

Flash Player, cible préférée des kits de piratage

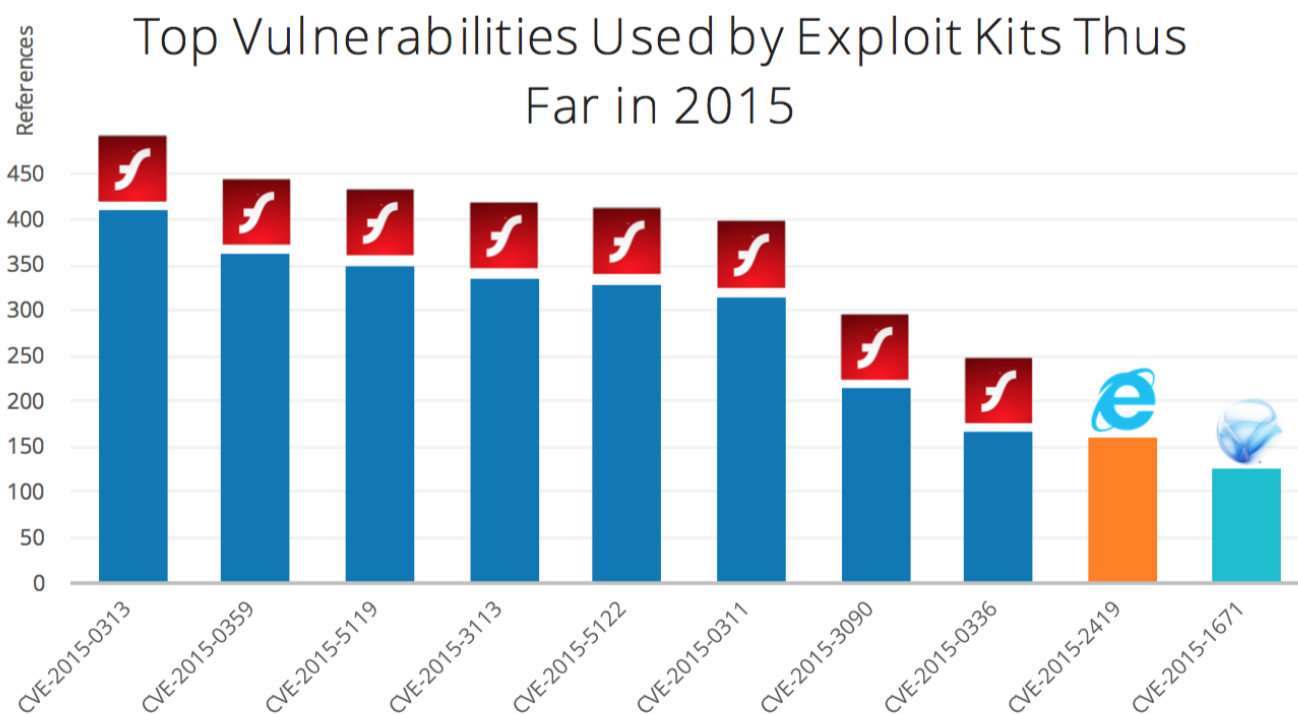
Les appels à supprimer Flash pour des questions de sécurité devraient connaître un regain avec la [récente étude](#) de Recorded Future. Cette société a mené l'enquête à travers des centaines de forums, médias sociaux, mais également sur des sites .onion (utilisant le réseau Tor) concernant les différents kits de piratage. Du 1^{er} janvier au 30 septembre 2015, l'analyse a recensé 108 kits d'exploits dont les plus connus et les plus utilisés sont Angler, Neutrino ou Nuclear Pack. Pour mener à bien leurs méfaits, ces boîtes à outils s'appuient sur des vulnérabilités dans des logiciels populaires.

Flash Player et le reste du monde

Recorded Future a dressé un palmarès des logiciels préférés par les kits de piratage. **Flash Player d'Adobe** est sans conteste le logiciel « roi » pour mener à bien des attaques. Le lecteur occupe **les 8 premières places du Top 10**. La première faille est connue sous le code CVE 2015-0313 qui affectait Flash Player 16.0.0.296. Cette brèche a été corrigée en février 2015, mais a été découvert dans plusieurs kits comme Hanjuan, Angler et Fiesta.

En troisième et cinquième position, on retrouve deux failles CVE-2015-5119 et CVE-2015-5122 issues du piratage de la société italienne **Hacking Team**. L'étude montre que la propagation de ces vulnérabilités a été très rapide après le piratage. Des traces ont été retrouvées dans Neutrino dès juillet 2015. Après ce piratage plusieurs voix se sont élevées pour supprimer définitivement Flash. Le journaliste spécialisé en sécurité Brian Kerbs s'est fendu d'un billet « [vivre un mois sans Flash Player](#) » en juin 2015.

En 9^{ème} position, on retrouve un zero day pour **Internet Explorer version 10 et 11**. La CVE 2015-2419 a été découverte par la société Vectra et provoque une corruption de mémoire Jscript9. Enfin pour clore ce palmarès, un autre produit de Microsoft, le plug-in **SilverLight** se positionne comme un vecteur d'attaques privilégié depuis le début de l'année.



La plaie des mises à jour

L'étude recommande donc aux utilisateurs de mettre à jour et d'appliquer les correctifs proposés par les éditeurs. Un vœu pieux, car la plupart des logiciels sont peu ou pas actualisés. Une plaie dénoncée récemment par [Secunia](#) qui élevait [VLC Player comme risque majeur de sécurité](#) pour les PC Français. Ce logiciel populaire est très rarement mis à jour par les internautes.

Dans son classement, Flash Player n'est pas absent, mais on le retrouve en tête du palmarès des programmes en fin de vie. Certains acteurs ont accéléré la mise à la retraite des anciennes versions de logiciels. Ainsi, à la fin du mois d'août, [Google enterrait les pubs Flash dans Chrome](#). Un exemple qui pourrait faire tâche d'huile...

A lire aussi :

[Faille Zero Day : Et de trois pour Flash Player !](#)

[Alerte aux failles critiques pour Adobe Flash Player 18](#)

Crédit photo : malesevic-shutterstock