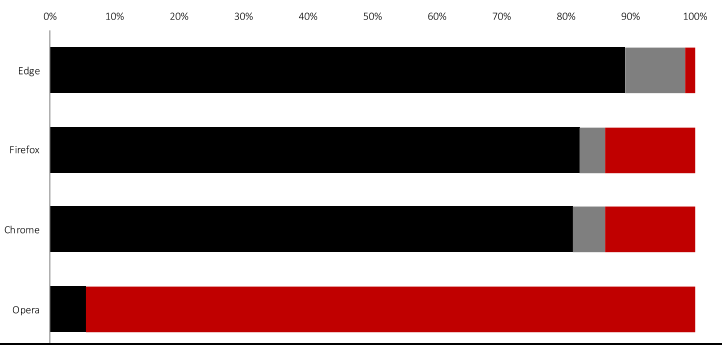
2020 年第 2 季 比較測試報告

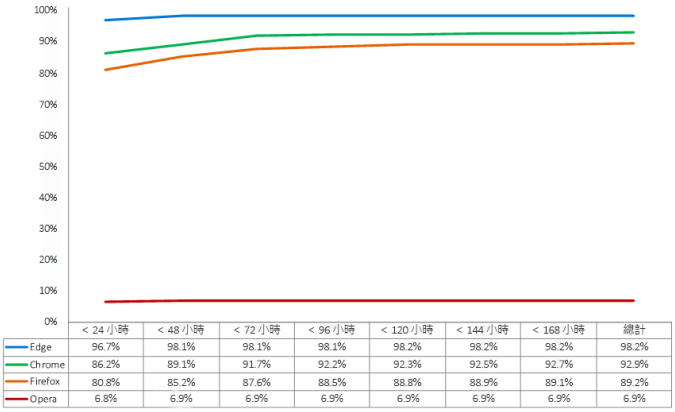
概觀

2020 年第 2 季期間，NSS Labs 針對網頁瀏覽器所提供的惡意程式碼保護進行一項獨立測試：在 34 天內採用 1,065 個獨立樣本，進行 32,267 次離散測試 (每個網頁瀏覽器)。為了防範惡意程式碼，Microsoft Edge 使用 Microsoft Defender SmartScreen；Google Chrome 和 Mozilla Firefox 使用 Google Safe Browsing API，而 Opera 使用 Yandex。

Microsoft Edge 提供的保護最強，可封鎖 98.5% 的惡意程式碼，同時提供最高零時差保護率 (96.7%)。Firefox 提供第二強的保護，平均封鎖 86.1% 的惡意程式碼，接著是 86.0% 的 Google Chrome。Opera 則封鎖 5.6%。



結果摘要

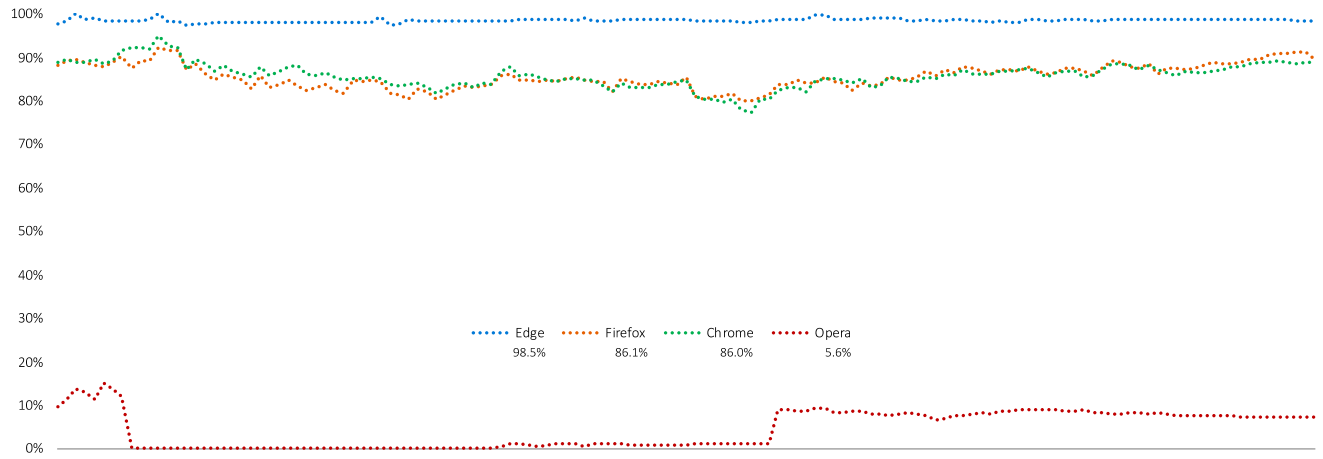


	< 24 小時	< 48 小時	< 72 小時	< 96 小時	< 120 小時	< 144 小時	< 168 小時	總計
Edge	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Chrome	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Firefox	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Opera	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

信譽系統藉由預防或警告使用者某個 URL、檔案或應用程式是危險的，縮短攻擊者達到其目標所需花費的時間。然而，使用者不斷造訪新網站並下載檔案及安裝應用程式。信譽系統無法單純地封鎖所有新項目。基於這點，攻擊者的惡意程式碼活動會不斷改變，並且所有的攻擊大多數會在活動啟動後幾個小時內發生。因此，精確、快速地分類內容是成功保護的關鍵。

NSS Labs 已評定各瀏覽器在網際網路上找到惡意程式碼時可快速加以封鎖的能力。我們繼續每 6 小時測試惡意 URL、檔案和應用程式一次，判斷廠商需要花費多久時間才能新增保護 (如果他們真的做了)。

一段時間內的惡意程式碼保護



在整個測試中，新的惡意程式碼不斷地增加。無法再連線或裝載惡意程式碼的 URL、檔案和應用程式都已移除。每個資料點是從特定時間點記錄的數值來計算。如果攻擊開始後不久即封鎖惡意程式碼，那麼過一段時間後瀏覽器的保護一致性分數就會提升。或者，如果瀏覽器並未封鎖惡意程式碼，則分數會減少。

測試以 Web Browser Test Methodology v4.0 為基礎 (請參閱 www.nsslabs.com)。

背景

社交工程惡意程式碼 (SEM) 攻擊會變換組合社交媒體、遭劫持的電子郵件帳戶、假的電腦問題通知以及其他詐騙手法，鼓吹使用者下載惡意程式碼。網路罪犯會使用劫持的電子郵件帳戶來利用連絡人之間未言明的信任，欺騙受害者相信惡意檔案的連結是可信任的。網路罪犯利用遭劫持的社交媒體帳戶的方式與遭劫持的電子郵件帳戶方式相同。然而，在社交網路的情況中，這樣的循環變得更廣：朋友、甚至朋友的朋友都可能遭到欺騙。

社交工程策略可能會使用快顯訊息；例如，建議使用者需要安裝如 Adobe Flash Player 等應用程式，或者他們的電腦受到感染或需要更新。一旦安裝惡意程式碼，受害者可能會遭到身分盜用、銀行帳戶遭入侵，以及其他可能嚴重後果。

防範惡意程式碼的網頁瀏覽器保護

為了防範惡意程式碼，瀏覽器使用雲端式信譽系統，這些信譽系統會清查網際網路上的惡意網站，然後根據內容，將網站歸類於封鎖清單或允許清單，或者加以評分 (視廠商的方式而定)。

這些分類技術可以手動或自動執行。防範惡意程式碼的第二個基本要件是，網頁瀏覽器從雲端式信譽系統要求有關特定 URL、檔案或應用程式的信譽資訊，然後進行警告或封鎖惡意程式碼。

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警告訊息，說明該 URL、檔案或應用程式是惡意的。此外，某些信譽系統還會加入其他教育內容。相反地，如果判斷內容是「沒問題的」，網頁瀏覽器就不會採取任何行動，並且使用者也不會察覺瀏覽器剛執行過安全性檢查。

Google 和 Firefox 使用 Google Safe Browsing API 檢查 URL 信譽，並且封鎖或警告使用者下載特定檔案類型。Microsoft Edge 使用 Microsoft Defender SmartScreen，其中包括應用程式信譽服務，可提供防範網路釣魚和惡意程式碼威脅的保護。Opera 搭配使用來自 Netcraft[1]、PhishTank[2] 和 Metamask[3] 的封鎖清單，以及來自 Yandex[4] 的惡意程式碼封鎖清單。

此外，Microsoft Defender SmartScreen 已透過 Windows 10 2017 年 10 月更新，併入成為全作業系統的功能。SmartScreen 保護的作業系統版本是所有瀏覽器、電子郵件用戶端、USB 及其他應用程式的後捕網，成為防範惡意程式碼的作業系統保護的一部分。使用者因而從瀏覽器 URL 保護、瀏覽器應用程式/檔案保護，以及作業系統保護中受益。

測試組合 – 惡意程式碼樣本

這份報告中的資料包括 2020 年 4 月 21 日到 2020 年 5 月 25 日之間，共 34 天的測試時間。所有測試都是在位於德州奧斯丁的 NSS 測試機構進行。測試期間，NSS 工程師經常監視連線能力，以確保測試中的瀏覽器能存取惡意程式碼，以及雲端中的信譽服務。

重點在於時效性，因此，評估的樣本數目比最後保留做為結果測試組的樣本數目多一點，因為新樣本不斷地加入測試且無效樣本已移除。

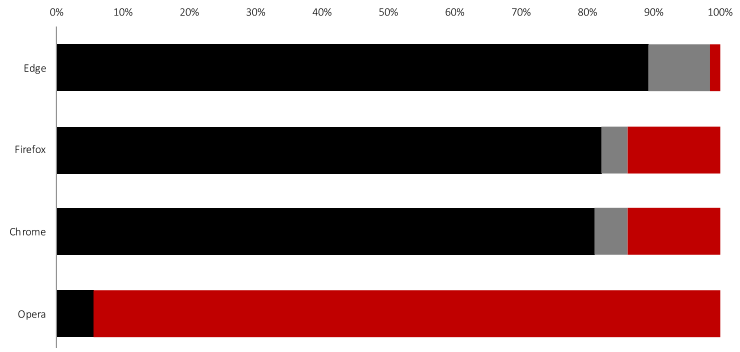
測試的惡意樣本總數

每個網頁瀏覽器共有 1,844 個原始、未經驗證的樣本進行測試，連續 822 個小時 (每 6 小時一次，共 34 天) 裡總共進行 182,676 次離散測試。NSS 工程師已移除未通過驗證條件的樣本，其中包括遭到惡意探索 (不屬於這次測試) 汙染的樣本。最後，1,065 個獨立、有效的惡意程式碼樣本包含在 129,068 次離散、有效的惡意程式碼測試中 (每個網頁瀏覽器 32,267 次)，誤差邊際少於百分之 2 (<2%)，信賴等級為 95%。

[1] http://www.netcraft.com/
[2] http://www.phishtank.com/
[3] https://github.com/metamask/eth-phishing-detect
[4] https://yandex.com

惡意程式碼封鎖率

警告可能的受害者他們即將誤入惡意網站的能力，讓網頁瀏覽器處於對抗社交性工程的惡意程式碼的特殊處境。由於惡意程式碼網站的生命週期短暫，因此，必須盡快發現網站、進行驗證、分類並新增到信譽系統。因此，良好的信譽系統必須精確且快速，才能實現高攔截率。瀏覽器開發人員明白了解這層關係，並且在偵測後的前 24 個小時裡所封鎖的惡意程式碼比之後多了許多。



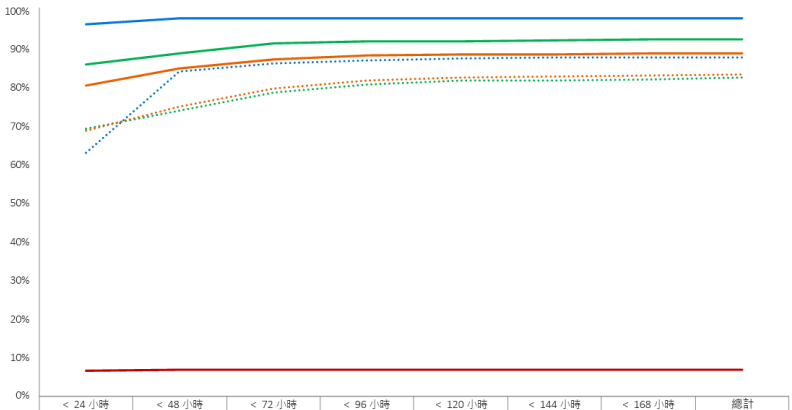
	Opera	Chrome	Firefox	Edge
URL 信譽	5.6%	80.9%	82.1%	89.2%
URL + 應用程式信譽	0.0%	5.0%	4.0%	9.3%
URL + 應用程式 + OS 信譽	93.1%	13.1%	13.0%	0.7%
填滿	1.4%	0.9%	0.9%	0.8%

Edge 內採用的核心保護技術是 SmartScreen，其透過整合的雲端式 URL 信譽服務，以及可封鎖惡意檔案的應用程式信譽，提供以 URL 為基礎的保護。Edge 的 SmartScreen 應用程式信譽封鎖了 98.5%。Mozilla Firefox 和 Google Chrome 使用 Safe Browsing API。Firefox 封鎖 86.1%。Google Chrome 封鎖 86.0%。搭配使用數個來源的封鎖清單的 Opera 則封鎖 5.6%。

此外，當我們嘗試執行時，Microsoft Defender SmartScreen 還為 Opera 封鎖 93.1% 的惡意檔案；為 Chrome 封鎖 13.1% 的惡意檔案；為 Firefox 封鎖 13.0% 的惡意檔案，並且為 Edge 封鎖 0.7% 的惡意檔案。

惡意程式碼保護長條圖

立即防範新的惡意程式碼是必要的。一發現裝載惡意程式的網站，網站通常會在相當短的時間內撤下。若無法及時新增保護，產品反擊威脅的速度可能太慢。此長條圖顯示將樣本引入測試週期之後，每個瀏覽器花費多少時間來封鎖惡意程式碼。在 7 天的時間裡，每天都會計算累積保護率，直到封鎖威脅為止。



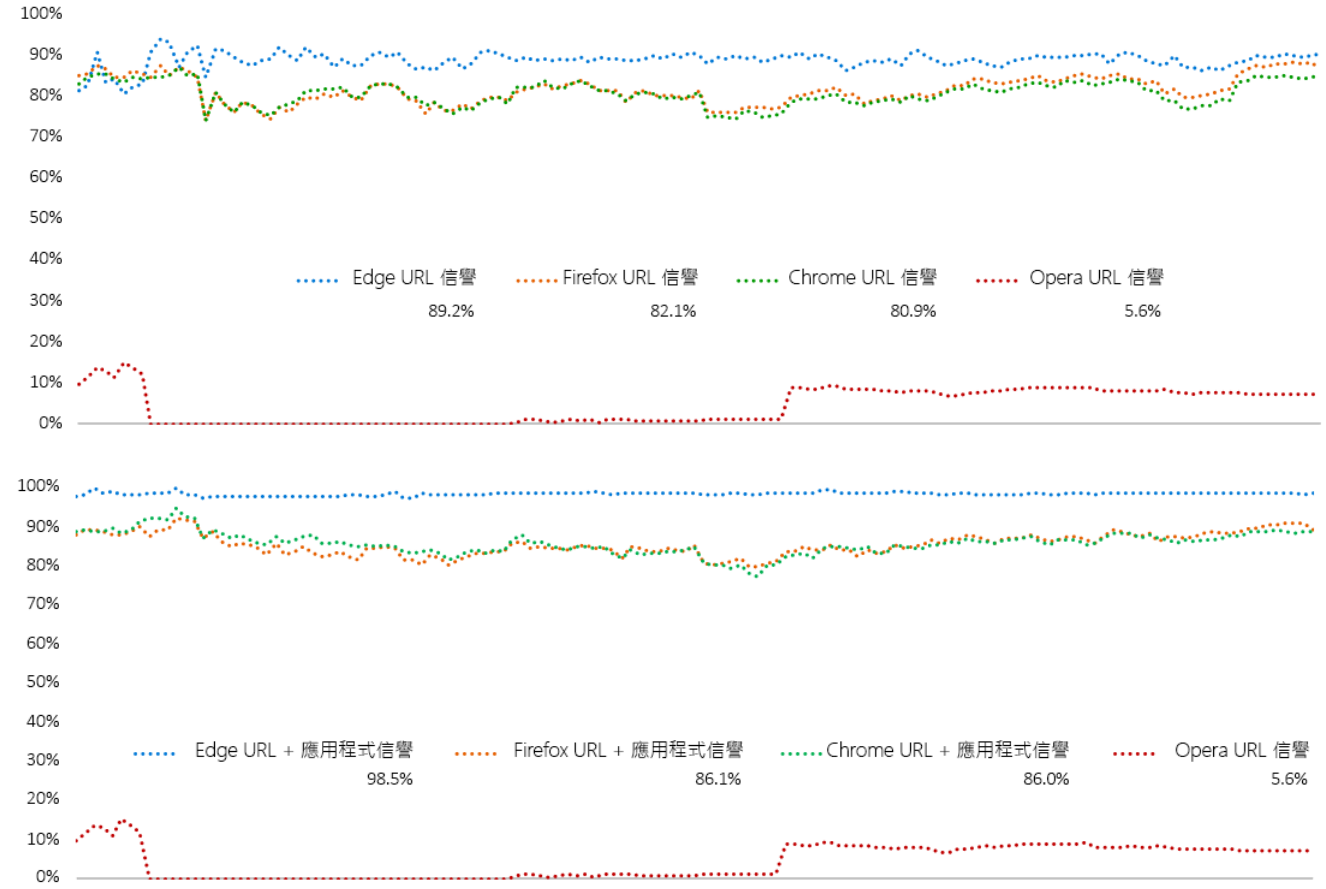
	< 24 小時	< 48 小時	< 72 小時	< 96 小時	< 120 小時	< 144 小時	< 168 小時	總計
Edge 與應用程式信譽	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Edge 與 URL 信譽	63.4%	84.5%	86.5%	87.3%	87.8%	88.1%	88.1%	88.1%
Chrome 與應用程式信譽	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Chrome 與 URL 信譽	69.7%	74.4%	79.0%	81.0%	82.0%	82.2%	82.4%	82.7%
Firefox 與應用程式信譽	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Firefox 與 URL 信譽	69.1%	75.3%	80.0%	82.1%	82.9%	83.0%	83.4%	83.6%
Opera 與 URL 信譽	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

測試期間，Microsoft Edge 證明防範惡意程式碼的初始保護率為 96.7%。Google Chrome 和 Mozilla Firefox 的初始保護率分別達到 86.2% 和 80.8%。Opera 的初始保護率則為 6.8%。到了測試第 7 天結束時，所有網頁瀏覽器的保護都已提升。Microsoft Edge 增加 4.5%，達到 98.2%。Google Chrome 增加 6.7%，達到 92.9%；Mozilla Firefox 增加 8.4%，達到 89.2%；Opera 則增加 0.1%，達到 6.9%

一段時間的保護一致性

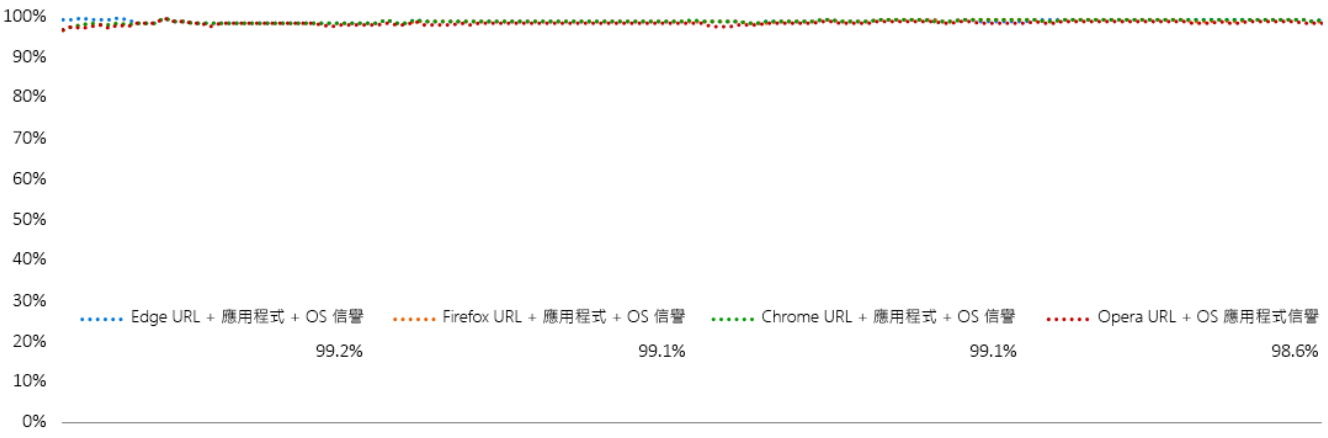
在整個測試中，新的惡意程式碼不斷地增加。無法再連線或裝載惡意程式碼的 URL、檔案和應用程式都已移除。每個資料點是從特定時間點記錄的數值來計算。如果攻擊開始後不久即封鎖惡意程式碼，那麼過一段時間後瀏覽器的保護一致性分數就會提升。或者，如果瀏覽器並未封鎖惡意程式碼，則分數會減少。

測試顯示三層保護：URL 信譽、瀏覽器中的應用程式信譽，以及作業系統應用程式信譽。URL 信譽提供的保護相當不錯。



加上應用程式信譽加強保護。

作業系統信譽則提供額外保護。以理想而言，網頁瀏覽器會封鎖惡意程式碼，使惡意程式碼絕不會接觸到作業系統。然而，測試指出作業系統信譽極為有效。



測試環境

- BaitNET™ (NSS Labs 專利)
- 64 位元 Microsoft Windows 10 專業版 (版本 1909 組建：18363.592)
- Ubuntu 18.04.3 LTS
- Kali (核心發行版本 4.19.0-kali5-amd64)
- VMware vCenter (版本 6.7u2 組建 6.7.0.30000)
- VMware vSphere (版本 6.7.0.20000)
- VMware ESXi (版本 6.7u3 組建 14320388)
- VMware Tools 10.3.5
- Wireshark 版本 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (組建 283)
- GNU Wget 1.19.4
- Curl 7.58.0

測試的產品

- Google Chrome：版本 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge：版本 83.0.478.10 – 84.0.516.1
- Mozilla Firefox：版本 75.0 – 76.0.1
- Opera：版本：67.0.3575.137 – 68.0.3618.125

作者

Dipti Ghimire、Thomas Skybakmoen、Vikram Phatak

測試方法

如需 NSS Labs Web Browser Security (WBS) Test Methodology v4.0，請前往 www.nsslabs.com。

連絡資訊

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com