Télégrammes : Backdoor Facebook, Sécuriser l'IoT, Flash préféré des kits d'exploit, Déblocage d'iPhone sans Apple

Une backdoor dans un serveur interne de Facebook ? C'est un chercheur en sécurité du nom d'Orange Tsai, travaillant pour la société taiwanaise spécialisée en sécurité DevCore, qui a découvert le pot aux roses. Il était à la recherche d'un bug sur Facebook pour glaner au passage quelques récompenses, quand il est tombé accidentellement sur la porte dérobée. En surfant sur les adresses IP du réseau social, il a découvert un nom de domaine intéressant, tfbnw.net, et un accès VPN, via vpn.tfbnw.net. S'il n'a pas réussi à casser le VPN géré par Juniper, le spécialiste recense néanmoins les classes d'adresses des serveurs qui y sont rattachés. Orange Tsai découvre notamment files.fb.com. Il s'agit de l'application (basée sur l'outil d'Accelion) utilisée par les employés de Facebook pour communiquer et partager des fichiers. Restait à trouver une faille sur Accelion, c'est chose faite avec un script caché écrit en PHP, Web Shell, présent sur le serveur de Facebook. Le réseau social a été averti et a récompensé d'une prime de 10 000 dollars le chercheur. Les équipes de sécurité de Facebook n'ont pas communiqué davantage sur la présence de cette backdoor et vont mener une enquête approfondie.

Flash, le soft préféré des kits d'attaques. Dans un rapport sur la cybersécurité, NTT Group estime qu'en 2015, les kits d'exploits se sont appuyés davantage sur les vulnérabilités de Flash d'Adobe que sur les faiblesses de Java. C'est même la première année que l'écart est si grand entre les deux solutions. Plusieurs raisons sont avancées par le NTT Group pour expliquer cette inversion. Tout d'abord, les différentes vagues de correctifs promues par Oracle sur Java ont permis de limiter l'utilisation de certaines failles. De l'autre côté, plusieurs failles zero day Flash ont été découvertes pendant l'année 2015. On se souvient par exemple que 4 failles critiques de la technologie d'Adobe entraient dans la besace de Hacking Team, société italienne sulfureuse spécialisée dans la vente de vulnérabilités inconnues. Un récent rapport de Symantec montrait que 17% des failles zero day portaient sur le logiciel d'Adobe.

Sécuriser l'IoT : les budgets vont manquer. Selon le Gartner, les dépenses mondiales pour sécuriser l'Internet des objets ont atteint 348 M$ en 2016, contre 282 M$ l'année précédente. Pour le cabinet d'études, ce total atteindra 547 M$ en 2018. Soit près de 30 % de croissance annuelle au cours des deux ans qui viennent. Mais, dans le même temps, le nombre d'objets connectés devrait passer de 6,4 à 11,4 milliards, soit une progression plus rapide d'environ 10 points. Pour le cabinet d'études, l'IoT sera impliqué dans 25 % des attaques en 2020, alors qu'il ne représentera alors que 10 % des budgets de sécurité IT. Gartner s'attend aussi à un basculement vers les solutions de sécurité dans le Cloud, qui pourraient, en 2020, être associées à plus de la moitié des déploiements IoT.

Déblocage d'iPhone : les Etats-Unis n'ont plus besoin d'Apple. Les services de police n'ont plus besoin de l'aide d'Apple pour débloquer un iPhone 5s tournant sous iOS 7 saisi dans le cadre d'une affaire de stupéfiants. Le ministère de la Justice américain a retiré sa requête devant une cour du district de New York, expliquant qu'un « individu avait fourni le mot de passe de l'iPhone concerné

». Dans cette affaire, le gouvernement avait, dans un premier temps, fait appel d'une décision de justice jugeant qu'Apple n'avait pas à fournir son aide en pareil cas. Selon le Wall Street Journal, c'est l'accusé, un dénommé Jun Feng, qui a fourni le code du smartphone après avoir décidé de plaider coupable. Cet épisode vient clore la seconde affaire où Apple s'opposait aux demandes d'assistance du gouvernement américain. Rappelons que la principale querelle concernait l'iPhone 5c d'un des auteurs de la tuerie de San Bernardino (14 morts en décembre 2015). Dans cette affaire, le FBI a acheté une ou plusieurs failles à des hackers anonymes pour contourner les sécurités d'iOS 9.