

TechNews

科技新報

《財訊雙週刊》一年26期 週年慶降價 最後倒數 **1,980元**

XcodeGhost 不僅 iOS 有麻煩，Android 也同時身陷其中

作者 愛范兒 | 發布日期 2015 年 09 月 23 日 | 分類 [Android](#) , [iOS](#) , [資訊安全](#)



在中國 XcodeGhost 病毒爆發攻破 iOS 安全壁壘的時候，其實還是有不少 Android 用戶是在看笑話的。但是事實告訴我們，Android 平台的安全性也非常堪憂，過往的例子已經說得夠多了。但是在 XcodeGhost 這件事的後續發酵上，Android 手機也未能逃脫投毒者的魔爪。

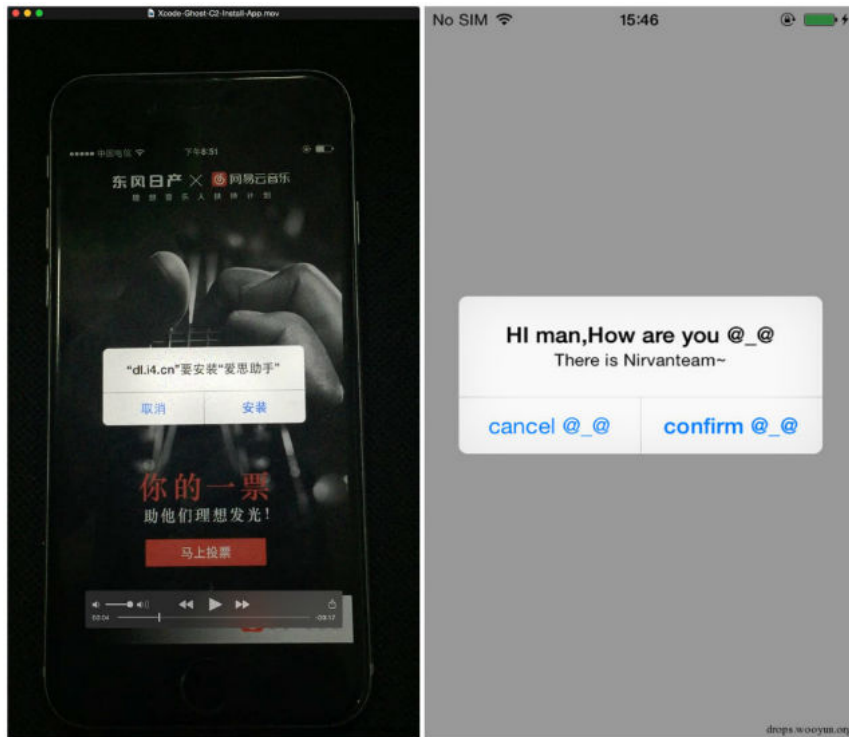
私人技术专家为您的 Mac 保驾护航



在談 Android 的事情前，我們還是來回顧一下 XcodeGhost 在 iOS 上發展到何種程度：

- 進展一：疑似投毒者在社群網路現身，表示這次惡意篡改 Xcode 只是一場實驗，沒有進行惡意活動。但是根據後續發展，還有眾多網路安全從業者分析，這個聲明不可信。
- 進展二：根據 21 日傍晚盤古團隊的資料，他們的雲端被感染列表庫中已經有 4,389 條記錄，其中某些應用程式有多個版本被感染，覆蓋 3,418 個不同的應用程式。他們並推斷，App Store 中被感染的應用程式遠大於這個數字。

- 進展三：360 涅槃團隊日前還原了惡意 iOS 應用程式與 C2 伺服器的通訊協議，從而可以實際測試受感染的 iOS 應用程式可以有哪些惡意行為，主要包括「做應用程式推廣、偽造內購頁面，透過遠端控制在用戶手機上彈出提示」三種。



▲ 安全團隊用後門模擬可能的惡意行為。

並且綠盟科技還表示，這些後門的存在還可以發起更為惡劣的行為，比如發起 DDoS 攻擊。

同時，在這份 9 月 20 日的報告中，綠盟科技還提到了 Android 的類似的安全隱憂：

“

Android 平台對於審核 App 更為糟糕，Google 是完全被封閉的，中國的開發者完全只能從非官方管道下載，且其 App 市場更為混亂，一旦發生安全事件，影響更為惡劣。

果不其然，22 日，阿里巴巴行動安全發布報告：

“

雖然 XcodeGhost 作者的伺服器關閉了，但是受感染的 App 的行為還在，這些 App 依然持續向伺服器（比如 init.icloud-analysis.com、init.icloud-diagnostics.com 等）發送請求。這時候駭客只要使用 DNS 劫持或者污染技術，聲稱自己的伺服器就是「init.icloud-analysis.com」，就可以成功的控制這些受感染的 App。

在 360 涅槃團隊總結的可能的攻擊行為之外，阿里巴巴行動安全經過測試發現，XcodeGhost 的存在還可以下載企業證書簽名的 App，定向在用戶端彈出（詐騙）消息、推送釣魚頁面等，危害使用者安全。

Unity 也有同樣的安全問題

另外，百度安全實驗室還披露另一個令人震驚的消息：

在大家以為一切都完結的時候，百度安全實驗室稱已經確認「Unity-4.X 的感染樣本」，邏輯行為和 XcodeGhost 一致，只是上線功能變數名稱變成了 init.icloud-diagnostics.com。這意味，凡是用過被感染的 Unity 的 App，都有竊取隱私和推送廣告等惡意行為。

Unity 是由 Unity Technologies 開發的一個讓玩家創建諸如三維影像遊戲、即時三維動畫等類型互動內容的多平台綜合型遊戲開發


工具，很多有名的手機遊戲比如《Temple Run》、《紀念碑谷》、《爐石戰記：魔獸英雄傳》都是用 Unity 進行開發的，包括 Android 版。Unity 4.6.4 – Unity 5.1.1 各個版本都有可能被篡改。而且在這個消息被曝出後，之前疑似 XcodeGhost 投毒者、網名為 coderFun 的人半夜開始刪除之前散播的被感染的 Unity 貼文，這極有可能意味著，製作被感染的 Xcode 和 Unity 是同一個人或團隊。

隨著 Unity 感染被確定，是時候發出對 Android 系統的安全預警了，這件事情持續發酵，而且中國 Android 系統版本演化更複雜，應用商店割據更嚴重，預計 Android 系統手機面臨的安全問題更為瑣碎、更難以解決。

(本文由 [愛范兒](#) 授權轉載；首圖來源：[Flickr/Perspecsys Photos](#) CC BY 2.0)

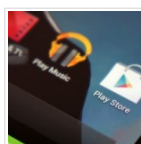
延伸閱讀：

- [蘋果官方確認 XcodeGhost 感染部分應用程式：已著手刪除](#)
- [iOS App 安全危機，XcodeGhost 木馬入侵多款中國軟體](#)

 38 如果你喜歡我們的分享和文章，請幫我們按個讚

 分享到 Facebook

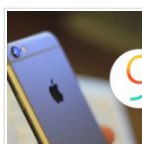
你可能有興趣的文章：



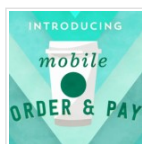
Google Play 遭攻擊，安全機制被繞過



Uitox 結盟 91App，台灣電商生態圈更進化？



XcodeGhost 事件後續：蘋果將 Xcode 工具下載移一份到中國網內



免開口也免排隊！星巴克 App 點餐服務全美上線



電子支付大戰開打！通訊軟體「忠誠客戶」成優勢



蘋果官方確認 XcodeGhost 感染部分應用程式：已著手刪除



按讚  看科技新報 | TechNews

 分享 304,778 人說這讚。成為你朋友中第一個說讚的人。

關於作者

相關文章



愛范兒

愛范兒：Beats of bits //發現創新價值的科技媒體，MobileMonday 廣州授權組織者

關鍵字: [Android](#) , [app](#) , [iOS](#) , [XcodeGhost](#)

讀者留言

0則回應

排序依據  熱門



新增回應……

 Facebook Comments Plugin

