Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

	Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

Les experts de l'éditeur de logiciels de sécurité informatique ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT (Advanced Persistent Threat ; Menaces persistantes avancées).

2015 sera l'année de la furtivité des cyber-menaces. © D.R.

Ces dernières années, Kaspersky Lab, un éditeur majeur de solutions de protection contre les cyber-attaques, a mis en lumière certaines des plus grosses campagnes d'attaques APT (Advanced Persistent Threats ; Menaces persistantes avancées), notamment RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/ The Mask et d'autres. Les experts de l'équipe de recherche du GReAT (Global Research et Analysis Team) de Kaspersky Lab ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT.

Fragmentation des plus gros groupes APT

En 2015 il faudra s'attendre à ce que les plus gros et les plus importants groupes d'attaques APT se divisent en plusieurs unités plus petites, opérant de manière indépendante. Cela entrainera une base d'attaque plus étendue et, donc, plus d'entreprises seront touchées du fait que chaque petit groupe diversifiera ses attaques. Dans le même temps, cela signifie que les plus grosses entreprises précédemment infectées par deux ou trois groupes APT majeurs (par ex. Comments Crew et Wekby) connaîtront plus d'attaques, provenant d'un panel de sources élargi.

La méthode APT sera utilisée pour un cyber-crime plus vaste

Pendant nombre d'années, les cybercriminels se sont focalisés exclusivement sur le vol d'argent de l'utilisateur final. Une explosion des taux de vols de cartes de crédit, de piratages des comptes de paiement électronique ou des connexions de banque en ligne ont causé aux consommateurs la perte de millions d'euros. Cependant les experts de Kaspersky Lab observent une tendance plus intéressante qui deviendra prééminente en 2015 : les attaques ciblant directement les banques et qui utiliseront des méthodes tout droit sorties des stratégies APT.

Les réseaux d'hôtels deviendront des cibles privilégiées.

Le Groupe Darkhotel est ainsi l'un des acteurs APT connus pour avoir ciblé des visiteurs particuliers durant leur séjour dans les hôtels de certains pays. Actuellement, les hôtels fournissent un excellent moyen de cibler une certaine catégorie de personnes, comme des dirigeants d'entreprise. Cibler les hôtels est également très lucratif car cela fournit des renseignements sur les mouvements d'individus importants dans le monde. En 2015, ce type d'attaques pourra se multiplier à plus grande échelle.

Evolution des techniques d'attaques.

Aujourd'hui, nous voyons déjà des groupes APT déployer constamment des malwares de plus en plus évolués pour des systèmes informatiques qui se complexifient constamment (comme Turla et Regin). En 2015, nous nous attendons à voir des implantations de malwares encore plus sophistiquées qui tenteront de déjouer encore plus efficacement les outils de détections des attaques.

Nouvelles méthodes d'exfiltration des données. Les jours où les attaquants activaient simplement une backdoor dans un réseau d'entreprise pour voler des téraoctets d'informations depuis les serveurs FTP dans le monde sont révolus. Aujourd'hui, des groupes plus sophistiqués ont recours aux SSL de manière régulière en plus des protocoles de communication personnalisés. En 2015, plus de groupes d'attaquants feront usage des services cloud afin de rendre l'exfiltration plus discrète et plus difficile à remarquer.

Utilisation de fausses bannières lors des attaques

Les attaquants commettent des erreurs. Dans la vaste majorité des cas analysés, nous observons des artefacts qui fournissent des indices sur le langage utilisé par les attaquants. Par exemple, dans le cas de RedOctober et d'Epic Turla, nous avons conclu que les attaquants parlaient probablement couramment le russe. Dans le cas de NetTraveler, nous avons abouti à la conclusion que les attaquants parlaient couramment chinois. Cependant les attaquants commencent à réagir à cette situation. En 2014, nous avons observé plusieurs opérations « fausses bannières» où les attaquants ont introduits des malwares inactifs communément utilisés par d'autres groupes APT. En 2015, avec la propension croissante des gouvernements à « nommer et pointer du doigt » les attaquants, les groupes APT vont prudemment ajuster leurs opérations et placer de fausses bannières dans la partie.

« Si nous pouvons qualifier l'année 2014 de 'sophistiquée', alors 2015 sera sous le signe de la 'furtivité'

Nous pensons que les groupes d'attaques APT évolueront pour devenir plus sournois et seront encore plus difficile à traquer. Cette année, nous avons déjà découvert des attaques APT utilisant les vulnérabilités dites « zéro day » ainsi que d'autres techniques plus persistantes et plus insidieuses encore. A partir de ces découvertes, nous avons développé et déployer de nouveaux outils de défense pour nos utilisateurs », explique Costin Raiu, directeur du GReAT de Kaspersky Lab.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-f344b63add3ab82ad1ae1f0fc9ae7dc8.htm par Erick Haehnsen