OpenDNS détecte les DNS malveillants avec le langage naturel

Un chercheur du laboratoire de sécurité d'OpenDNS (un service gratuit de redirection DNS) a développé une autre façon de détecter automatiquement et de bloquer des sites qui diffusent des malwares. L'opération se fait instantanément sans avoir de les scanner. Jeremiah O'Connor explique qu'il s'est servi du **langage naturel et d'autres outils analytiques** pour découvrir des domaines malveillants avant qu'ils puissent opérer sous un nom de domaine de camouflage. La solution de sécurité se nomme **NLPrank** et cible les requêtes DNS pour les sites qui ont des noms similaires aux sites légitimes (g00gle.com au lieu de google.com, par exemple). Ces sites ont en général des adresses IP qui ne correspondent pas aux blocs d'adresses affectés aux sites officiels.

Cette pratique de noms de domaine proches ou similaires est souvent utilisée par les cybercriminels pour pousser les internautes à visiter des sites compromis ou à les forcer à télécharger. Mais le côté artisanal du simple typo-squatting est dépassé pour des méthodes plus abouties comme le montre de récentes attaques. Sur un blog, le chercheur rappelle l'affaire du groupe Carbanak qui avait réalisé le hold-up de l'année en piratant les systèmes informatiques de plusieurs banques dans différents pays et en dérobant au total près de 1 milliard de dollars. Selon Kaspersky et Fox-IT, qui ont travaillé sur cette opération, les attaquants sont entrés dans le SI par des actions ciblant les employés avec des demandes par mail de mettre à jour Java ou Adobe via des domaines de type (java-udpate.net ou adobe-update.net).

La création d'un langage malveillant pour être plus réactif

Jeremiah O'Connor a donc croisé les différents domaines trouvés dans cette attaque, mais aussi dans l'affaire Darkhotel, qui avait pour vocation de piéger les voyageurs d'affaires dans les hôtels et de rentrer dans leur ordinateur via les hotspots. « *Nous avons observé qu'ils ont tous un champ lexical similaire. Nous avons donc construit un « **langage malveillant** » au sein duquel nous intégrons les termes du trafic DNS (qui passe par la plateforme OpenDNS) en scrutant certains mots comme update, install, exe, adobe, gmail, etc. Nous appliquons ensuite une analyse par rapport aux critères définissant les domaines absolus (FQDN, Full Qualified Domain Name)* ».

Ce procédé permet d'affecter un score (ranking) aux noms de domaines et donc de blacklister plus rapidement ceux qui se voient attribuer des points négatifs. Par exemple, un domaine se revendiquant de Facebook, mais dont les adresses IP ne correspondent pas à celles du réseau social. Idem pour un site qui a été enregistré la veille avec une adresse mail temporaire.

Traditionnellement, les solutions de sécurité se basent sur des techniques comme l'analyse de réputation à travers une base de données centralisées. Mais les attaquants sont très réactifs et enregistrent très rapidement d'autres noms de domaines sosies. Ils contournent ainsi les analyses dans le cadre d'opération très ciblée et menée très rapidement. Le NLPrank devrait donner plus de réactivité aux responsables sécurité des entreprises. Encore au stade expérimental, cette méthode

a été éprouvée avec succès lors de tests pour détecter des faux positifs.

A lire aussi :

Darktrace : le Machine Learning au service de la sécurité

OpenDNS sécurise le Net avec DNSCrypt