Découverte Lookout : eSurvAgent

Lookout recherche et découvre en permanence de nouvelles menaces pour protéger et conseiller nos clients

Contexte et chronologie de la découverte

Début 2018, Lookout a enquêté sur eSurvAgent, un agent sophistiqué de surveillanceware sous Android ayant des liens avec une société italienne nommée eSurv, anciennement connue sous le nom de Connexxa. Cet agent, aussi appelé Exodus, semble être en développement depuis au moins cinq ans et se divise en plusieurs étapes : l'injection du surveillanceware dans un premier temps, puis le téléchargement d'une charge active importante dans un second temps et l'obtention d'un accès root à l'appareil dans un troisième temps. Les chercheurs de Lookout ont récemment découvert un composant de la même menace sous iOS, que les utilisateurs ont téléchargé sur des sites de phishing se faisant passer pour des sites d'assistance client. De plus, en utilisant frauduleusement le système de provisioning des applications d'entreprise d'Apple, les applications eSurv étaient signées avec des certificats Apple légitimes.

Informations clés

1. Semble avoir été créé pour le marché de l'interception légale
2. Utilise frauduleusement le système de provisioning des applications d'entreprise d'Apple
3. Sa fonctionnalité est contrôlée via des charges utiles accompagnées de notifications Push pour qu'un attaquant puisse spécifier les données à extraire

Fonctionnalités et parties concernées

La variante disponible sous iOS contenait un sous-ensemble de fonctionnalités des versions Android, mais ne disposait pas de fonctionnalités complètes pour compromettre le terminal. Cependant, cette version exploitait le processus de certification d'Apple pour paraître légitime et se déployer sur les appareils iOS pour exfiltrer les types de données suivantes :

Contacts | Photos | Localisation GPS | Enregistrements audio | Vidéos | Informations concernant l'appareil

Le logiciel a été découvert sur des sites de phishing se faisant passer pour des opérateurs mobiles italiens et turkmènes, ainsi que dans le Play Store italien. Depuis, il a été retiré du Play Store officiel et Apple a révoqué les certificats concernés.

Comment Lookout détecte des menaces du type eSurvAgent et protège vos appareils

Les équipes Lookout Security Intelligence recherchent et découvrent en permanence de nouvelles menaces pour protéger et conseiller nos clients en associant une analyse statique et dynamique à notre moteur de machine learning. Nous avons classé eSurvAgent dans la catégorie des surveillancewares dès qu'il a commencé à utiliser un chiffrement avancé, pour obfusquer le trafic à destination des serveurs de C&C, créer des GUID unique pour chaque appareil et accéder à certains chemins d'accès inadaptés. Depuis mars 2018, les appareils sur lesquels Lookout a été installé détectent et alertent de la présence de l'agent eSurvAgent. Lookout fournit également une protection contre les autres surveillancewares sophistiqués qui pourraient passer inaperçus.

Service Lookout Threat Advisory

Dans le monde en constante évolution de la sécurité mobile, être à l'affût de la moindre menace n'est pas de tout repos. Lookout Threat Advisory s'appuie sur l'immense ensemble de données provenant du réseau mondial de capteurs de Lookout, composé de millions d'appareils, qu'il associe à des informations que lui fournissent ses chercheurs chevronnés en sécurité pour vous donner des renseignements exploitables sur les dernières menaces et risques mobiles.