L’exploitation des vulnérabilités Flash ont explosé en 2015

Flash a décidément mauvaise réputation. Si, dans le sillage d’Apple, plusieurs acteurs, dont Facebook, commencent à bannir la technologie d’Adobe de leurs solutions, le *player* reste largement déployé à l’échelle mondiale. Et ses failles de sécurité sont toujours plus exploitées pour mener des attaques. C’est notamment ce que constate Bromium. *« Adobe Flash est l’une des applications les plus exploitées [pour des attaques] sur le terminal utilisateur »*, note le fournisseur de solutions de sécurité *Endpoint* en résumé de son rapport sur les tendances des *exploits* 2015. L’année dernière, la technologie d’Adobe a ainsi vu le nombre de ses vulnérabilités progresser de 333% par rapport à 2014 alors que la hausse du secteur se limite à 60% en moyenne.

Si Bromium n’explique pas directement cette inflation, plusieurs raisons peuvent en être à l’origine. A commencer par l’attaque de Hacking Team dont les failles zero day, que la société a l’habitude de vendre aux plus offrants, se sont retrouvées dans la nature. Et immédiatement intégrées aux kits d’attaques proposés sur le Dark Web. Flash constitue ainsi la technologie ciblée à hauteur de 73% au sein des kits d’exploitation (au premier rang desquels Angler) devant Internet Explorer (20%) et Silverlight (7%). Autre phénomène : les kits sont toujours plus à jour des dernières vulnérabilités exploitables et développent leurs capacités de contournement des technologies de détection d’attaques de base.

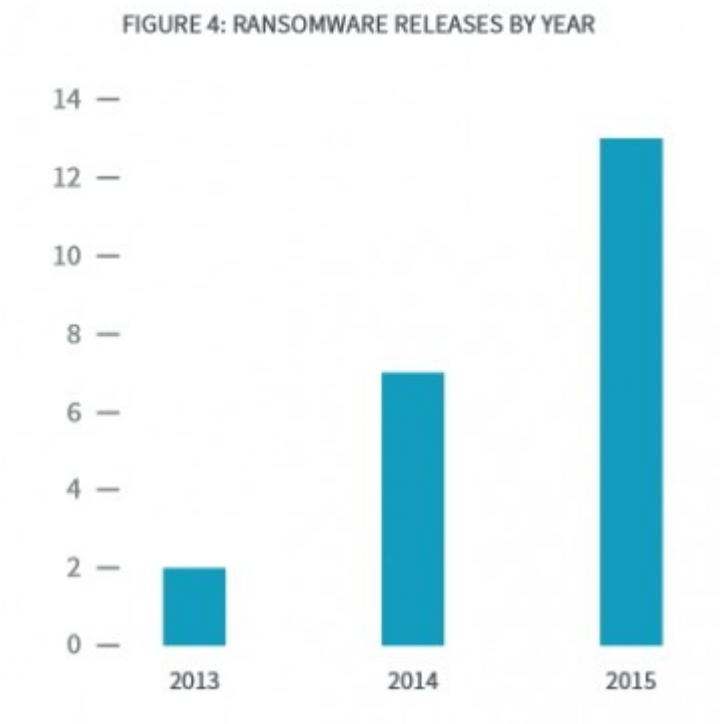
Les malwares macro reprennent du poids

Une tendance confirmée par Secunia Research. La filiale de Flexera Software spécialisée dans l’analyse des vulnérabilités logicielles place Adobe Flash en tête des logiciels les plus problématiques. Notamment en France alors que Flash 19 reste la version la plus distribuée sur les ordinateurs de près de trois quarts des utilisateurs français et qu’elle ne bénéficie plus de mise à jour de la part d’Adobe, selon l’analyste. *« Des vulnérabilités découvertes au sein de nouvelles versions de programmes peuvent être exploitées dans le but de pirater d’anciennes versions »*, note Secunia.

Les plugins pour navigateurs ne sont pas les seuls vecteurs d’attaque. Malgré les correctifs à la chaîne de Microsoft et l’évangélisation des utilisateurs, les malwares de type macro embarqués dans un document Word ou Excel et envoyés au travers de campagnes de phishing, repartent à la hausse à alors qu’ils se faisaient plus discrets jusqu’en 2014. *« Les volumes élevés de logiciels macro malveillants peuvent être attribués à une réaction [des cybercriminels] à l’élargissement des mesures de sécurité*, explique Bromium. *En réponse, les cybercriminels ont commencé à reprendre d’anciennes techniques pour propager de nouveaux malwares. »*

Hausse des crypto-ransomwares

Les crypto-ransomware connaissent également une croissance inquiétante avec le quasi-doublement de leur nombre en 2015. Pas moins de 10 familles de ces malwares, qui consistent à prendre en otage (par chiffrement) les données d'un PC et de les libérer contre rançon, étaient actives l'année dernière. Deux d'entre elles sont leaders, Cryptowall et TeslaCrypt. Dans tous les cas, tous les ransomwares arrivent sur les disques durs (ou flash) des utilisateurs par des attaques *drive-by-download* (installation automatique suite à la visite d'une page ou l'activation d'un logiciel), ou bien par l'intermédiaire d'un malware caché dans une macro.



« Les attaques en 2015 démontrent clairement la capacité des attaquants à contourner les technologies de détection –une tendance qui qui se poursuivra en 2016 », prévient Bromium.

Lire également
Sécurité : Apple, Mac OS X et iOS les plus vulnérables en 2015
Adobe Flash : c'est fini (dans Creative Cloud)
Adobe refroidit les entreprises d'utiliser Flash

crédit photo © drx – Fotolia.com