Le malware YiSpecter frappe les iPhone non dévérouillés

Jusqu'à présent, les malwares visant iOS s'appuyaient sur des terminaux déverrouillés (*jailbroken*), afin d'exploiter les droits administrateurs qui en découlent, pour s'attaquer aux contenus et fonctions de l'appareil. Mais Palo Alto Networks déclare avoir découvert YiSpecter, un malware capable de s'en prendre à tous les iPhone, déverrouillés ou non.

« Plus précisément, c'est le premier malware que nous avons vu en circulation qui abuse les API privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes », indique la firme de sécurité. Une fois installé, YiSpecter peut télécharger, installer et lancer arbitrairement des applications, remplacer celles du terminal affecté, détourner d'autres applications pour afficher sauvagement de la publicité, changer le moteur de recherche par défaut de Safari, mettre en favori des pages du navigateur et les ouvrir et, cerise sur le gâteau, envoyer des informations sur le terminal à un serveur de contrôle distant. Un catalogue de cauchemars.

YiSpecter confiné à la Chine et Taïwan

Pour le moment, YiSpecter affecte principalement les utilisateurs en Chine et à Taïwan. Il se répand de manière inédite, notamment à partir du détournement de trafic des opérateurs nationaux. Mais aussi par l'intermédiaire d'un ver Windows qui se propage sur les sites de réseaux sociaux ou encore par l'installation hors ligne d'une application. La bestiole n'est pas nouvelle et ses premières discussions à son sujet dans les réseaux sociaux remontent à plus 10 mois. Apple a été alerté du problème et sur les 57 éditeurs d'antivirus du service de détection Virus Total, un seul est capable de le détecter, souligne Palo Alto.

Il faut dire que les auteurs de YiSPecter ont particulièrement soigné leur travail. Le malware se compose de quatre composants signés de certificats d'entreprise. En trompant les API privées, ces composant se téléchargent et s'installent à partir d'un serveur de Command and Control (C2). Trois d'entre eux rusent en cachant leur icones sur l'écran d'accueil (SpringBoard) de l'iPhone se rendant ainsi visuellement indétectable par l'utilisateur qui aura d'autant plus de mal à les supprimer donc. Et ceux qui s'y essayent ne peuvent que constater le retour de l'application malveillante. *« Les composants utilisent aussi le même nom et les logos d'applications du système de tromper les utilisateurs »*, ajoute le fournisseur de services de sécurité.

Un argument sécuritaire en moins face à Android

YiSpecter n'est pas le premier malware à tenter de s'attaquer aux iPhone non modifiés. WireLurker avait démontré ses capacités à s'en prendre à des terminaux non-jailbreakés, notamment en exploitant des certificats signés d'entreprises. Et les discussions sur l'utilisation des API privées pour implanter des fonctionnalités sensibles dans iOS reviennent régulièrement dans les cercles de recherches en sécurité. Mais YiSpecter est le premier agent malveillant à exploiter ces deux techniques d'attaque. *« Il repousse un peu plus loin la ligne de sécurité d'iOS »*, prévient Palo Alto.

Mais au-delà de YiSpecter, plus de cent applications de l'App Store ont abusé les API privées et contourné l'examen rigoureux du code par Apple, rappelle Palo Alto. En conséquence, la technique visant à tromper les API du système peut être utilisée séparément pour affecter les utilisateurs qui n'ont pas modifié leur téléphone et n'installent que des applications trouvées sur l'App Store et supposément légitimes. En d'autres termes, Apple peut aujourd'hui difficilement arguer de la fiabilité plus grande de sa plate-forme face à celle de son concurrent Android grâce à son environnement fermé. Un argument qui peut notamment faire mouche pour gagner du terrain sur le marché de l'entreprise. Palo Alto a bien suggéré à Apple de renforcer les mécanismes de sécurisation d'iOS et de revoir la procédure de validation de code. Sans succès à ce jour, visiblement.

Eradiquer YiSpecter


For iOS users that are potentially infected by YiSpecter, we suggest removing it with the following steps:

1. In iOS, go to Settings -> General -> Profiles to remove all unknown or untrusted profiles;
2. If there's any installed apps named "情涩捕放器", "快播私密版" or "快播0", delete them;
3. Use any third-party iOS management tool (e.g., iFunBox, though note that Apple's iTunes doesn't work in this step) on Windows or Mac OS X, to connect with your iPhone or iPad;
4. In the management tool, check all installed iOS apps; if there're some apps have name like Phone, Weather, Game Center, Passbook, Notes, or Cydia, delete them. (Note that this step won't affect original system apps but just delete faked malware.)

La firme de sécurité, qui proposer de filtrer le trafic du serveur C2 de YiSpecter, fournit un mode d'emploi pour éradiquer le malware (voir capture ci-contre): globalement il faut supprimer tous les profils inconnus ou suspicieux; effacer les applications nommées en chinois; et éradiquer toutes les applications qui utilisent des noms génériques comme Phone, Weather, Game Center, Passbook, Notes, ou Cydia à partir d'un gestionnaire d'applications tiers depuis un PC ou un Mac.

Lire également

Le malware XcodeGhost gangrène l'App Store d'Apple

Le nombre de smartphones Android infecté s'affiche à la baisse