



Rapport sur le paysage des menaces au 4e trimestre 2010

L'année écoulée a été synonyme de transformation et d'évolution dans le domaine de la cybersécurité. Tout au long de l'année, nous avons assisté à une augmentation des attaques ciblées, à un renforcement de la sophistication et à une hausse des attaques ciblant les nouvelles catégories de périphériques, qui semblent devenir monnaie courante. Informer l'ensemble des utilisateurs de ces menaces sans pour autant déclencher une vague de panique inutile n'est pas chose aisée. Chez McAfee Labs, notre objectif est de permettre l'utilisation des technologies de la manière la plus sûre possible. Pour ce faire, nous devons analyser et expliquer ouvertement les conséquences des phénomènes auxquels nous assistons.

Ce trimestre a enregistré plusieurs des changements les plus intéressants de l'année. Durant ces trois derniers mois, nous avons observé le volume de spam le plus faible depuis 2007, mais avons identifié dans le même temps des attaques ciblant les nouveaux périphériques, tels que les smartphones équipés du système d'exploitation Android. Les logiciels malveillants (malwares) et les menaces visant l'environnement mobile circulent depuis des années, mais nous les acceptons désormais comme faisant partie intégrante du paysage mobile, que ce soit en termes de prise de conscience ou de déploiement. Ce trimestre a également connu des changements radicaux au niveau de la diversité des logiciels malveillants dans le monde, laquelle présente actuellement de grandes variations selon la localisation géographique des utilisateurs. La diversité des réseaux de robots a également connu des bouleversements majeurs au niveau mondial depuis le dernier trimestre, Cutwail ayant cédé sa place de n° 1 mondial. Enfin, les types de menaces numériques auxquels les utilisateurs sont confrontés varient en fonction de leur localisation géographique et du périphérique utilisé.

Impossible d'aborder ce trimestre sans mentionner le cyberactivisme, WikiLeaks et le groupe de cyberactivistes Anonymous. Ce chapitre de l'action politique pourrait devenir l'un des événements marquants de l'année 2010 — avec les divulgations de données et l'activisme bien présent dans les deux camps. Quelle que soit la ligne de conduite adoptée par les entreprises ou les utilisateurs, le cyberactivisme et le phénomène WikiLeaks sont voués à influencer les questions liées aux fuites de données, à la divulgation de données et à l'activisme politique pendant quelque temps encore. Mis à part WikiLeaks, de nombreuses autres activités cyberactivistes mondiales ont été identifiées ce trimestre. Dans le même temps, les pays de l'Europe de l'Est ont fait des progrès significatifs en matière de lutte contre la cybercriminalité.

Fin 2010, les logiciels malveillants ont atteint le taux de croissance global le plus élevé jamais enregistré tout en continuant d'afficher une grande diversité dans les catégories prédominantes de trimestre en trimestre. Nous passerons en revue certains des anciens « favoris », tels que le ver Koobface, les faux antivirus, les chevaux de Troie voleurs de mots de passe et les logiciels malveillants autoexécutables, afin de vérifier leur activité récente.

Fin 2009, McAfee Labs prédisait que 2010 serait une année très productive pour les exploits ciblant les produits Adobe et les faits lui ont donné raison. Les logiciels Adobe ont été de loin préférés aux logiciels Microsoft par les auteurs d'exploits, pour qui Adobe Reader et ses plug-ins Internet constituent aujourd'hui des cibles de prédilection. Les activités exploitant les vulnérabilités et les attaques par injection de code SQL nous ont également réservé quelques surprises au cours de ce trimestre. McAfee Labs a constaté quelques changements dans le détournement des termes et des moteurs de recherche, ainsi que dans les sites vers lesquels certains de ces liens redirigent les utilisateurs.

Les cybermenaces et la cybercriminalité trouvent de nouveaux terrains de jeu à mesure que les entreprises et les particuliers adoptent de nouvelles technologies et multiplient leurs activités en ligne au quotidien. Dans la mesure où les criminels traquent l'argent et les données, il serait irréaliste — et imprudent — de croire le contraire.