Des applications malveillantes dans l’App Store | Le Net Expert Informatique

Des pirates ont trouvé le moyen de faire entrer des applications malveillantes dans la boutiques d'Apple. Ils ont pour cela convaincu des développeurs d'utiliser une version modifiée de Xcode, introduisant ainsi des malwares sur l'App Store.

Pour minimiser les risques d'infection des terminaux mobiles, les éditeurs de plateformes recommandent (ou imposent) l'utilisation de leurs boutiques d'applications officielles. Il est malgré tout possible d'éviter les mécanismes de contrôle mis en place par exemple par Google et Apple.

Et Apple vient d'ailleurs d'en faire les frais. La firme a confirmé officiellement à Reuters avoir dû retirer plusieurs apps de l'App Store suite à la découverte d'une faille de sécurité. Des pirates ont trouvé une solution pour échapper à la vigilance de l'éditeur.

Xcode corrompu pour pénétrer l'App Store

Pour concevoir des applications pour iOS et OS X, les développeurs ont recours aux outils de développement d'Apple regroupés au sein du logiciel Xcode. Les pirates ont ainsi mis au point une version modifiée de Xcode, diffusée ensuite auprès de développeurs d'apps. Les applis réutilisant cet outil se transformaient dès lors en malwares.

Présenté sous la dénomination XcodeGhost, ce malware a pu faire son entrée sur l'App Store. Plusieurs applications populaires ont été compromises par cette méthode dont la messagerie WeChat, CamCard ou le concurrent chinois d'Uber, Didi Chuxing.

WeChat a précisé dans un billet de blog que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

« Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps » déclare un porte-parole d'Apple auprès de Reuters. Le malware XcodeGhost est présenté par la société de sécurité Palo Alto Networks comme particulièrement nuisible et dangereux.

L'éditeur de sécurité précise également que la version compromise de Xcode a été identifiée sur un serveur en Chine. Et si elle a été utilisée par les développeurs, c'est probablement car elle s'avérait plus rapide à télécharger que le logiciel officiel hébergé chez Apple.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

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.zdnet.fr/actualites/apple-contraint-de-supprimer-des-apps-malveillantes-de-l-app-store-39825174.htm