Des pirates injectent du porno dans les tags de Google Analytics

Hacker des routeurs pour exploiter les tags de Google Analytics afin d'envoyer des publicités illégitimes, voire des images pornographiques, sur des sites web, telle est la dernière trouvaille des pirates et que la société Ara Labs Solutions met en lumière, rapportent nos confrères de *TechWeek Europe*.

Détournement d'adresse IP

Le principe est simple et bien connu parmi les méthodes de piratage : il vise à dérouter les requêtes IP des utilisateurs vers un serveur de domaines (DNS) compromis afin de contrôler leur navigation web. *« Si un attaquant contrôle le serveur DNS que vous utilisez pour vos connections IP, il peut substituer l'adresse IP légitime par celle d'un serveur sous son contrôle »*, explique le chercheur Sergei Frankoff sur le blog de l'entreprise. Une méthode qui, combinée à des techniques de phishing, vise à envoyer les utilisateurs vers de faux sites web, comme ceux des organismes bancaires par exemple, afin de récupérer des identifiants de connexion et des informations confidentielles.

Dans le cas présent, les cybercriminels exploitent cette méthode pour substituer les tags de Google Analytics par des contenus illégitimes, en injectant leur propre code en retour d'une requête détournée. Les tags « Analytics » sont des petits scripts fournis gratuitement par Google pour permettre aux webmasters de mesurer le trafic en les insérant sur les pages de leurs sites web. Autant dire que leur usage massif, promesse d'une audience toute aussi importante, en fait une cible de choix pour les pirates du web.

Le piratage de routeur, un exercice facile

D'autant que le piratage de routeurs s'avère un exercice facile. Pour y parvenir, les attaquants exploitent notamment les failles de sécurité propres au *firmware* de l'équipement réseau qui n'est pas toujours mis à jour par ses utilisateurs (si tant est que le constructeur fournisse encore le support pour les produits vieillissants), ou encore en parvenant à déchiffrer des mots de passe trop faibles (si tant est que le code livré par défaut ait été changé depuis l'installation de l'appareil).

En décembre dernier, études à l'appui, l'éditeur de sécurité Avast rapportait que le mot de passe administrateur installé sur les routeurs résidentiels et TPE était *« trop faible dans 80 % des cas »*. Une aubaine pour les cybercriminels. Tout récemment, le chercheur en sécurité Kyle Lovett a levé le voile sur une faille de sécurité qui affectent 700 000 routeurs fournis par des FAI à leurs abonnés dans le monde.

Pour prévenir, ou éliminer, les éventuels piratages de routeur, le plus simple est d'en changer les identifiants de connexion après avoir effectué la mise à jour du micrologiciel pour en combler les éventuelles vulnérabilités.

Lire également
D-Link s’apprête à fermer la backdoor de ses routeurs
Piratage WiFi dans les hôtels, la France mal préparée ?
Piratage : pourquoi vous êtes concerné

crédit photo @ GlebStock – Shutterstock