網路與系統安全期中報告

資財三乙 108AB0721 胡欣慧

在分析案例前我們先來認識一下什麼是Xcode,Xcode是一個由蘋果公司所開發設計的Mac OS及iOS應用程式整合開發環境(IDE)。身為開發iPhone應用程式時會使用到的整合開發環境，因此本身提供了開發人員圖形化介面的文字編輯器(texteditor)以及所需的編譯器(compiler)，此外也包含了除錯器(debugger)及方便開發者的自動生成工具，最後更提供了各式樣板(template)來協助建立應用程式。

案例分析：XCSSET木馬程式於Xcode專案入侵Mac電腦。

一、它的攻擊途徑很特殊，惡意程式碼是不知如何被注入本機Xcode專案，但因為這些Xcode專案已被修改，因此從一開始便執行惡意程式碼，結果就是在執行的系統上植入木馬程式XCSSET。

二、XCSSET進入Mac系統後，會開採蘋果軟體的零時差漏洞。它會先使用Data Vaults的漏洞來讀取或倒出cookies，或是利用Safari開發版本漏洞，以便發動通用跨站指令碼（Universal Cross-site Scripting，UXSS）攻擊注入JavaScript後門到網站上。理論上，UXSS攻擊可以透過JavaScript任意程式碼修改幾乎所有瀏覽器設定，包括顯示的網站、取代比特幣電子錢包網址、偷取Apple ID、Google、Paypal、Yandex密碼，Apple Store信用卡資訊、封鎖用戶修改密碼、竊取特定網站的螢幕擷圖。

趨勢科技指出，這相當嚴重，因為他們發現到有些開發人員已將問題Xcode專案經由GitHub分享其專案，對仰賴GitHub的開發人員可能導致類似供應鏈攻擊的風險。他們也在VirusTotal上發現這個惡意程式。

A.12 APPLE XCODE: INTEGRATED DEVELOPMENT ENVIRONMENT

Apple Xcode is a development environment used to develop OSX and iOS applications[91]. In March 2021, researchers reported that an individual malicious Xcode project was being used to infect Xcode developers with a backdoor[92]. The malicious Xcode project was a copy of a real one. The malicious Xcode project infected the user by exploiting a weakness in Xcode that allowed attackers to automatically run a script when the project build was launched[92].

There is no attribution to this attack and it is not clear whether customers where ever attacked[93]. It is also not clear how the trojanized Xcode project was delivered to the potential victims, or if it ever was.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Unknown	Code	Malware Infection	Unknown