Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender publie ses prévisions en matière de sécurité. Dans son rapport, Bitdefender énonce les cinq évolutions notables qui impacteront notre façon de travailler, de jouer et de se sociabiliser sur Internet, au cours de l'année prochaine.

L'année 2016 verra un changement majeur dans la façon dont opèrent les cybercriminels. Le domaine probablement le plus impacté par cette refonte sera celui des PUA, dont l'activité s'est déjà accrue sur des plates-formes telles que Mac OS X et Android.
Suite aux nombreuses fermetures de réseaux de machines zombies et arrestations en 2015, les nouveaux cybercriminels transiteront probablement vers des systèmes de monétisation publicitaire spécifiques aux adwares agressifs, plutôt que de développer de nouvelles souches de malwares. Si pour le moment les botnets constituent toujours une partie importante de l'écosystème de la cybercriminalité, nous assisterons à une augmentation de la sophistication des PUA et des programmes incluant plus de greywares à l'installation.

La publicité sur le Web va également évoluer : étant donné le taux d'adoption ainsi que la popularité des bloqueurs de publicités, les régies publicitaires chercheront à utiliser des mécanismes plus agressifs afin de contourner ces blocages.

Les APT abandonneront le facteur de longévité
Les entreprises et les institutions gouvernementales feront toujours face à des attaques de ce type tout au long de 2016. Cependant, les APT (Advanced Persistent Threats, menaces persistantes avancées) mettront l'accent sur l'obfuscation et la récolte d'informations plutôt que sur la longévité. Les pirates ne s'infiltreront sur le réseau de l'entreprise que quelques jours, voire quelques heures.
Le monde de l'entreprise connaîtra une augmentation des attaques ciblées et des bots fortement obfusqués, avec une courte durée de vie et des mises à jour fréquentes, estime Dragoş Gavriluţ, Chef d'équipe au sein des Laboratoires antimalwares de Bitdefender. La plupart de ces attaques se spécialiseront dans le vol d'informations.
Également, l'évolution latérale de l'infrastructure des fournisseurs de services Cloud ira de pair avec l'avènement d'outils permettant aux pirates de compromettre l'hyperviseur à partir d'une instance virtuelle et de passer d'une machine virtuelle à l'autre. Ce scénario est particulièrement dangereux dans des environnements de « mauvais voisinage », où un tiers mal intentionné serait amené à partager des ressources sur un système physique avec un fournisseur de services ou une entreprise légitimes.

Des malwares mobiles de plus en plus sophistiqués
Du côté des particuliers, les types de malware sous Android sont désormais globalement les mêmes que sous Windows. Alors que les rootkits sont en perte de vitesse sur Windows, ils vont probablement devenir monnaie courante sur Android et iOS, car les deux plates-formes sont de plus en plus complexes et offrent une large surface d'attaque, affirme Sorin Dudea, Chef de l'équipe de recherche antimalwares. De nouveaux malwares mobiles, aux comportements similaires à ceux des vers, ou un réseau botnet mobile géant, sont deux autres possibilités envisagées pour l'année prochaine, selon Viorel Canja, Responsable des Laboratoires antimalwares et antispam chez Bitdefender. Ces attaques pourraient être la conséquence de techniques d'ingénierie sociale ou de l'exploitation de vulnérabilités majeures (telles que Stagefright) sur des plates-formes non patchées.

L'Internet des Objets (IOT) et la vie privée
La façon dont nous gérons notre vie privée va aussi changer durant l'année 2016. En effet, les récents vols de données ont contribué à mettre une quantité importante d'informations personnelles en libre accès sur Internet, rendant ainsi le « doxing » (processus de compilation et d'agrégation des informations numériques sur les individus et leurs identités physiques) beaucoup plus facile pour des tiers.
Les objets connectés vont devenir de plus en plus répandus, donc plus attrayants pour les cybercriminels. Compte tenu de leur cycle de développement très court et des limites matérielles et logicielles inhérentes à ce type d'objet, de nombreuses failles de sécurité seront présentes et exploitables par les cybercriminels ; c'est pourquoi la plupart des objets connectés seront compromis en 2016, ajoute Bogdan Dumitru, Directeur des Technologies chez Bitdefender. Également, les réglementations de surveillance de type « Big Brother », que de plus en plus de pays essaient de mettre en place pour contrecarrer le terrorisme, déclencheront des conflits quant à la souveraineté des données et le contrôle de leur mode de chiffrement.

Les ransomwares deviennent multiplateformes
Les ransomwares sont probablement la menace la plus importante pour les internautes depuis 2014 et resteront l'un des plus importants vecteurs de cybercriminalité en 2016. Alors que certains pirates préfèrent l'approche du chiffrement de fichiers, certaines versions plus novatrices se concentreront sur le développement de « l'extortionware » (malware qui bloque les comptes de services en ligne ou expose les données personnelles aux yeux de tous sur Internet).
Les ransomwares visant Linux vont se complexifier et pourraient tirer parti des vulnérabilités connues dans le noyau du système d'exploitation pour pénétrer plus profondément dans le système de fichiers. Les botnets qui forcent les identifiants de connexion pour les systèmes de gestion de contenu pourraient aussi se développer. Ces identifiants pourraient être ensuite utilisés par les opérateurs de ransomwares visant Linux pour automatiser le chiffrement d'une partie importante d'Internet.
Enfin, les ransomwares chiffrant les fichiers s'étendront probablement aux systèmes sous Mac OS X, corrélant ainsi avec les travaux de Rafael Salema Marques et sa mise en garde illustrée autour de son 'proof of concept' malware nommé Mabouia. En effet, si le principe de conception de Mabouia reste pour le moment privé, il pourrait être créé par des cybercriminels enrichissant alors leurs offres orientées MaaS (Malware-As-A-Service).

Réagissez à cet article

Source : *Bitdefender : Les 5 tendances en cybercriminalité pour 2016 – Global Security Mag Online*