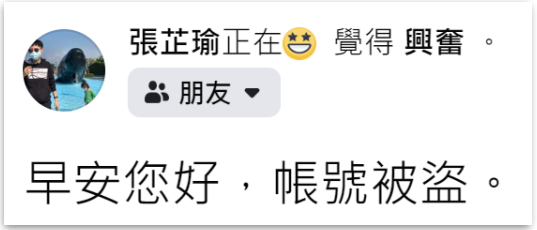
HACK INTO YOUR FACEBOOK

摩茲達 酷 cool いいね
111550090 劉思予 111950031 陳妍沂
111550131 張芷瑜 111550168 陳奕

TABLE OF CONTENTS

Abstract



Motivation

- Chrome extension 是我們常用的工具，但它真的安全嗎？
- 會不會在不經意的情況下，我們的個資早已被駭客駭光了呢？

What we do

- 實作惡意 Chrome Extension 取得別人 Cookies
- Email 傳送取得的 Cookies 資訊給自己
- 登入他的Facebook！
- （幫他發文向長輩問好）

Introduction

Chrome extension

- 擴展 Google Chrome 瀏覽器功能的小型程式，允許用戶自訂和增強瀏覽器體驗。
- 可以添加新功能、甚至與網頁內容互動
- 例：廣告攔截、密碼管理。

cookie

- 小型文字檔案，用於儲存用戶相關信息
- Cookie 由網頁伺服器送到瀏覽器並儲存在用戶的電腦
- 提高用戶體驗
- 例：session state (登錄狀態) 、user preference

Secession key

- 由server生成的唯一識別碼，用來在網頁app中維持用戶登入狀態。
- 通常儲存在 Cookie 中，讓server能識別用戶身份，避免每次請求都需要重新驗證。
- 例：Facebook

System Architecture

Chrome extension

在使用者點擊擴充視窗的觸發按鈕後，獲取使用者Facebook的cookies，並將該值傳到後端伺服器

Server

將收集的cookie values透過第三方信箱寄回給攻擊者

Hack.py

將cookies添加到一個尚未登入的FB網站頁面，執行後重整會直接登入

Live Demo

How to Prevent ?

安全設置和策略

設置防火牆、限制用戶權限、定期清理Cookies和緩存、開啟第二階段驗證登入等

入侵檢測和預防系統

偵測到異常系統行為時阻止網路連結，以防止cookie被寄送到外部伺服器

安全審計和測試

設置Cookie中的HttpOnly、Secure屬性，防止通過JavaScript獲取或在非加密連接中傳輸

Contribution

- 希望能引起大家對 Chrome Extension 安全性的重視，不要隨便下載來路不明的東西
- 讓大家知道即便能通過 Chrome Web Store 安全性測試的軟體也不一定是真的安全的

References

- Exploiting Leaky Chrome Extension API
- Adventures with Facebook’s session cookie

THANKS