a décelé « que » **163 vulnérabilités** (essentiellement du côté d'Android qui s'impose désormais comme la première plate-forme du marché en nombre de smartphones utilisés) mais en rapide augmentation de 42 % (115 failles en 2009). Une tendance qui va aller en s'accentuant,

notamment avec l'émergence des tablettes.

286 millions de *malwares*

Tidserv, Mebratix, Mebroot… Les rootkits sont à l'honneur du rapport de Symantec. Ces techniques de camouflage de *malware* autorisent la mise en oeuvre de *« menaces de plus en plus furtives et qui recherchent la discretion maximale »*, tout autant que persistante. Installés au plus profond du système d'exploitation, notamment au niveau du MBR (qui contient notamment le fichier de démarrage), les rootkits sont en effet très difficiles à détecter.

Enfin, les kit d'attaques connaissent une véritable explosion en termes d'utilisation. Véritable mallette à outil du cybercriminels, ils peuvent être exploités par les experts comme par les débutants. En 2010, leur développement s'est notamment focalisé sur les vulnérabilités Java susceptibles de toucher plusieurs plates-formes pour le prix d'un seul développement du fait de la portabilité de la technologie développée par feu Sun Microsystems (mais son créateur, James Goslin, est bien vivant). Java concentre désormais **17 % des vulnérabilités** constatés dans les extensions des navigateurs.

Sans surprise, les menaces informatiques ont continué leur progression en 2010. Elles ont même explosé puisque Symantec a dénombré pas moins de **10 millions de signatures virales** contre 5 millions en 2009. Et quelques 286 millions d'agents malveillants, essentiellement constituées de variantes qui chercheront à exploiter les 6.253 nouvelles vulnérabilités (en hausse de 30 %) dont 14 de type «zero day» (sans correctif déployé au moment de sa constatation). Une augmentation compensée par la hausse des protections. Si les navigateurs restent vulnérables (191 failles pour Chrome, 100 pour Firefox, 59 pour IE), leur fenêtre d'exposition se réduit : 1 jour ou moins pour Chrome, Opera et Safari, 2 jours pour Firefox et 4 pour IE. Le jeu du chat et de la souris n'est pas prêt de prendre fin…