Le phishing aussi migre vers le HTTPS, grâce à Let's Encrypt

Entre mars 2016 et mars 2017, Let's Encrypt a émis 15 270 certificats SSL contenant le terme PayPal dans le nom de domaine ou dans l'identité du certificat. Mais 14 766 d'entre eux ont été émis pour des domaines hébergeant des services de phishing, si on se fie à une analyse menée sur un échantillon par Vincent Lynch, expert en chiffrement de l'autorité de certification The SSL Store. Ce résultat tend à confirmer certaines craintes d'experts en sécurité qui, dès 2015, redoutaient de voir l'initiative Let's Encrypt, visant à offrir des certificats SSL gratuits, récupérée par les cybercriminels. Via cette autorité de certification, ces derniers peuvent déplacer leurs services de phishing, de malvertising ou d'hébergement de malwares vers des sites HTTPS, vus comme plus sûrs par les navigateurs.

En janvier 2016, l'éditeur Trend Micro mettait d'ailleurs en lumière l'existence d'une campagne de malvertising utilisant des certificats Let's Encrypt. L'analyse de Vincent Lynch tend à montrer que le phénomène aurait pris des proportions industrielles. En menant des analyses via un outil de recherche (crt.sh) de Comodo, Lynch montre que les cybercriminels, en particulier ceux animant des sites de phishing pour lesquels PayPal constitue une cible (l'objectif étant de se faire passer pour un service de confiance), ont testé les certificats Let's Encrypt dès mars 2016 avant de commencer à les déployer massivement à partir de l'automne 2016. « *Il ne semble pas qu'il y ait une cause précise à cette croissance*, écrit Vincent Lynch. *Il est possible simplement qu'il ait fallu un peu de temps pour que la pratique se répande au sein de la communauté du phishing et pour que l'expertise technique se développe.* » En tout cas, la machine est aujourd'hui bel et bien lancée, avec plus 5 000 certificats PayPal émis pour le seul mois de février 2017.

HTTPS = sécurité, une généralisation dangereuse

« *En prolongeant la tendance actuelle, Let's Encrypt va émettre 20 000 certificats 'PayPal' supplémentaires d'ici à la fin de l'année* », ajoute l'expert. Qui note que son analyse se cantonne au service de paiement, mais que le phénomène doit aussi toucher d'autres « *cibles* » comme Apple ou Google.

Certes, Lynch travaille pour une autorité de certification, qui vend des certificats et peut donc voir Let's Encrypt comme une initiative menaçant son activité. Mais son argumentation, tendant à montrer que l'approche de Let's Encrypt, consistant à tout chiffrer, ouvre la porte aux spécialistes du phishing, touche souvent juste. Et d'estimer que toutes les autres autorités de certification réunies n'émettent que moins d'un dixième du total des certificats 'PayPal' détournés par les cybercriminels. Bref, que le détournement à des fins criminelles du SSL se concentre sur Let's Encrypt. « *Depuis de nombreuses années, l'industrie de la cybersécurité explique de façon inappropriée aux utilisateurs qu'il faut associer le HTTPS et le cadenas vert (le sigle retenu par les navigateurs pour identifier un site chiffré, NDLR) avec des services sécurisés. Il s'agit d'une mauvaise généralisation, qui peut pousser les utilisateurs à penser qu'un site de phishing est un site de confiance simplement parce qu'il utilise SSL* », conclut l'expert.

A lire aussi :

50 % du trafic Web est protégé par HTTPS

Pour pousser le HTTPS, Google devient une autorité de certification racine

HTTPS : 50 % du trafic Internet est chiffré… merci Let’s Encrypt

Crédit photo : Pavel Ignatov – Schuttersock