Résumé

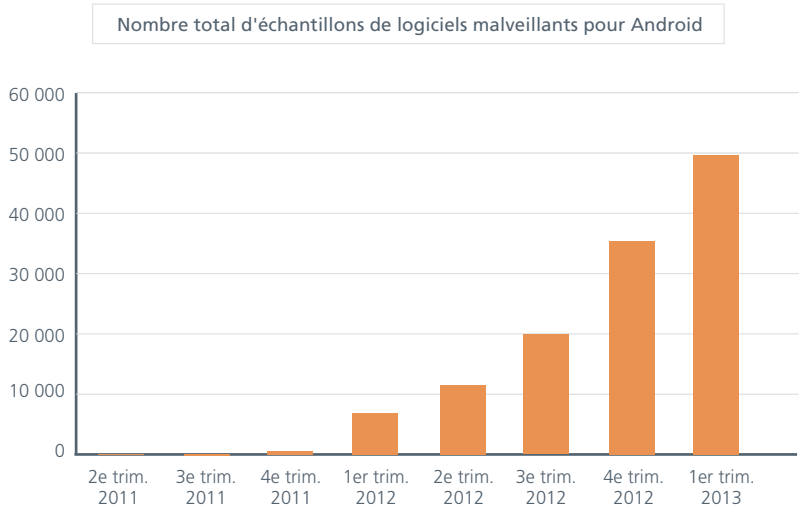
Rapport de McAfee sur le paysage des menaces : 1er trimestre 2013

McAfee® Labs

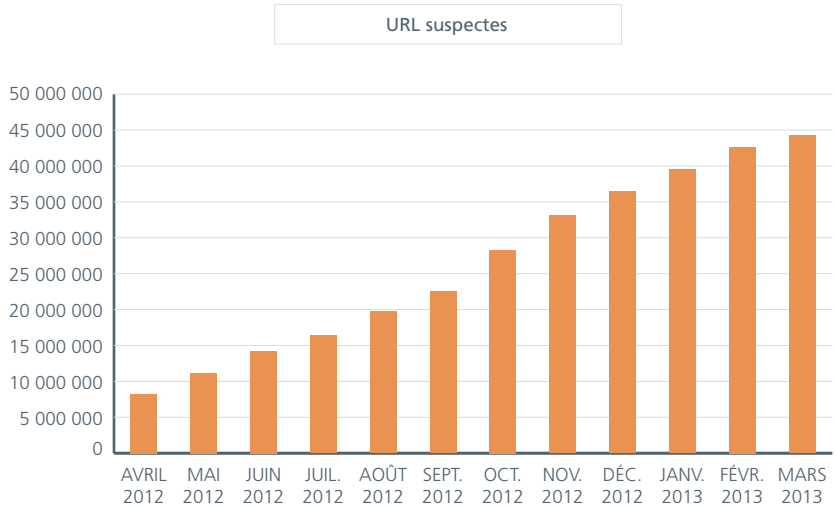
Au 1er trimestre 2013, la communauté cybercriminelle internationale semble avoir été inspirée par *Retour vers le futur* dans sa quête implacable d'argent et de victimes. Un grand nombre des tendances les plus significatives observées par McAfee Labs au cours des trois trimestres précédents sont en net recul, tandis que des types d'attaques plus anciens et une tendance que l'on pourrait qualifier de « rétro » ont enregistré une croissance importante.

Voici quelques-unes des tendances qui se sont essoufflées au 1er trimestre 2013 :

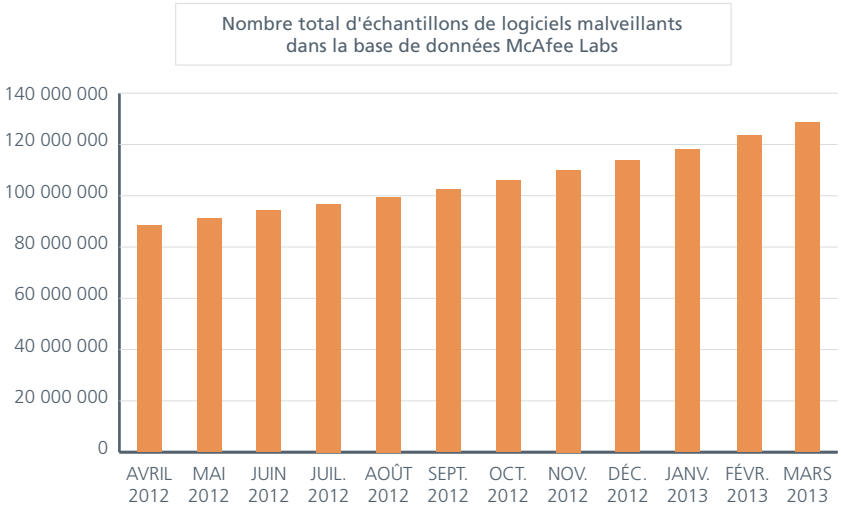
Un ralentissement a été constaté dans l'apparition de nouveaux logiciels pour mobiles (Android). Même si le nombre absolu de nouveaux échantillons de logiciels malveillants pour Android a grimpé de 40 %, cela représente en réalité une réduction de 10 % de leur taux de croissance par rapport au 4e trimestre 2012.



De la même manière, le nombre d'URL malveillantes détectées a progressé de 12 % au 1er trimestre, mais le taux de croissance, qui dépassait les 80 % au 4e trimestre, a chuté de près de 40 %.



Même la croissance des échantillons de logiciels malveillants connus a reculé légèrement au 1er trimestre, pour atteindre 28 % — contre 38 % au 4e trimestre 2012. McAfee Labs a ajouté plus de 14 millions de nouveaux échantillons de malware à sa base de données au 1er trimestre.



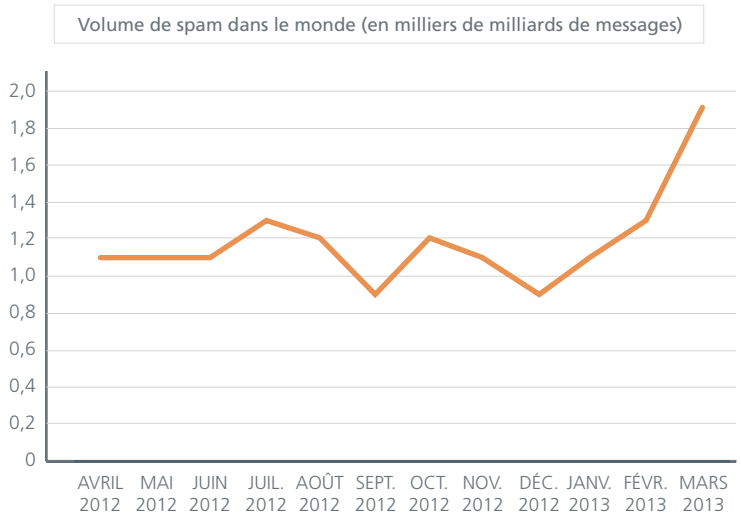
Enfin, le taux de croissance en volume des détections de rootkits, voleurs de mots de passe, faux antivirus et logiciels de demande de rançon (*ransomware*) est resté relativement stable au 1er trimestre. Toutes ces menaces continuent à augmenter en nombre absolu, tandis que leurs taux de croissance respectifs se tassent légèrement.

Ce ralentissement des taux de croissance ne doit toutefois pas nous laisser penser que le cyberespace devient plus sûr. Bien au contraire, si l'on combine ces chiffres à d'autres tendances observées au 1er trimestre, il apparaît que la communauté cybercriminelle devient plus avisée et plus disciplinée, dans la mesure où elle manifeste une préférence de plus en plus marquée pour les attaques ciblées visant des communautés ou des régions géographiques particulières. Comme toute entreprise, les organisations criminelles aspirent à optimiser leur efficacité opérationnelle et leurs bénéfices. Cette tendance en faveur des attaques ciblées semble indiquer que le paysage mondial des menaces informatiques prend une nouvelle direction extrêmement dangereuse.

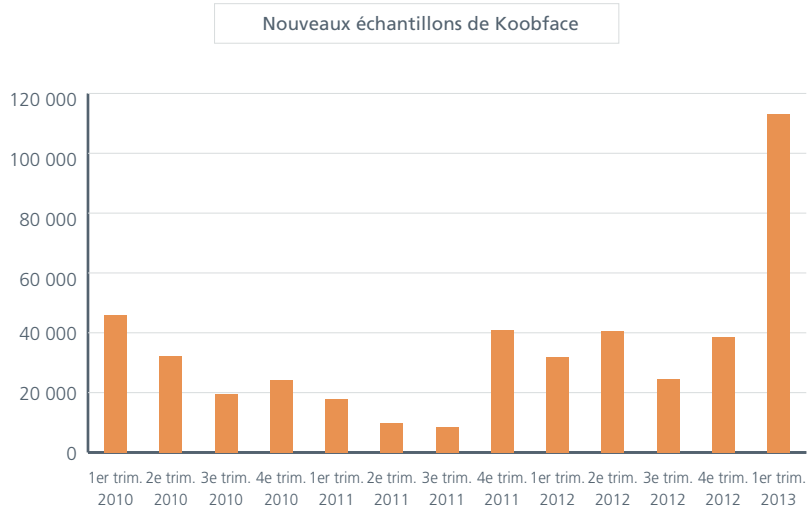
Le cheval de Troie Citadel constitue d'ailleurs un exemple représentatif de cet intérêt de plus en plus marqué pour les attaques ciblées. Conçu au départ pour voler de l'argent sur les comptes de certaines banques en particulier, Citadel a été « amélioré » et peut désormais servir à extraire des informations personnelles des victimes ciblées par l'auteur de l'attaque.

D'autres tendances du 1er trimestre 2013 sont des réminiscences du passé, mais désormais déployées dans des attaques ciblées et plus dangereuses. En voici quelques exemples :

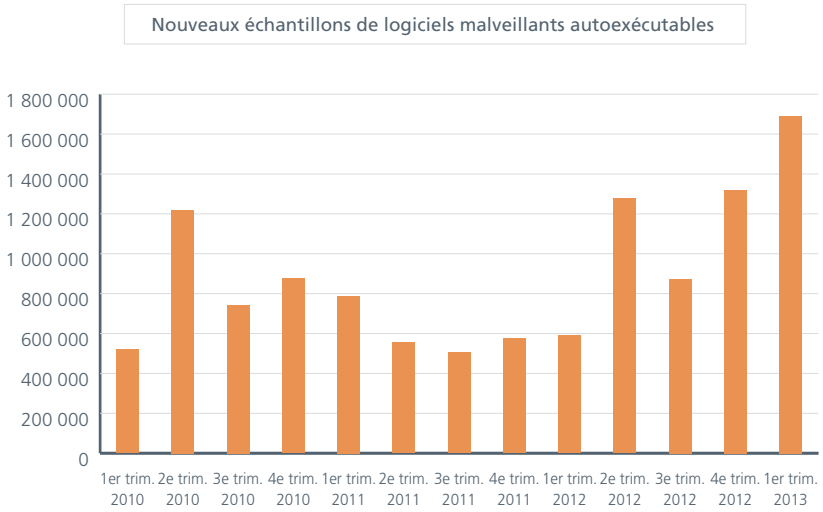
McAfee Labs a identifié la première augmentation du volume mondial de spam en plus de trois ans. Et il ne s'agit pas d'une résurgence mineure, puisque ce volume a pratiquement doublé au 1er trimestre 2013. Cela dit, le chiffre pour le monde est légèrement trompeur, car McAfee Labs a observé des différences très significatives dans la croissance du spam considérée au niveau régional. Une fois de plus, les cybercriminels semblent cibler des régions précises au moyen d'escroqueries bien particulières dans l'espoir de duper de nouvelles victimes. Parmi les plus utilisées au 1er trimestre, citons par exemple la résurrection des arnaques aux titres boursiers (*pump-and-dump*) ou aux prétendues hormones de croissance.



Les détections de Koobface, un ver découvert en 2008, avaient été relativement stables au cours de l'année dernière. Or, elles ont *triplé* au cours du 1er trimestre 2013 pour atteindre des niveaux record. La communauté cybercriminelle pense de toute évidence que les adeptes des médias sociaux constituent un riche vivier de cibles potentielles.



Autre tendance « rétro » : les échantillons de logiciels malveillants autoexécutables ont eux aussi connu une recrudescence au 1er trimestre. Par le passé, les vers autoexécutables étaient distribués via des CD ou des clés USB. Ces vers présentent un intérêt particulier pour les cybercriminels car ils peuvent servir à installer des voleurs de mots de passe ou des portes dérobées sur les machines infectées. Le pic dans les détections de logiciels malveillants autoexécutables est sans doute dû à la popularité des services de partage de fichiers dans le cloud.



En plus de ces attaques *Retour vers le futur*, McAfee Labs a constaté une hausse importante des attaques de la pile de stockage, une technique relativement récente. Aussi appelées attaques du secteur de démarrage principal (MBR, *master boot record*), leur objectif est d'infecter le système de stockage d'une machine et, à partir de là, de prendre le contrôle du terminal tout entier. La détection des échantillons de logiciels malveillants MBR a augmenté de plus de 30 % au 1er trimestre.

Que signifient ces tendances pour les entreprises qui souhaitent optimiser leur niveau de protection ? En ce qui concerne les postes clients, cette évolution du paysage des menaces impose l'emploi de défenses multiniveau, qui comprennent non seulement un antivirus de base, mais aussi la prévention des intrusions et le filtrage web. Au vu de l'utilisation croissante de sites web infectés pour la distribution des logiciels malveillants, ces deux fonctions sont plus importantes que jamais. Dans certains environnements, il peut être nécessaire d'ajouter à la fois des outils de contrôle des applications et de protection des équipements, dans le but d'assurer la sécurité des informations stratégiques hébergées sur les terminaux des utilisateurs finaux.

En plus de cette protection multiniveau des postes clients, il est indispensable d'équiper les administrateurs de la sécurité d'outils plus fonctionnels pour la génération de rapports et la réponse aux événements problématiques. Cette tour de contrôle évolutive sera de plus en plus importante pour permettre aux professionnels de terrain de réagir rapidement et efficacement face aux nouvelles attaques ciblées émergentes.

La protection de l'infrastructure exigera également une approche multiniveau dans le but de contrer les menaces transmises par le Web, la messagerie électronique et le réseau. La meilleure façon de se prémunir contre de nouvelles menaces consiste à les bloquer avant qu'elles ne s'insinuent dans l'infrastructure de l'entreprise. Toutefois, en plus des mécanismes standard de défense du périmètre, l'utilisation croissante des services de cloud exige que la sécurisation de l'entreprise soit étendue au cloud, et mise en œuvre de façon cohérente indépendamment de l'emplacement où sont déployées les données et les applications stratégiques.

Un exemplaire du rapport complet est disponible à l'adresse suivante :
http://www.mcafee.com/fr/resources/reports/rp-quarterly-threat-q1-2013.pdf.

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr