Un nouveau logiciel malveillant cible les iPhone | Le Net Expert Informatique

	Un nouveau logiciel malveillant cible les iPhone

Décidément, les terminaux à la pomme intéressent de plus en plus les pirates. Après la découverte le 4 février par les experts du cabinet de sécurité informatique Trend Micro du premier logiciel espion baptisé « XAgent » exploitant des failles sur les téléphones Apple non débridés (dits « non jailbreakés »), c'est au tour de l'unité de recherche 42 de l'entreprise de sécurité informatique Palo Alto Networks de publier dimanche 4 octobre une alerte sur un nouveau logiciel malveillant (malware) affectant les iPhones du commerce.

Baptisé « YiSpecter », il attaque sans distinction les iPhone du commerce vendus avec le système d'exploitation officiel iOS d'Apple et ceux qui ont été débridés. Apple, qui a reconnu l'existence de ce malware, a indiqué lundi 5 octobre que les utilisateurs d'iOS 8.4 et d'iOS 9 étaient désormais protégés. La particularité de ce programme – qui serait actif depuis plus de 10 mois à Taïwan et en Chine continentale d'où il proviendrait – est d'utiliser des failles que l'on pensait impossible à exploiter, et de se propager de façon inédite, selon Palo Alto Networks.

Un fonctionnement et une propagation inédits

Détournant certaines interfaces de programmation propres au système d'exploitation iOS, cette nouvelle forme de logiciel malveillant ne laisse rien présager de bon pour l'avenir des terminaux mobiles à la pomme selon la firme de sécurité à l'origine de la découverte : « C'est le premier malware que nous avons vu en circulation qui abuse les API [interfaces de programmation] privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes. »

En se propageant seul soit grâce à « Lingdun », un ver informatique sous Windows (qui se charge d'envoyer des liens malicieux de téléchargement d'YiSpecter à tous ses contacts), soit par le piratage des connexions WiFi des boîtiers des fournisseurs d'accès à Internet, cette nouvelle variante de malware inquiète la société californienne. Ses quatre composants, tous authentifiés par des certificats d'entreprises réels émanant de sociétés comme Verisign ou Symantec, s'installent de façon furtive sur les iPhone, en masquant ses programmes, mais aussi en dupliquant les noms et les logos des icônes système (Game Center, Météo, Notes, PassBook, Téléphone, etc.), piégeant même les utilisateurs les plus avertis.

Une fois installé, YiSpecter peut télécharger, installer et lancer des applications de l'App Store, mais aussi les modifier, par l'affichage de publicités en plein écran par exemple. Il permet également de collecter les données des utilisateurs, notamment celles utilisées dans le navigateur Internet Safari. S'il est découvert, sa suppression par méthode classique ne fonctionnera pas car il se réinstalle automatiquement après un redémarrage système. Enfin, peu d'espoir du côté des antivirus, qui ne détectent toujours pas sa présence sur les terminaux infectés.

Des malwares aux origines peu claires

Certains indices repérés par Palo Alto Networks font converger les soupçons vers « YingMob », une entreprise chinoise de publicité mobile ayant pignon sur rue, qui aurait programmé et diffusé ce malware à des fins publicitaires, n'hésitant pas à en faire sa promotion au grand jour. Mais la complexité et les méthodes de propagation de YiSpecter cachent peut-être des visées plus opaques.

Déjà le mois dernier, 344 applications iOS officielles présentes dans l'App Store, la boutique d'applications d'Apple, avaient été retirées en urgence car infectées par le malware « XcodeGhost », découvert le mercredi 16 septembre par les équipes sécurité du groupe chinois Alibaba. L'origine de ce malware est encore incertaine, mais les méthodes utilisées sont très similaires aux techniques de programmation qu'emploie la CIA – selon des documents publiés en mars par The Intercept.

Tout début septembre, c'était le logiciel malveillant « KeyRaider » également découvert par la société Palo Alto Networks, qui faisait parler de lui : selon la société de sécurité, plus de 225 000 comptes et identifiants Apple auraient été dérobés, uniquement sur des iPhone et iPad débridés.

La société de sécurité américaine est également à l'origine de la chute d'un mythe : c'est elle qui annonçait il y a moins d'un an, en novembre 2014, la découverte, toujours en Chine, de « Wirelurker », le tout premier malware pour iPhone touchant des téléphones non débridés. Depuis, il ne se passe pas un mois sans qu'une nouvelle alerte concernant les terminaux mobiles d'Apple ne soit lancée.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lemonde.fr/pixels/article/2015/10/07/un-nouveau-logiciel-malveillant-cible-les-iphone_4784509_4408996.html