Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigés contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (RDP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

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

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html