TEXTE: EDDY WILLEMS

Malware et cybercriminalité prolifèrent...

Eddy Willems est Security Evangelist et Analist chez Kaspersky Lab. Depuis près de 2 décennies, il est actif dans l'univers anti-malware, et est Directeur de l'Information et la Presse d'EICAR (European Institute for Computer Anti-Virus Research).

"Il faisait froid. J'ai rapidement refermé la porte derrière moi. 'A l'aéroport' ai-je indiqué au chauffeur de taxi, qui a aussitôt démarré. Après avoir discouru durant une dizaine de minutes de la pluie et du beau temps, mon chauffeur s'est lancé dans une histoire bizarre à propos de son ex-femme qui, selon lui, l'espionnait. Il me confia que son ex connaissait pratiquement tout de lui, depuis ses SMS jusqu'aux noms des personnes qu'il était seul à connaître. Je lui demandai alors de me montrer son GSM, un tout nouvel iPhone. Et devinez quoi? A son insu, son appareil hébergeait un spyware. Il était donc très facile à son ex-femme de consulter SMS et courriels, et de voir où se trouvait notre homme grâce au GPS.

Cette histoire démontre notamment la conception très "élastique" que certains ont de l'éthique, ainsi que la dangerosité de votre plus grand ami: votre GSM. Et puisque nous en sommes à parler d'éthique, citons le cas récent de ce magazine néerlandais qui, sur demande, a fait monter un canular à un "spécialiste en protection", à savoir lancer une 'brute-force attack' contre la boîte à messages d'une personnalité via le réseau social 'Hyves'. Les gens n'ont-ils donc plus aucune limite? Une série de spécialistes sont d'ailleurs d'accord avec moi pour dire que c'est précisément cet "estompement de la norme" qui expliquerait en partie, sous l'angle psychologique du moins, la cybercriminalité. Essentiellement motivée par la perspective d'un gain facile, la cybercriminalité règne en maître. L'an dernier, j'affirmais encore que vous étiez protégé durant environ 20 secondes sur le net. Aujourd'hui, la durée effective de protection n'avoisine plus qu'une seule seconde. Les chiffres issus de notre laboratoire indiquent en effet qu'en un an, nous sommes passés de plus de 2 millions de malware, virus et autres chevaux de Troie à près de 20 millions. Au début de 2008, nous annoncions d'ailleurs déjà de tels chiffres, et l'histoire nous a malheureusement donné raison. En ce moment, je n'ose d'ailleurs plus m'aventurer à ce type de calcul, tout ce que je puis dire, c'est que nous sommes inondés de malware. De ce fait, un grand nombre de fournisseurs se voient contraints de changer leur fusil d'épaule, et l'on voit pointer ici et là un nouveau buzzword: la prévention 'in-the-cloud'. Personnellement, je serais enclin à qualifier ce phénomène d'"évolution logique", et il n'est que normal que davantage de moyens soient mobilisés afin de mettre le holà à ce véritable flot de malware, ainsi qu'à cette cybercriminalité délirante. Les criminels n'hésitent pas, eux, à s'organiser, et deviennent de plus en plus professionnels, ce qui se traduit d'ailleurs par la prolifération que l'on sait. Quant à la crise économique, elle joue également un rôle dans l'histoire, et constitue vraiment du pain béni pour la cybercriminalité. Du reste, plus il y a de données en ligne, plus le risque s'accentue. S'il est clair en effet que l'informatisation peut contribuer à une utilisation efficace et effective de l'information, la mise en relation d'une masse croissante de données nous fait courir un risque encore plus grand, à savoir celui de voir ces données tomber entre de mauvaises mains. Alors, y a-t-il un espoir à l'horizon? Disons plutôt que les vecteurs d'infection ont tendance à se déplacer. Un magnifique exemple est la diminution de la diffusion de malware par courriel. Les attaques de type malware se focalisent aujourd'hui davantage sur les sites ou les environnement Web 2.0. Un très bel exemple nous est fourni par les vers ou parties de botnets, parfois dissimulés dans les grands réseaux sociaux comme Facebook. Or, à l'heure actuelle, force est de constater que la moitié de la Belgique se retrouve sur Facebook! Certains sont à peine capables d'utiliser un ordinateur, mais passent facilement une demi-journée sur Facebook. Et sur ce genre de sites, on a tendance à faire confiance à tout le monde et à n'importe qui.

Côté "security", sur le plan purement technologique, je suis plutôt de ceux qui pensent qu'au cours des prochains mois, nous devrions voir débouler des techniques novatrices et plus intéressantes. Après les technologies 'in-the-cloud', nous devons en effet nous demander s'il n'y a pas d'autres approches envisageables du concept de sécurité. Une entrée composée de cryptage et d'opportunités telles que parefeu, un plat principal qui verrait la virtualisation évoluer de concert avec des techniques proactives et heuristiques, accompagnées de whitelisting et assaisonnées d'une sauce IPS, le tout couronné d'un dessert à base de DLP et Vulnerability Checking et Remediation. En termes de malware, les choses iront donc de mal en pis au cours des prochains mois: botnets plus grands et plus complexes, soit davantage de malware basé sur Web 2.0, davantage de sites de réseaux sociaux confrontés à des problèmes, augmentation des problèmes de malware avec les Mac, irruption éventuelle du malware sur GSM, multiplication des "zero-day attacks" liées à la cybercriminalité.

Personnellement, je continue à plaider pour une collaboration internationale des fournisseurs avec les services de police et les organisations gouvernementales. D'ailleurs, les premiers jalons d'une collaboration internationale sont déjà posés. Ainsi, l'Union européenne propose des "patrouilles" en ligne. Une bonne idée, mais pas forcément facile à mettre en application, car le scénario pourrait prendre une tournure internationale très embarrassante.¶