Découverte Lookout : Monokle

Lookout découvre en permanence de nouvelles menaces pour protéger nos clients des attaques mobiles

Contexte et chronologie de la découverte

En 2018, Lookout a trouvé la première version de Monokle et a depuis réalisé des recherches approfondies sur ce surveillanceware Android. Après avoir fait de plus amples recherches, l'équipe de Lookout s'est aperçue que ce surveillanceware partageait un signataire avec un antivirus Android nommé Defender, développé par une entreprise russe du nom de STC (Special Technology Center). STC est l'une des trois entreprises russes que l'administration Obama a sanctionnées après qu'elles aient été suspectées de fournir un soutien matériel au GRU, service du renseignement militaire russe, pour interférer dans les élections présidentielles américaines de 2016.

СПЕЦИАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР

Informations clés

1. Surveillanceware avancé développé par STC, société sanctionnée par le gouvernement américain
2. Dispose d'une fonctionnalité Cheval de Troie d'accès à distance (RAT). Utilise des techniques avancées d'exfiltration de données et peut installer des certificats
3. A l'apparence d'une application légitime afin de masquer ses intentions malveillantes

Fonctionnalités et parties concernées

Monokle apparaît dans un nombre limité d'applications, indiquant que les attaques exploitant le surveillanceware ciblent des personnes très précises. Étant donné la légitimité apparente de ces applications, bien qu'elles contiennent un cheval de Troie, l'utilisateur final ignore complètement qu'il est la cible d'une attaque. Nous connaissons bien le mode opératoire de ces applications contenant un cheval de Troie, mais Monokle utilise une fonctionnalité tout à fait inédite pour les chercheurs de Lookout.

Ici, la fonctionnalité Cheval de Troie d'accès à distance (RAT pour « Remote Access Trojan ») de Monokle utilise des techniques d'exfiltration de données avancées et peut installer un certificat spécifiant une attaque dans la liste des certificats de confiance sur un appareil infecté, préalablement au lancement d'une attaque du type man-in-the-middle. Elle permet aussi d'exfiltrer en un clin d'œil les données d'applications tierces, sans devoir accéder à la racine d'un appareil. Elle peut utiliser des dictionnaires à saisie intuitive pour déterminer les centres d'intérêt de la cible et mieux préparer des attaques. Elle peut également enregistrer l'écran d'un appareil lors de son déverrouillage et exfiltrer son code de déverrouillage.

Comment Lookout détecte Monokle et protège vos appareils

Pour prévenir toute attaque de Monokle, les clients de Lookout peuvent créer des politiques basées sur les applications dans la plateforme Lookout. Elles vont les alerter lorsque des applications contiennent un cheval de Troie et leur permettre ensuite de créer des stratégies de réponse adaptées. Les appareils sur lesquels Lookout a été installé sont protégés contre Monokle depuis début 2018. Lookout va poursuivre ses recherches sur ce surveillanceware et tenir informé le marché de ses découvertes, car il a été prouvé que Monokle fait l'objet d'un développement permanent sur Android et qu'il s'étend même aux appareils iOS.

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.