Données personnelles et objets connectés au centre des attaques en 2015

Explosion des malwares, multiplication des attaques sur les objets connectés, données toujours plus menacées ou encore opérations de cyber-espionnage constitueront les **principales menaces numériques attendue pour 2015, selon McAfee**. L'éditeur filiale d'Intel Security s'est appuyé sur les rapports dressés par ses quelque 400 chercheurs répartis dans le monde sur la base des données récoltées par ses 12 datacenters pour établir les tendances de l'année prochaine.

Les chercheurs en sécurité n'ont pu que constater la **courbe exponentielle de l'apparition des nouvelles menaces**. *« En 2003, quand je suis arrivé chez McAfee, nous recevions 5 000 échantillons (de code malveillant, NDLR) par mois*, relate David Grout, directeur Europe du Sud. *Aujourd'hui, nous en recevons 307 par minute, soit 5 par seconde environ. »* Une tendance qui pourrait s'accélérer en 2015 pour faire exploser les 300 millions de malwares répertoriés chez l'éditeur aujourd'hui. Avec un phénomène relativement récent qui prend de l'importance : l'**apparition d'échantillons personnalisés à usage unique** pour une cible et une opération précise. Un phénomène qui touche aujourd'hui **trois échantillons sur dix**.

« Il y a une véritable industrialisation du code malveillant, soutient le responsable de McAfee, *on trouve facilement sur Internet **des entreprises qui proposent des attaques sous forme de phishing, de spam**, disponibles 24/7 et avec garantie de résultats ou remboursement. »* Ces organisations peu scrupuleuses se retrouvent notamment dans les pays de l'Est, en Asie ou Afrique du Nord. *« Mais l'attribution géographique tend à disparaître. Ces organisations volatiles cherchent surtout les régions où la contrainte juridictionnelle est moins forte. »*

Vols d'identités

Autant d'attaques qui s'en prendront aux données personnelles. *« Une identité avec quelques renseignements précis se vend autour de 10 dollars, plus qu'un numéro de carte bancaire »*, soutient David Grout. La problématique des données personnelles sera un sujet d'autant plus brulant de 2015 que **pouvoirs publics et entreprises peinent à définir ce qu'est une donnée privée**. Une absence d'encadrement qui complexifie les moyens de protection à mettre en œuvre.

(Voir notre infographie : 2014, l'année de tous les records pour les vols de données)

Les ransomwares s'inscriront également comme un véritable sujet d'inquiétude l'année prochaine. *« Il y a un vrai risque sur le monde mobile, Android particulièrement, et **il faut s'attendre à voir une ou plusieurs vagues de cryptolockers sur la zone Europe**. »* Assez développées en Chine pour l'heure, les attaques par ransomwares consistent à chiffrer les données d'un système, PC ou smartphone, et à réclamer une rançon pour rendre l'accès aux fichiers. Rançon qu'il est, au passage, inutile de verser. *« Dans 99% des cas, les attaquants n'ont aucun intérêt à fournir la clé de décriffrement. C'est une opération supplémentaire qui pèse sur le retour sur investissement du cybercriminel et, surtout, c'est risquer de laisser des traces qui pourraient aider les forces de police à remonter à la source »*, explique le porte-parole de McAfee. **Les auteurs de ransomwares élargissent aujourd'hui leurs cibles aux données**

stockées dans le Cloud. Seule parade, faire des sauvegardes régulières sur des systèmes de stockage extérieurs ou demander à son fournisseur de services Cloud à revenir à une version antérieure de l'état du stockage.

L'Internet des objets figure également en bonne place des domaines suscitant la convoitise des cybercriminels. Ou plus précisément, *« tout ce qui sera doté d'une adresse IP »*. Un volume estimé à 15 milliards d'unités aujourd'hui (estimation qui intègre les objets connectés en Wifi et Bluetooth) et projeté à 50 milliards ou plus en 2020, selon les études. *« On a d'ores et déjà vu des preuves de concept sur* ***des Google Glass détournées pour prendre des photos toutes les dix secondes*** *»*. Plus récemment, l'attaque de milliers de webcam par un site russe a défrayé la chronique. Des pompes à insulines ou pacemaker contrôlables à distance, y compris en falsifiant les données que ces appareils vitaux produisent, à la voiture connectée en passant par les caméras intégrées aux télévisions connectées, c'est un nouveau monde plein de potentiel qui s'ouvre aux hackers. Autant de systèmes dont la gestion de la sécurité échappe par défaut à nombre d'utilisateurs. *« Vous pensez à mettre à jour votre système d'alarme à domicile, vous ? »*, glisse malicieusement David Grout.

Attaques non Windows

Autre tendance attendue pour 2015 en matière de sécurité : la multiplication des attaques des systèmes non Windows. Stimulés par la vulnérabilité Shellshock, les cybercriminels devraient **multiplier leurs tentatives contre les systèmes Unix, Linux et Mac OS X,** mais aussi les routeurs, filaires ou sans fil, les contrôleurs industriels, les systèmes de vols aéronautiques ou les infrastructures de gestion des terminaux, selon l'éditeur. Le monde Windows ne sera pas épargné pour autant. *« On constate une* ***grosse recrudescence du marché noir de la vulnérabilité non patchée****, non documentée, voire inconnue des éditeurs. »* Des failles dites zero day parfois vieilles de plusieurs années *« et exploitées sans qu'on le sache »*. Notre interlocuteur précise également que de plus en plus d'attaques visent la **destruction des données** (voir notamment le cas de Sony Pictures). Notamment pour effacer toute trace de passage des intrus.

Sans surprise, le monde mobile sera au centre de toutes les attentions en 2015. *« Il devient de plus en plus intéressant pour les hackers qui commencent à y voir un vrai intérêt en terme de retour sur investissement »*, indique David Grout. Sur les 300 millions d'échantillons de codes malveillants que référence McAfee, 5 millions sont consacrés aux plates-formes mobiles, Android quasi exclusivement. Avec une progression annuelle de 250 à 300 %. *«* ***On en attend 12 à 15 millions d'échantillons l'année prochaine****. »* Les attaques de mobiles accompagnerons celles visant les points de ventes (Target et Home Depot, notamment, en savent quelque chose) surtout aux Etats-Unis et en Asie où les terminaux de paiement sont seulement en cours d'adoption du système sécurisé par code PIN comme en Europe.

Enfin, 2015 pourrait être l'année des attaques des Etats par les Etats. *«* ***Beaucoup d'Etats voient aujourd'hui le monde cyber comme un nouveau champ d'opérations militaires*** *au même titre que la Terre, l'Air et la Mer. »* En France, cette vision est désormais intégrée à la loi de programmation militaire (LPM) adoptée en décembre 2013. DarkSeoul en 2013 (qui avait notamment bloqué les distributeurs de billets en Corée du Sud), The Mask en 2014 ou plus récemment Regin en sont quelques illustrations. Pour les Etats, attaquer les systèmes d'un pays est une démonstration de forces numériques, *« un coup de semonce »*, illustre David Grout. 2015, champ de bataille

numérique ?

Lire également
David Grout, McAfee : « sur la sécurité, les entreprises sont ambivalentes »
Les RSSI veulent faire du DSI un porte-parole de la sécurité
La sécurité informatique ? Les dirigeants français s'en moquent

crédit photo © bloomua – shutterstock