Sécurité: les attaques contre les entreprises ont augmenté en 2009

« Nous constatons de plus en plus d'attaques très ciblées qui peuvent viser quelques personnes dans une entreprise », annonce **Laurent Heslault**. Rien de très nouveau en soi mais pour le directeur des technologies de sécurité pour Symantec Europe de l'Ouest c'est *« une vraie confirmation de ce que l'on observe depuis deux ans »*. Le dirigeant intervenait dans le cadre de la présentation à la presse du 15e rapport ISTR (Internet Security Threat Report) qui porte sur l'analyse de l'activité cybercriminelle sur l'année 2009.

Parmi les nombreux événements qui ont rythmé 2009 en matière de sécurité informatique, l'année a été particulièrement marqué par deux principaux acteurs : le ver Conficker et le cheval de Troie Hydrac (également popularisé dans l'opération Aurora visant les attaques Google depuis Microsoft Internet Explorer). Apparu début 2009, le premier déploie une stratégie d'attaques massives, Symantec déclarant arrêter entre 9 et 12 000 instances du vers par jour. Le second, arrivé en fin d'année, misant sur des attaques ciblées, avec quelques dizaines démasquées hebdomadairement par l'éditeur de sécurité. Si Hydraq a notamment monopolisé l'attention début 2010, *« il ne s'agissait en fait que de la dernière d'une longue série d'attaques ciblées de ce genre, parmi lesquelles Shadow Network en 2009 et Ghosnet en 2008 »*, note l'expert en sécurité.

A la pèche aux informations

Il en résulte une augmentation des attaques des entreprises. Mais les méthodes infectieuses évoluent pour se concentrer sur quelques individus clés au sein de l'organisation. Les cybercriminels récoltant les abondantes informations personnelles distribuées sur les réseaux sociaux pour tenter de déduire les mots de passe pour manipuler ou usurper l'identité de la victime (comme l'a parfaitement démontré Hacker-croll sur Twitter).

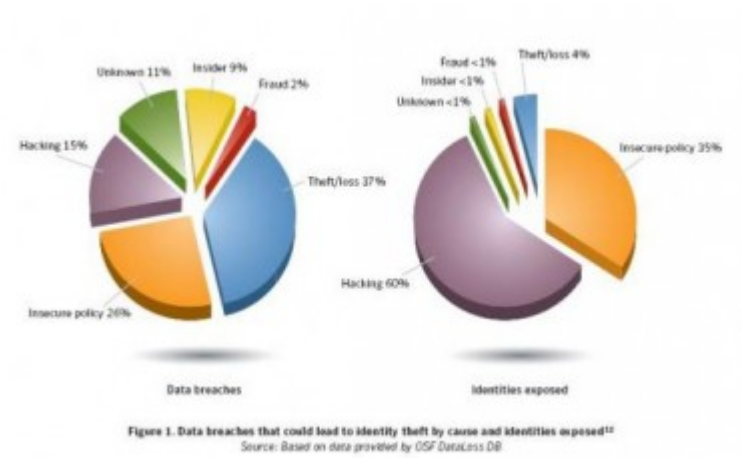

Figure 1. Data breaches that could lead to identity theft by cause and identities exposed[12]
Source: Based on data provided by OSF DataLoss DB

Au final, 60% des identités exposées en ligne ont été victimes d'attaques. Et 35% d'entres elles profitent des politiques d'insécurité des entreprises. Les pertes ou vols de données et les attaques internes ne concernent «que» 4% et 1% des attaques respectivement.

Flash et PDF en ligne de mire

L'année 2009 se distingue également par l'arrivée en force des attaques sur les vulnérabilités Flash et PDF, ces derniers comptant pour 49% des attaques web (11% en 2008). Mauvaise presse pour Adobe, éditeur des deux technologies mais Laurent Heslault rappelle que tous les lecteurs PDF sont concernés et pas uniquement PDF Reader. Si l'activité du phishing (*via* les campagnes de spam) reste intense, les attaques se concentrent sur les services financiers (78%) et les fournisseurs d'accès (12%). L'accès à un compte d'accès Internet ouvrant généralement la porte à nombre d'autres services (boîtes mail, etc.).

Attaques de plus en plus répétées à l'aide de kits disponibles sur Internet pour quelques centaines d'euros voire gratuitement. Ces boîtes à outils *« pour cybercriminels du dimanche »*, s'amuse le responsable, sont d'autant plus inquiétants qu'ils *« permettent à des novices de se lancer sur le marché du cybercrime »*. Ces kits sont notamment redoutables à cause de leur capacité à générer un grand nombre de variantes virales, d'autant plus difficiles à détecter par les antivirus traditionnels qu'ils nécessiteront une mise à jour indispensable de la base virale.

La France sort du Top 10

Symantec a par ailleurs relevé une moyenne de 46 541 botnets actifs (réseaux de PC infectés et contrôlés par les pirates) par jour et près de 6,8 millions d'ordinateurs zombies distincts. *« On a l'impression que le nombre de bot décline mais ils ont beaucoup évolué en terme de fonctionnalités et ils nous faut faire évoluer nos technologies de détection »*, reconnaît Laurent Heslault.

A noter que, selon l'éditeur de sécurité, les activités malveillantes suivent le développement des infrastructures et l'arrivée du haut débit dans les pays émergeants s'accompagne d'une montée en charge des cyberattaques. Si on observe une croissance des activités illicites au Brésil, en Inde et en Pologne, notamment, les Etats-Unis restent le premier territoire de la propagation des menaces informatiques avec 19% des attaques, en baisse cependant par rapport aux 23% de 2008. La Chine suit (8%) tandis que l'Allemagne perd sa 3e place (5%) derrière le Brésil (6%). A noter la sortie de la France du top 10. Pas parce que les Français sont plus malin que le reste de la planète mais parce que *« l'activité a continué de croître mais moins vite que dans les autres pays »*, analyse Laurent Heslault.