Switcher, le malware Android qui s'attaque aux réseaux Wifi

Switcher est un nouveau malware Android qui se sert du smartphone infecté pour… attaquer les réseaux sans fil auxquels se connecte l'utilisateur. Découvert par Kaspersky Lab, l'agent malveillant s'attaque plus précisément aux routeurs Wifi pour en détourner le trafic web.

Baptisé Trojan.AndroidOS.Switcher, la bestiole remplace les adresses des serveurs DNS dans les paramètres du routeur par celles des serveurs des cybercriminels. Ce faisant, ils leur est alors facile de détourner les requêtes des adresses alphanumériques vers des faux sites web afin, par exemple, de récupérer des identifiants et mots de passe de connexion à des services bancaires, administratifs, de messagerie, etc. Une technique de piratage dénommée DNS-hijacking.

Pénétration par force brute

L'attaque du routeur Wifi est, pour sa part, réalisée par force brute. Une fois trouvé l'identifiant du point de connexion Wifi (le BSSID), le trojan informe un serveur de commande & contrôle (C&C) qu'il est fonctionnel. Switcher tente ensuite d'obtenir le nom du fournisseur d'accès afin de déterminer quel serveur sera utilisé pour lancer l'attaque par DNS-hijacking. Il en existe trois à ce jour : 101.200.147.153, 112.33.13.11 et 120.76.249.59. Le premier est utilisé par défaut et les deux autres réservés à des fournisseurs d'accès spécifiques, explique le chercheur de Kaspesky Nikita Buchka, sans entrer dans les détails. Ensuite, l'attaque par force brute est lancée en essayant une succession de combinaisons de type admin:00000000, admin:admin, admin:123456, etc. Autrement dit, les administrateurs qui ont pris la peine de changer les identifiants de connexion par défauts de leurs routeurs ont peu de craintes d'être affectés par Switcher.

Si néanmoins le malware parvient à passer l'écran de connexion du routeur, il se rend dans les paramètres réseau de l'interface et change le DNS principal par celui pointant vers un serveur de résolution d'adresses infectieux. Le DNS secondaire pointe vers celui de Google (8.8.8.8) dans le but de continuer à rediriger les requêtes en cas de défection du DNS primaire, afin de ne pas éveiller les soupçons de l'utilisateur. *« Le code qui exécute ces actions est un bordel sans nom, car il a été conçu pour fonctionner sur une large gamme de routeurs et fonctionne en mode asynchrone »*, note le chercheur. Mais il n'en reste pas moins efficace. A l'heure où le chercheur publiait sa note, le 28 décembre, Switcher avait infecté 1 280 réseaux Wifi. Essentiellement des routeurs situés en Chine.

Fausses applications

Quand au *modus operandi* utilisé pour infecter un smartphone sous Android, il est tristement banal dans la mesure où c'est l'utilisateur lui-même qui l'installe. Switcher se cache en effet derrière de fausses applications qui circulent probablement sur les stores alternatifs à Android Play. Kaspersky Lab en dénombre deux à ce jour : com.baidu.com, une soi-disant version mobile du moteur de recherche chinois Baidu; et une version détournée de wifilocating, une application chinoise populaire pour partager des informations de connexion sur les réseaux Wifi d'accès publics. Pour

l’heure, le malware semble se concentrer sur les utilisateurs chinois. Mais rien ne dit qu’il n’élargira pas ses ambitions géographiques prochainement.

Lire également
Des routeurs WiFi Netgear à la portée des pirates
Le malware Gooligan terrorise des millions de terminaux Android
Un nouveau malware téléchargé toutes les 4 secondes