L'Instagram de Britney Spears, une planque pour les hackers russes

Vivons heureux, vivons cachés ! Cet adage s'applique parfaitement aux cybercriminels. Encore faut-il trouver la bonne planque ! Des chercheurs d'Eset, éditeur de sécurité, viennent de détecter une des cachettes d'un groupe de pirates russes, Turla. Ce dernier œuvre depuis 2007 et est à l'origine dun rootkit sophistiqué Uburos, créé en 2014. Spécialisé dans le cyberespionnage, Turla est soupçonné d'être d'origine russe ou pour le moins russophone. Ses techniques de piratage sont très élaborées, mais la découverte d'Eset est particulièrement originale.

Les chercheurs ont en effet déniché une backdoor dans les commentaires publiés sur le compte officiel de Britney Spears sur Instagram. Ce trojan donne des informations de localisation des serveurs de commandes et contrôle du groupe Turla.

Une backdoor maquillée en extension Firefox

Dans le détail, cette porte dérobée est maquillée en extension pour Firefox. Sa diffusion s'est déroulée via un site suisse compromis. Les visiteurs ont été invités à télécharger l'extension nommée HMTL 5 encoding. La backdoor basée sur JavaScript donne des indications sur les activités des utilisateurs.

Elle ressemble à une extension similaire pour Firefox découverte par BitDefender en juillet 2016 et provenant d'un groupe de pirates nommé Pacifier APT. En croisant les résultats de BitDefender, Eset a trouvé que les deux extensions téléchargeaient la backdoor Skipper, un malware attribué au groupe Turla. Les deux groupes pourraient donc avoir des liens ou être une même entité.

Un commentaire diablement chiffré

Pour le compte Instagram de Britney Spears, l'extension de Firefox génère un lien court bit.ly pour atteindre le serveur C&C, mais cette URL ne pointe sur rien. Le bon chemin se cache dans les commentaires publiés sur une photo spécifique sur Instagram. Dans le cas présent, il s'agit d'un commentaire sur une photo du compte de la chanteuse américaine. L'extension de Firefox va examiner les commentaires de chaque photo et va appliquer une valeur de chiffrement (hashage) personnalisé. Dans la photo, il y a un seul commentaire correspondant à cette valeur de hash en l'occurrence 183.

En transformant ce commentaire, les chercheurs ont trouvé une phrase pour obtenir une piste sur l'url courte : (?:\\u200d(?:#|@)(\\w). Au sein de cette phrase, \\200d correspond à une séquence de séparation entre les émojis. En l'intégrant dans le commentaire, les spécialistes ont découvert l'adresse http://bit.ly/2kdhuHX , qui pointe sur l'URL complète static.travelclothes.org/dolR_1ert.php. Cette adresse a été utilisée dans le passé par le groupe Turla.

A lire aussi :

Les pirates de Turla jouent à cache-cache grâce aux satellites

Opération Epic Turla : les services européens de renseignement espionnés