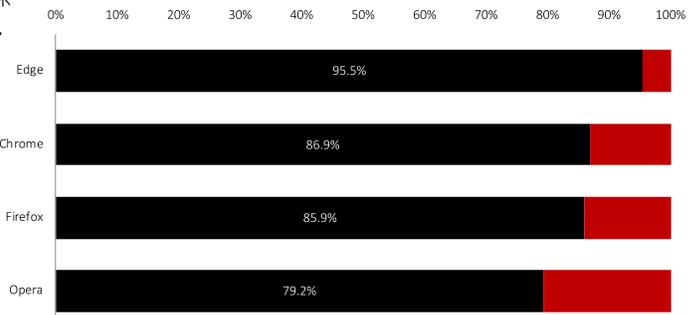


2020 年第 2 季

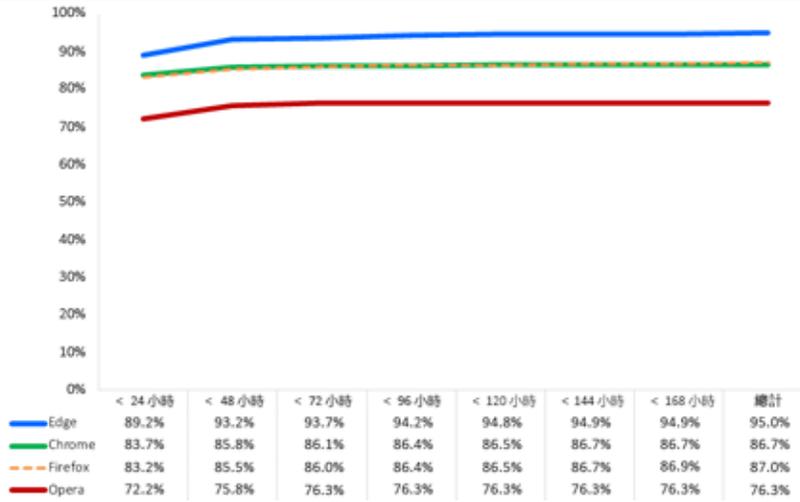
比較測試報告

概觀

2020 年第 2 季期間，NSS Labs 針對網頁瀏覽器所提供的網路釣魚保護進行一項獨立測試：在 18 天內採用 2,443 個獨立網路釣魚 URL，進行 47,274 次離散測試 (每個網頁瀏覽器)。為了防範網路釣魚，Microsoft Edge 使用 Microsoft Defender SmartScreen；Google Chrome 和 Mozilla Firefox 運用 Google Safe Browsing API，而 Opera 搭配使用協力廠商的封鎖清單。Microsoft Edge 提供的保護最強，可封鎖 95.5% 的網路釣魚 URL，同時提供最高零時差保護率 (89.2%)。Google Chrome 提供第二強的保護，平均封鎖 86.9% 的網路釣魚 URL，接著是 85.9% 的 Mozilla Firefox。Opera 則封鎖 79.2%。



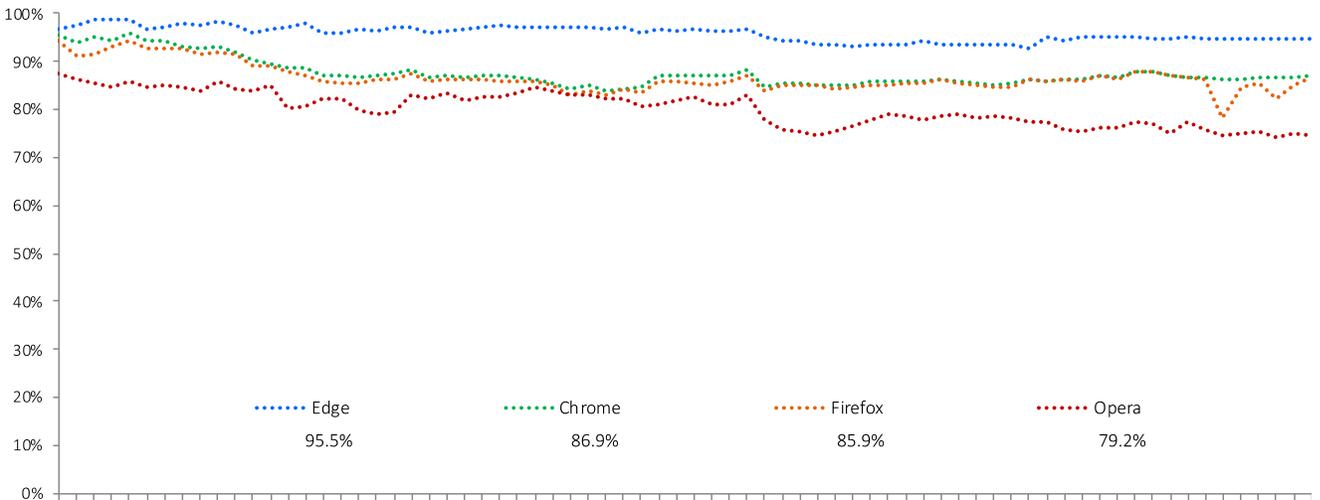
結果摘要



URL 信譽系統藉由預防/警告使用者某個 URL 是已知的網路釣魚網站，縮短攻擊者達到其目標所需花費的時間。然而，由於使用者會造訪各種網站，其中許多是新的網站，因此，URL 信譽系統無法單純地封鎖所有新的 URL。基於這點，攻擊者的網路釣魚活動會不斷改變，大量新攻擊會在攻擊發動後幾個小時內發生。

NSS Labs 已評定各瀏覽器在網際網路上找到惡意 URL 時可快速加以封鎖的能力。我們繼續每 6 小時測試惡意 URL 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)。

一段時間內的網路釣魚保護



在整個測試中，新的網路釣魚 URL 每天增加，並且無法再連線或不再傳遞網路釣魚攻擊的 URL 都已移除。每個資料點代表特定時間點的保護。如果攻擊開始後不久即封鎖 URL，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 URL，則分數會減少。

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

這份報告為機密且明示僅限 NSS Labs 的授權客戶使用。

背景

網路釣魚是一種社交工程攻擊，此攻擊會試圖說明受害者將敏感性個人資訊提供給攻擊者。幾個敏感性資訊的範例包括信用卡號碼、身分證號碼，以及登入資訊和銀行帳戶密碼。電子郵件、即時訊息、手機簡訊以及社交網路網站上的連結，全是網路釣魚攻擊的媒介。通常，網路釣魚網站的登陸頁面也會試圖以無訊息方式利用造訪者的電腦並安裝惡意軟體 (又稱為路過式惡意探索)。

網路釣魚攻擊藉由威脅入侵或取得敏感性的個人和企業資訊，對個人和組織而言，都會造成極大風險。Anti-Phishing Working Group (APWG) 回報在 2020 年第一季，總共有 165,772 個獨立電子郵件網路釣魚活動。¹網路釣魚攻擊變得越來越複雜且精良，讓人們更難以偵測、預防。

防範網路釣魚的網頁瀏覽器保護

網路釣魚保護是由網頁瀏覽器內的應用程式所提供，並且會向雲端中的信譽伺服器要求 URL 的信譽。信譽伺服器會清查網際網路，尋找網路釣魚網站，然後為每個 URL 指派分數並新增到封鎖清單。如此一來，當使用者指示網頁瀏覽器造訪某個 URL 時，瀏覽器的網路釣魚保護 (例如 Safe Browsing、SmartScreen 等) 會向雲端式信譽伺服器要求 URL 的信譽，如果結果指出網站「有問題」，網頁瀏覽器就會將使用者重新導向警告訊息，說明該 URL 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，如果判斷網站是「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。

這份報告中的資料包括 2020 年 4 月 21 日到 2020 年 5 月 8 日之間，共 18 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網路釣魚 URL，以及雲端中的瀏覽器信譽服務。

重點在於時效性，因此，評估的網站數目比最後保留做為結果測試組的網站數目多一點，因為新的 URL 不斷地加入測試且無效網站已移除。

測試中的惡意 URL 總數

每個網頁瀏覽器共有 4,020 個原始、未經驗證的 URL 進行測試，連續 430 個小時 (每 6 小時一次，共 18 天) 裡總共進行 222,527 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) 污染的樣本。最後，2,443 個獨立、有效的網路釣魚 URL 包含在 189,096 次離散、有效的網路釣魚測試中 (每個網頁瀏覽器 47,274 次)，誤差邊際少於百分之 2 (<2%)，信賴等級為 95%。

每天平均增加的惡意 URL 數目

平均而言，每天有 136 個全新、通過驗證的 URL 新增到測試組；由於犯罪活動層級變動，數目依某些天數而定。

封鎖網路釣魚 URL

NSS 已評定瀏覽器在網際網路上找到惡意 URL 時可快速加以封鎖的能力。工程師們每 6 小時重複這些測試一次，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)。

新版 Microsoft Edge 以 Chromium 為基礎，並且已於 2020 年 1 月 15 日發行。此瀏覽器與所有支援的 Windows 和 macOS 版本相容。下載瀏覽器將會取代 Windows 10 電腦上的舊版 Microsoft Edge。

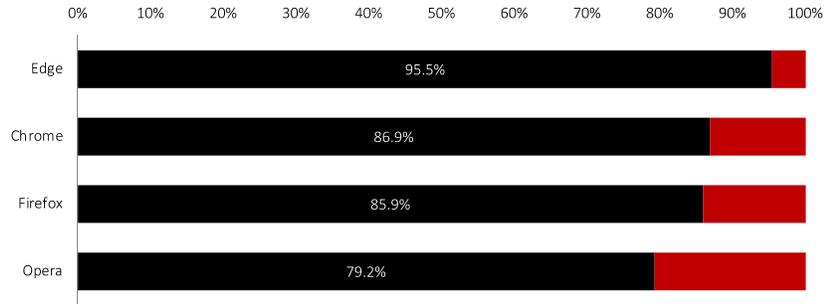
<https://support.microsoft.com/zh-tw/help/4501095/download-the-new-microsoft-edge-based-on-chromium>

¹ APWG 網路釣魚活動趨勢報告

網路釣魚封鎖率

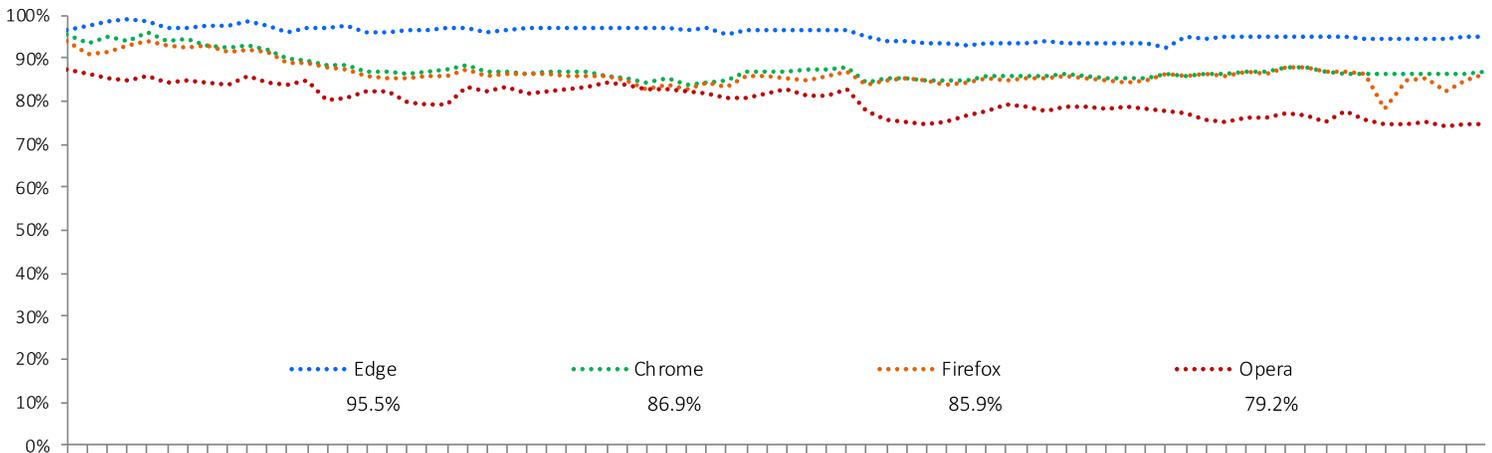
Google Chrome 和 Mozilla Firefox 使用 Google 的 Safe Browsing API。Microsoft Edge 使用 Microsoft Defender SmartScreen，其中包括應用程式信譽服務，可提供防範網路釣魚和惡意程式碼威脅的保護。Opera 搭配使用來自 Netcraft²、PhishTank³ 和 Metamask⁴ 的封鎖清單，以及來自 Yandex⁵ 的惡意程式碼封鎖清單。

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網路釣魚和其他犯罪活動的特殊處境。由於網路釣魚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。這說明平均封鎖時間與攔截率的關聯性。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 個小時裡所封鎖的網路釣魚網站比之後多了許多。



測試持續測量每個瀏覽器的個別封鎖效能，並且瀏覽器所測試的所有 URL 的整體封鎖率都已記錄下來。瀏覽器的整體封鎖率的計算方式是，成功封鎖的數目除以測試案例總數。舉例來說，在每 6 個小時進行一次的測試中，上線 48 小時的 URL 會進行 8 次測試。如果瀏覽器在 6 個測試回合（最多 8 個回合）中加以封鎖，將會達到 75% 的封鎖率。

一段時間的保護一致性



在整個測試中，新的網路釣魚 URL 每天增加，並且無法再連線或不再傳遞網路釣魚 URL 的 URL 都已移除。每個資料點代表特定時間點的保護。如果攻擊開始後不久即封鎖 URL，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 URL，則分數會減少。

² <http://www.netcraft.com/>

³ <http://www.phishtank.com/>

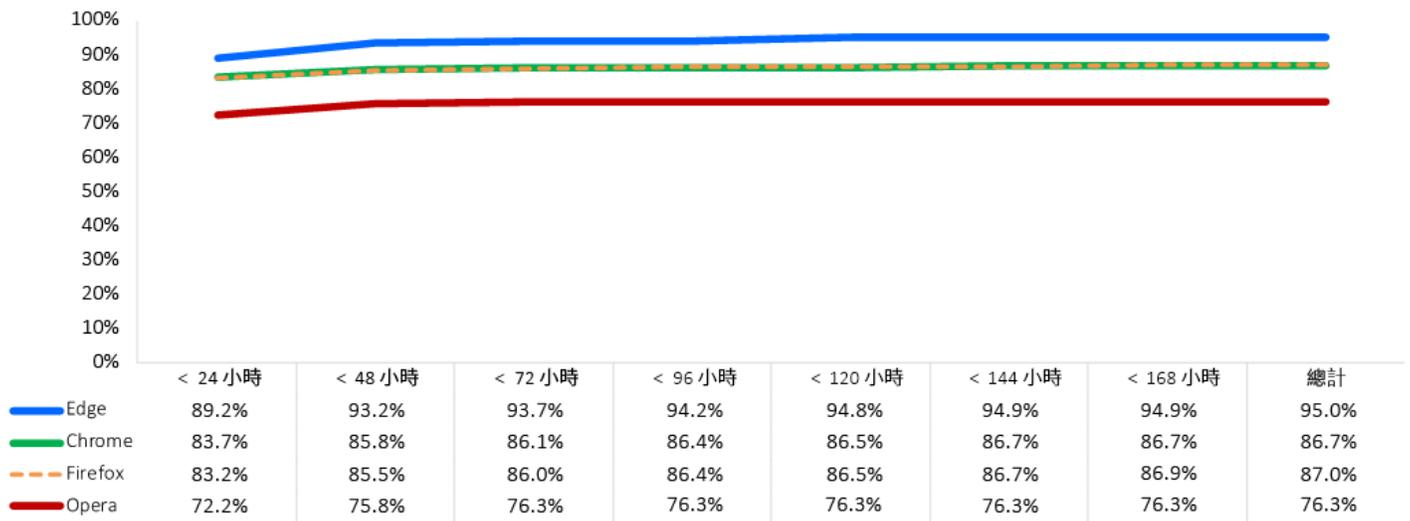
⁴ <https://github.com/metamask/eth-phishing-detect>

⁵ <https://yandex.com>

網路釣魚保護長條圖

立即防範新的網路釣魚 URL 是必要的。一發現網路釣魚網站，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。下面的長條圖顯示將網路釣魚網站引入測試週期之後，每個瀏覽器花費多少時間來封鎖網路釣魚網站。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。

測試期間，Microsoft Edge 證明防範網路釣魚攻擊的初始保護率為 89.2%。Google Chrome 和 Mozilla Firefox 的初始保護率分別達到 83.7% 和 83.2%。Opera 的初始保護率則為 72.2%。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 5.7%，達到 94.9%。Mozilla Firefox 增加 3.7%，達到 86.9%；Google Chrome 增加 3%，達到 86.7%。Opera 則增加 4.1%，達到 76.3%。



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 – 84.0.502.0
- 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

如需這份和其他相關文件，請前往：www.nsslabs.com。若要取得授權複本或回報誤用，請與 NSS Labs 連絡。

© 2020 NSS Labs, Inc. 著作權所有，並保留一切權利。未經 NSS Labs, Inc. (「我們」) 書面許可，貴用戶不得重製、複製/掃描本出版物的任何部分，也不得將本出版物的任何部分儲存於檢索系統 (a retrieval system)、以電子郵件傳送或其他方式發佈或傳送。

請閱讀這個方塊中的免責聲明，其中包含與您有關的重要資訊。如果您不同意這些條件，則不應閱讀這份報告的其餘部分，相反地，請立即將報告退回給我們。「您」或「您的」是指存取這份報告的人員，以及代表何人取得這份報告的任何實體。

1. 我們可能隨時變更這份報告中的資訊，恕不另行通知，並且我們不提供任何更新義務之擔保。
2. 我們相信但不保證這份報告中的資訊在發表時是正確且可靠的。請自行承擔使用及信賴這份報告的風險。我們對於任何損壞、遺失或因這份報告中的任何錯誤或疏失而產生的任何費用，概不負責。
3. 我們並未做出任何明示或默示擔保。我們特此免責並排除所有默示擔保，包括適售性、適合某特定用途及未侵權之默示擔保。在任何情況下，我們對於任何直接、衍生性、附隨性、懲罰性、懲戒性或間接損害，或者任何利益、收益、資料、電腦程式或其他資產之損失，不需負任何責任，縱然已經事先通知此種損害發生之可能性。
4. 這份報告不代表贊成、推薦或保證任何測試的產品 (硬體或軟體) 或測試產品所使用的硬體及/或軟體。此測試不保證產品沒有錯誤或瑕疵，或產品將符合貴用戶的期望、需求、需要或規格，或者產品將會運作而不中斷。
5. 這份報告不代表與其中所提之任何組織有任何背書、贊助、關係或驗證之聯繫。
6. 這份報告中使用的所有商標、服務標章和商標名稱均為其各自擁有者的商標、服務標章和商標名稱。