APT28 exploite EternalBlue pour pirater le WiFi des hôtels

La faille EternalBlue, publiée par les Shadow Brokers, n'en finit pas de faire parler d'elle. WannaCry et Notpetya s'en sont servis pour mener de vastes opérations de ransomware et de sabotage. Selon FireEye, le groupe APT28 (ou Fancy Bear), connu pour être derrière de multiples opérations de cyber-espionnage (dont la déstabilisation électorale aux Etats-Unis), a utilisé récemment la vulnérabilité EternalBlue pour pirater le WiFi des hôtels.

Dans son rapport, le spécialiste de la sécurité indique que tout démarre par une campagne de phishing ciblé à différents hôtels, 7 sont situés en Europe et 1 au Moyen-Orient. Aucun nom n'a été divulgué. Le courriel comprend une pièce jointe nommé « Hotel_Reservation_From.doc », masquant le malware GameFish. Ce dernier est selon les chercheurs de FireEye une des signatures du groupe APT28.

EternalBlue pour se propager dans les réseaux

Une fois installée, GameFish se sert de la faille EternalBlue (visant le protocole SMB) pour se propager à travers le réseau et trouver les ordinateurs contrôlant le WiFi interne et celui à disposition des clients. Le malware installe ensuite un outil Open Source Responder, capable de voler les données d'authentification circulant sur le réseau sans fil. L'exploit a été réellement utilisé pour dérober des données clients.

Cette attaque rappelle une offensive similaire menée en 2014 sous le nom Dark Hotel. Elle avait pour but de dérober des informations sensibles aux cadres supérieurs, pendant leurs voyages d'affaires, via les bornes d'accès WiFi mis à disposition des clients dans les hôtels de luxe. Les pirates exploitant des failles logicielles à travers les réseaux WiFi « privés et sécurisées » de ce type d'établissements haut de gamme. Pour FireEye, les récentes attaques via EternalBlue ne sont pas à mettre au crédit du groupe derrière Dark Hotel, mais bien d'APT28.

A lire aussi :

Ransomware : les cybercriminels font maintenant la tournée des hôtels

Darkhotel récupère une faille chez Hacking Team

Crédit Photo : Diego Cervo