

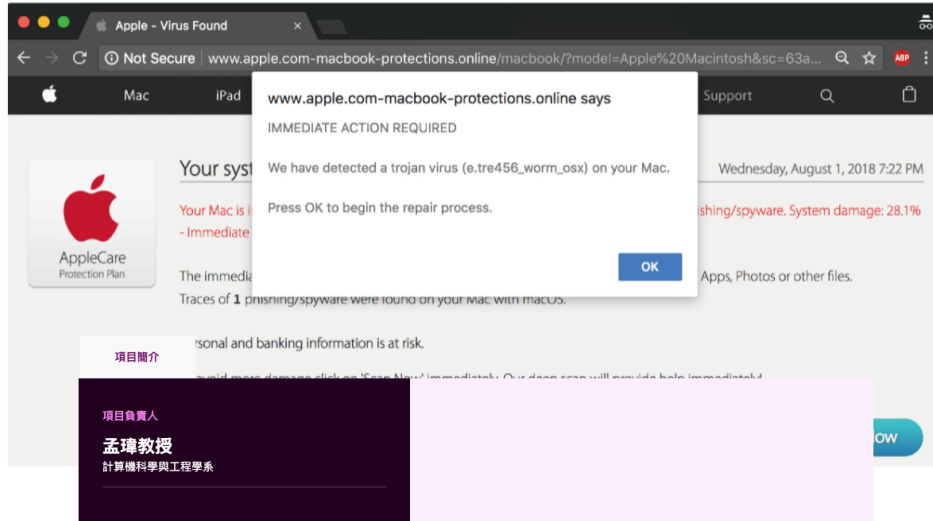


# 瀏覽器分析系統Observer

#2020

#Network

#Education

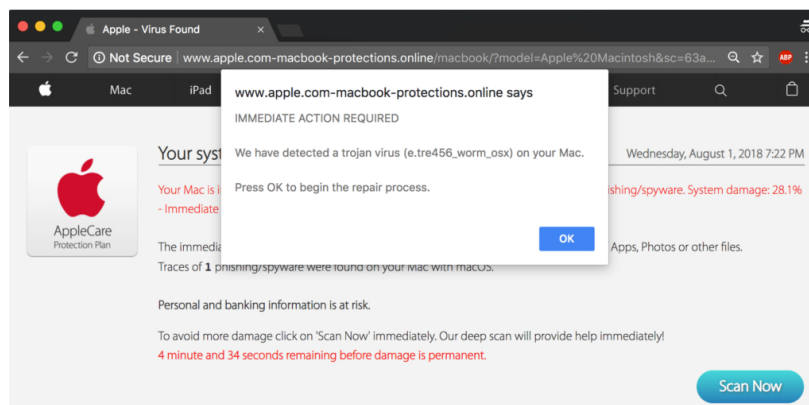


點擊是用戶與萬維網 (World Wide Web, WWW) 上內容進行互動的主要方式。不良第三方廣告商或駭客在網頁中加入惡意JavaScript代碼來攔截瀏覽器點擊，欺騙他們訪問不受信任的網頁，令網絡用戶安全受到威脅。攻擊者攔截真實的用戶點擊，製造廣告點擊流量以進行廣告點擊欺詐，或以用戶的身分向其他網站發送惡意指令，例如迫使用戶下載病毒程式。為了偵測此點擊攔截行為，本項目研發出瀏覽器分析系統Observer (觀察者)，可檢測三種用於攔截網絡用戶點擊的不同技術，有別於以往針對由第一方網站發起點擊攔截的研究，Observer可以應對由第三方JavaScript代碼發動的各種點擊攔截，針對全新領域。

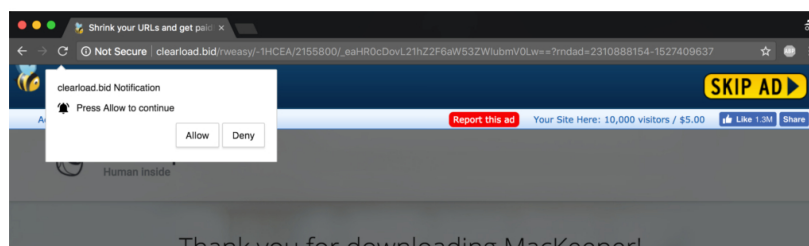
眾所周知，由第三方JavaScript代碼發動的網頁行為是很難用作記錄和分析的。Observer系統通過擴展瀏覽器以收集運行時的行為，針對點擊相關的行為作徹底分析，以此來檢測第三方的點擊攔截行為，保障用戶免受這些惡意攻擊威脅。我們利用Observer分析了Alexa (全球網站排名計算系統) 前25萬個網站，在其中613個受歡迎網站 (每日總瀏覽量約4,300萬人次) 上發現有437個第三方代碼在攔截用戶點擊。這些代碼通過攔截用戶點擊可誘騙用戶訪問3,251個被第三方操控的不受信任的網址，其中逾36%與在線廣告有關，另有部分點擊攔截網址會將用戶引向惡意內容如詐騙軟件，說明點擊攔截已成為網絡用戶的新威脅。我們的團隊已公開Observer系統源代碼，協助網絡用戶檢測惡意的點擊攔截，並就此惡意行為發出警告，保障他們免遭惡意網站的影響。

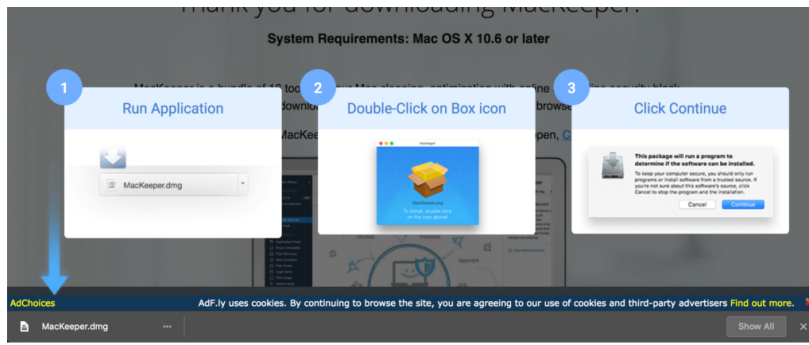
## 本研究確認了點擊攔截技術的三大類型：

1. 更改超連結的目標網址，當用戶點擊時將其引導至惡意網站。
2. 通過新增監聽事件 (Event Listener) 來欺騙用戶點擊。
3. 視覺攔截，例如模仿第一方網站內容製作網頁，欺騙用戶點擊由第三方控制的元素，或以透明介面覆蓋整個版面，攔截用戶對第一方內容的所有點擊，將用戶帶到由攻擊者控制的網頁。



受害用戶可被引導到偽造的防病毒頁面





受害用戶可被引導到路過式下載頁面。

## DO YOU LIKE OUR PROJECT?

[Tweet it](#)

[Share it](#)

[Share it](#)

[Contact us](#)

## MORE TO EXPLORE

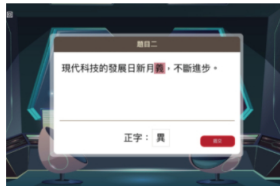
[All projects >](#)



信息及通訊科技

賽馬會社區關懷與創意教育實踐計劃

[Read more >](#)



信息及通訊科技

「知易行難」－基於人工智能的語言學習系統

[Read more >](#)



信息及通訊科技

突破性光子集成研究 實現高速光通信

[Read more >](#)



信息及通訊科技

虛擬香港殖民地時期建築之旅

[Read more >](#)