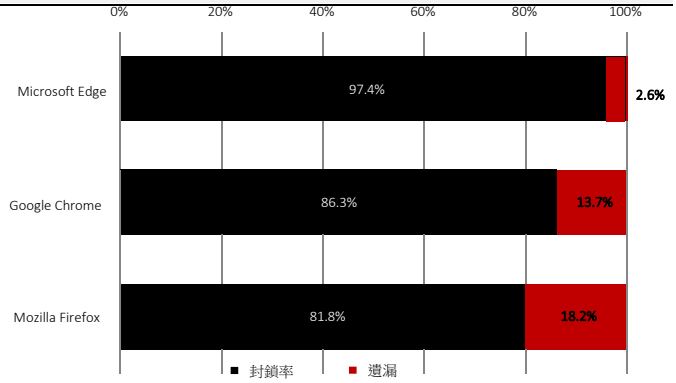
2021 年第 2 季　網頁瀏覽器對惡意程式碼

概觀

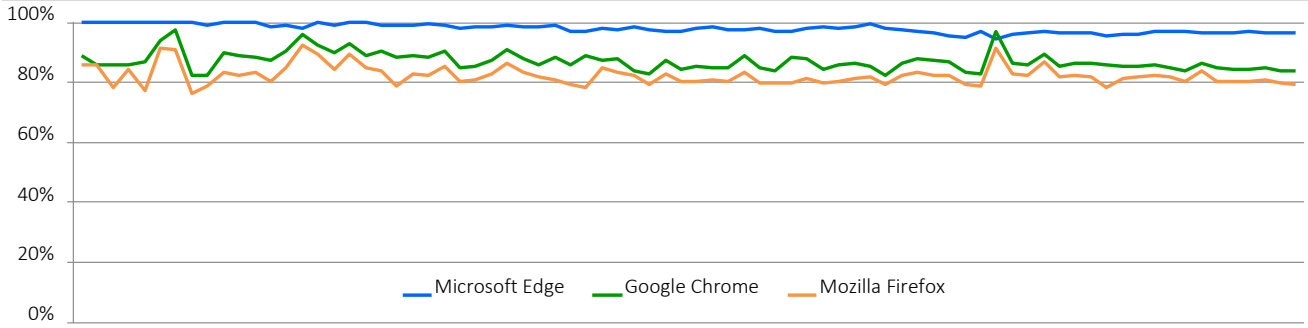
在 2021 年第 2 季期間，CyberRatings.org 針對網頁瀏覽器所提供的惡意程式碼保護力進行一項獨立測試。測試為期 20 天，期間進行 80 次離散的測試回合。為了防範惡意程式碼，Microsoft Edge 使用 Microsoft Defender SmartScreen；Google Chrome 和 Mozilla Firefox 則使用 Google Safe Browsing API。Microsoft Edge 的保護力最強，可封鎖 97.4% 的惡意程式碼，同時提供最高的零時差保護率 (97.7%)。Google Chrome 的保護力排名第二，平均可封鎖 86.3% 的惡意程式碼，第三則是 Mozilla Firefox，保護力為 81.8%。



結果摘要

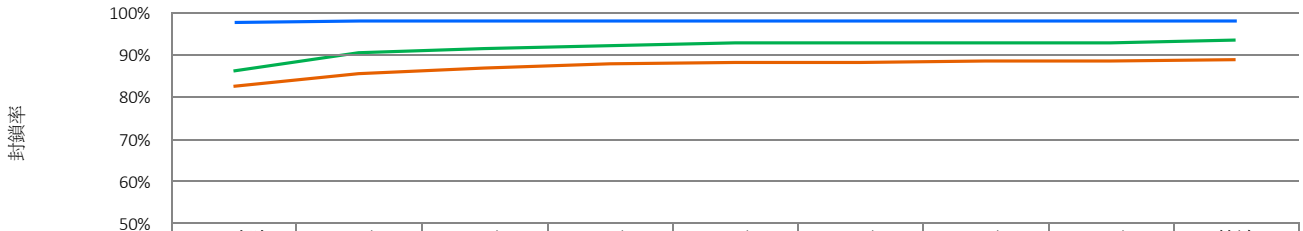
警告可能的受害者他們即將誤入惡意網站的能力，是網頁瀏覽器對抗惡意程式碼的獨特能力。引誘 (以社交工程的方式) 使用者下載惡意程式碼的網站的生命週期很短，所以，一定要盡快發現網站並新增到評價系統。因此，良好的評價系統必須正確又快速，才能實現高攔截率。

經過一段時間的惡意程式碼保護力



在整個測試期間，新的惡意程式碼不斷地增加。無法再連線或不再裝載的惡意程式碼的 URL 都已遭到移除。每個資料點都是根據特定時間點所記錄的測量來計算。如果惡意程式碼是在一開始時遭到封鎖，瀏覽器的保護力分數就會隨著時間而提高。反之，如果瀏覽器未封鎖惡意程式碼，則分數會減少。

經過一段時間的惡意程式碼封



	0 小時	1 天	2 天	3 天	4 天	5 天	6 天	7 天	總計
Microsoft Edge	97.7%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%	97.9%
Google Chrome	86.4%	90.6%	91.7%	92.5%	92.9%	93.1%	93.1%	93.1%	93.6%
Mozilla Firefox	82.8%	85.9%	87.1%	88.0%	88.3%	88.4%	88.6%	88.7%	89.1%

上圖顯示樣本引入測試週期後，每個瀏覽器花費多少時間來封鎖惡意程式碼。Microsoft Edge 內的核心保護技術是 SmartScreen，此技術透過整合式、雲端式 URL 評價服務，提供以 URL 為主的保護來防範攻擊，並且運用應用程式評價來封鎖惡意檔案。Google Chrome 和 Mozilla Firefox 則是使用 Google Safe Browsing API 同時進行 URL 評價，以及封鎖或警告使用者關於特定檔案類型的下載。

惡意程式碼攻擊

社交工程的惡意程式碼 (SEM) 攻擊利用欺騙引誘使用者下載惡意程式碼：遭到劫持的電子郵件和社交媒體帳戶會利用連絡人之間隱含的信任，哄騙受害者相信那個惡意檔案的連結是可信任的。其他欺騙手法包括快顯視窗訊息，建議使用者必須安裝應用程式 (例如 Adobe Flash Player)，或者警告使用者，電腦受到感染或需要更新。

一旦安裝惡意程式碼，受害者就會容易受到認證竊取、身分識別遭竊、銀行帳戶遭入侵等攻擊。

網頁瀏覽器防範惡意程式碼的保護力

為了防範惡意程式碼，雲端式評價系統會清查網際網路，尋找惡意網站，然後根據內容來分類。接著，網頁瀏覽器會詢問雲端式評價系統有關 URL、檔案或應用程式的資訊。如果結果指出存在惡意程式碼，網頁瀏覽器就會將使用者重新導向一個警告訊息，說明 URL、檔案或應用程式是惡意的。有些評價系統還會包含其他教育內容。

Google Chrome 和 Mozilla Firefox 則是使用 Google Safe Browsing API 同時進行 URL 評價和應用程式評價，以封鎖惡意檔案。Microsoft Edge 採用 Microsoft Defender SmartScreen，此技術透過雲端式評價服務進行 URL 評價，以防範攻擊，並且運用應用程式評價來封鎖惡意檔案。

惡意程式碼樣本每天新增的平均數目

平均來說，每天會有 49 個經過驗證的新惡意程式碼樣本新增到測試組；有些日期的數目會隨著犯罪活動程度變化而有所不同。

測試的惡意樣本總數

18,621 個原始、未經驗證的樣本已在每個網頁瀏覽器測試多次，每個瀏覽器總計進行 78 個測試週期，執行時間不間斷，超過 468 個小時 (每 6 小時一次，共 20 天)。我們的工程師已移除未通過驗證準則的樣本，其中包括那些遭到惡意探索 (不在本測試範圍內) 污染的樣本。最後，48,672 次離散、有效的惡意程式碼測試 (每個網頁瀏覽器 16,224 次測試) 中包含 950 個唯一、有效的惡意程式碼樣本，誤差邊際小於百分之 3.2 (<3.2%)，信賴水準 95%。

如何測試 – 惡意程式碼樣本

這份報告中的資料為 20 天的測試期間，從 2021 年 5 月 11 日到 5 月 31 日。測試期間，CyberRatings 工程師定期監測連線能力，以確保測試中的瀏覽器可以存取雲端中的惡意程式碼及評價服務。

重點在於時效性，因此持續地將新樣本加入測試並移除過期樣本。

如何評估結果

我們已測量每個瀏覽器一發現網際網路上的惡意程式碼，即盡快封鎖惡意程式碼的能力。工程師們每六個小時重覆執行這些測試一次，以判斷廠商會花費多久時間來增加保護。

每個瀏覽器的效能都連續不斷地進行測量，並且所有以瀏覽器進行測試的惡意程式碼樣本整體封鎖率都已記錄下來。每個瀏覽器整體封鎖率的計算方式是，成功封鎖數除以測試案例總數。例如，在每 6 個小時進行一次的測試中，上線 48 小時的惡意程式碼樣本已測試八 (8) 次。瀏覽器若在 6 次 (最多 8 次) 測試回合封鎖惡意程式碼，即達到 75% 的封鎖率。

測試環境

- Microsoft Windows 10 專業版、21H1

測試的產品

- Google Chrome：版本 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge：版本： 91.0.864.19 - 91.0.864.37
- Mozilla Firefox：版本 88.0.1 - 88.0.1

作者

Thomas Skybakmoen、Vikram Phatak

測試方法

CyberRatings 網頁瀏覽器安全性測試方法 v1.0 可以在 www.cyberratings.org 取得

連絡資訊

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org