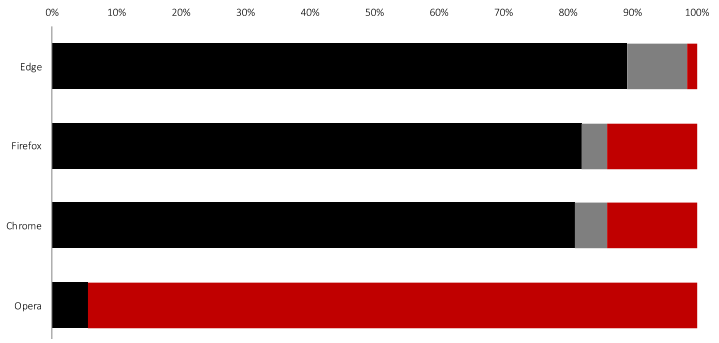
Q2 2020 LAPORAN PENGUJIAN KOMPARATIF

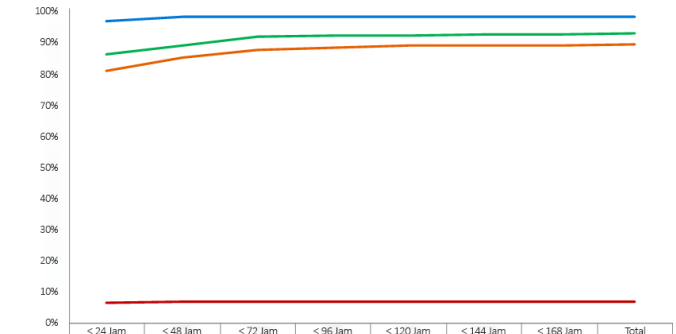
Ringkasan

Selama Q2, 2020, NSS Labs melakukan pengujian perlindungan malware independen yang ditawarkan oleh browser web: 32.267 pengujian terpisah (per browser web) menggunakan 1.065 sampel unik selama 34 hari. Untuk melindungi dari malware, Microsoft Edge menggunakan Microsoft Defender SmartScreen; Google Chrome dan Mozilla Firefox menggunakan API Penjelajahan Aman Google; dan Opera menggunakan Yandex.

Microsoft Edge menawarkan perlindungan tertinggi, memblokir 98,5% malware, sekaligus memberikan tingkat perlindungan seketika (96,7%). Firefox memberikan perlindungan tertinggi kedua, memblokir rata-rata 86,1%, diikuti oleh Google Chrome pada 86,0%. Opera memblokir 5,6%.



Ringkasan Hasil

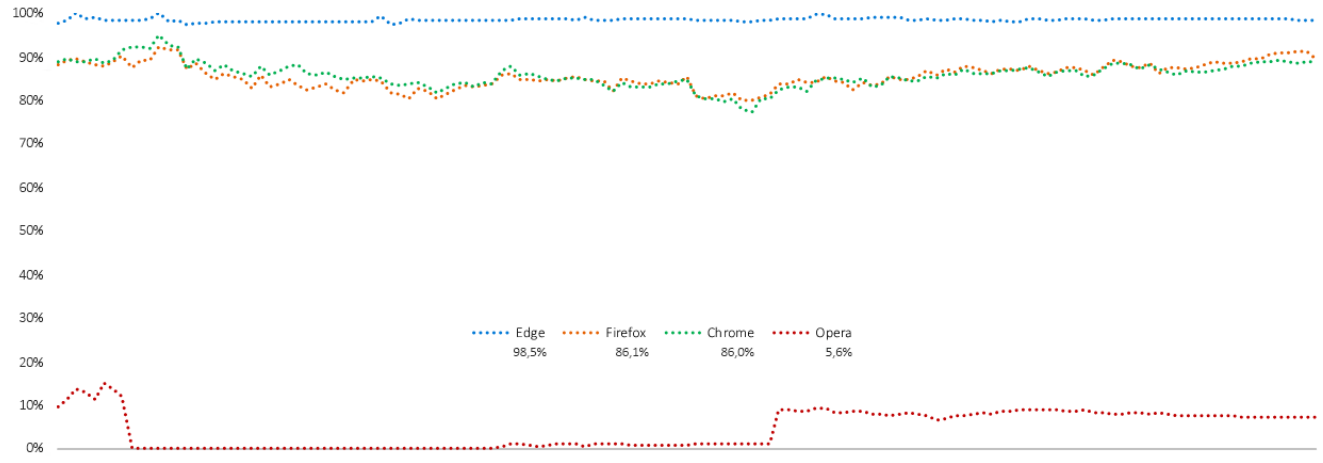


	< 24 Jam	< 48 Jam	< 72 Jam	< 96 Jam	< 120 Jam	< 144 Jam	< 168 Jam	Total
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Sistem reputasi mempersingkat waktu yang dimiliki penyerang untuk mencapai tujuan mereka dengan mencegah atau memperingatkan pengguna bahwa URL, file, atau aplikasi tersebut berbahaya. Namun, pengguna terus mengunjungi situs web baru dan mengunduh file serta menginstal aplikasi. Sistem reputasi tidak bisa begitu saja memblokir segala sesuatu yang baru. Mengetahui hal ini, kampanye malware penyerang terus berubah, dan sebagian besar dari semua serangan terjadi dalam beberapa jam pertama setelah kampanye diluncurkan. Oleh karena itu, mengklasifikasikan konten dengan cepat secara akurat adalah kunci keberhasilan perlindungan.

NSS Labs menilai kemampuan browser untuk memblokir malware secepat kami menemukannya di internet. Kami terus menguji URL, file, dan aplikasi berbahaya setiap enam jam untuk menentukan berapa lama waktu yang dibutuhkan vendor untuk menambahkan perlindungan, jika memang demikian.

Perlindungan Malware Sepanjang Waktu



Selama pengujian, malware baru terus ditambahkan. URL, file, dan aplikasi yang sudah tidak dapat dijangkau atau menghosting malware telah dihapus. Setiap titik data dihitung dari pengukuran yang direkam pada titik waktu tertentu. Jika malware diblokir sejak awal, skor browser untuk konsistensi perlindungan sepanjang waktu meningkat. Atau, jika browser tidak memblokir malware, skornya menurun.

Pengujian berdasarkan Metodologi Pengujian Browser Web v4.0 (tersedia di www.nsslabs.com).

Latar Belakang

Serangan malware rekayasa sosial (SEM) menggunakan kombinasi dinamis dari media sosial, akun email yang dibajak, pemberitahuan palsu tentang masalah komputer, dan tipuan lain untuk mendorong pengguna mengunduh malware. Penjahat cyber menggunakan akun email yang dibajak untuk mengambil keuntungan dari kepercayaan implisit antara kontak dan menipu korban agar percaya bahwa tautan ke file berbahaya dapat dipercaya. Akun media sosial yang dibajak digunakan dengan cara yang sama seperti akun email yang dibajak. Namun, dalam kasus jejaring sosial, lingkarannya menjadi lebih luas: teman atau teman dari teman berisiko ditipu.

Taktik rekayasa sosial mungkin menggunakan pesan pop-up; sebagai contoh, memberitahu pengguna bahwa aplikasi seperti Adobe Flash Player harus diinstal atau bahwa komputer mereka terinfeksi atau memerlukan pembaruan. Setelah malware terinstal, korban rentan terhadap pencurian identitas, pembobolan rekening bank, dan konsekuensi lain yang berpotensi merusak.

Perlindungan Browser Web Terhadap Malware

Untuk melindungi dari malware, browser menggunakan sistem reputasi berbasis awan yang menjelajahi internet untuk mencari situs berbahaya kemudian mengkategorikan konten yang sesuai, baik dengan menambahkannya ke daftar blokir atau daftar putih, atau dengan memberikan skor (tergantung pada pendekatan vendor).

Teknik kategorisasi tersebut dapat dilakukan secara manual atau secara otomatis. Komponen fungsional kedua dari perlindungan terhadap malware melibatkan browser web meminta informasi reputasi dari sistem reputasi berbasis awan tentang URL, file, atau aplikasi tertentu kemudian memperingatkan atau memblokir malware.

Jika hasilnya menunjukkan adanya malware, browser web mengalihkan pengguna ke pesan peringatan yang menjelaskan bahwa URL, file, atau aplikasi tersebut berbahaya. Beberapa sistem reputasi juga menyertakan konten edukasi tambahan. Sebaliknya, jika konten ditentukan sebagai "baik," browser web tidak mengambil tindakan, dan pengguna tetap tidak sadar bahwa pemeriksaan keamanan baru saja dilakukan oleh browser.

Google dan Firefox menggunakan API Penjelajahan Aman Google untuk reputasi URL dan untuk memblokir atau memperingatkan pengguna tentang mengunduh jenis file tertentu. Microsoft Edge menggunakan Microsoft Defender SmartScreen, termasuk layanan reputasi aplikasi untuk memberikan perlindungan terhadap ancaman phishing dan malware. Opera menggunakan kombinasi daftar blokir dari Netcraft,[1] PhishTank,[2] dan Metamask[3] serta daftar blokir dari Yandex.[4]

Selain itu, Microsoft Defender SmartScreen dimasukkan sebagai fitur seluruh OS dengan pembaruan Windows 10 Oktober 2017. Versi sistem operasi dari perlindungan SmartScreen adalah pengaman bagi semua browser, klien email, USB, dan aplikasi lain sebagai bagian dari perlindungan OS terhadap malware. Oleh karena itu, pengguna mendapat keuntungan dari perlindungan URL browser, perlindungan aplikasi/file browser, serta perlindungan sistem operasi.

Komposisi Pengujian–Sampel Malware

Data dalam laporan ini mencakup periode pengujian selama 34 hari antara 21 April 2020 dan 25 Mei 2020. Semua pengujian dilakukan di fasilitas pengujian NSS di Austin, TX. Selama pengujian, teknisi NSS secara rutin memantau konektivitas, untuk memastikan browser yang diuji dapat mengakses malware serta layanan reputasi di awan.

Penekanannya adalah pada kesegaran, sehingga sejumlah besar sampel dievaluasi daripada yang akhirnya disimpan sebagai bagian dari rangkaian pengujian yang dihasilkan, karena sampel baru terus ditambahkan ke pengujian dan sampel yang mati dihapus.

Jumlah Total Sampel Berbahaya yang Diuji

Sebanyak 1.844 sampel mentah dan tidak divalidasi diuji beberapa kali dengan setiap browser web, dengan total 182.676 pengujian terpisah dilakukan tanpa gangguan lebih dari 822 jam (setiap 6 jam selama 34 hari). Teknisi NSS menghapus sampel yang tidak lolos kriteria validasi, termasuk yang rusak karena eksploitasi (bukan bagian dari pengujian ini). Pada akhirnya, 1.065 sampel malware yang valid dan unik disertakan dalam 129.068 pengujian malware yang valid dan terpisah (32.267 per browser web), memberikan margin kesalahan kurang dari 2 persen (<2%) dengan tingkat kepercayaan 95%.

[1] http://www.netcraft.com/

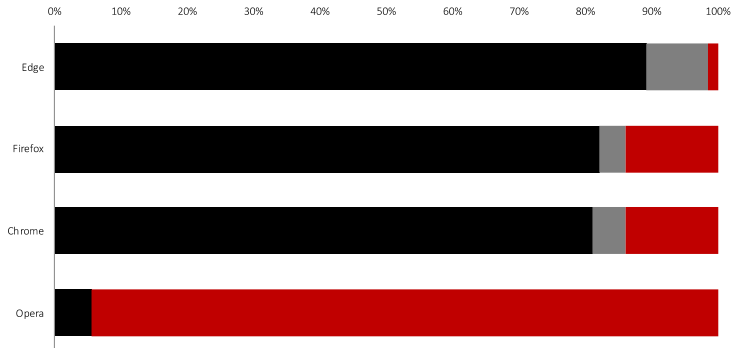
[2] http://www.phishtank.com/

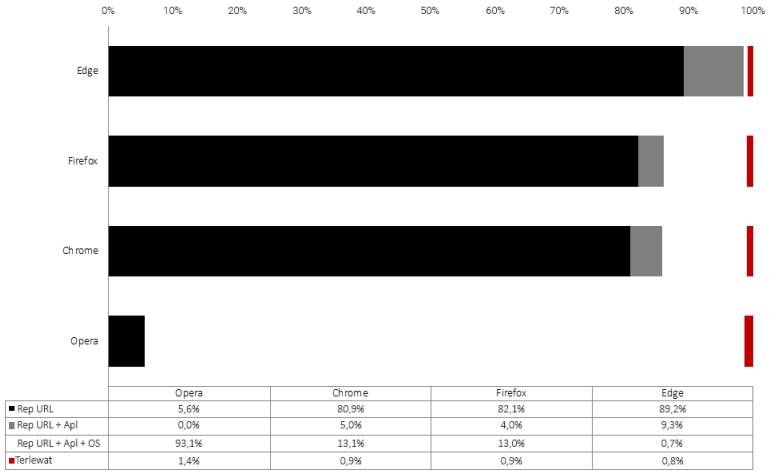
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Tingkat Pemblokiran Malware

Kemampuan untuk memperingatkan calon korban bahwa mereka akan menyimpang ke situs web berbahaya menempatkan browser pada posisi unik untuk memerangi malware yang direkayasa secara sosial. Karena situs malware memiliki masa hidup yang singkat, situs tersebut harus ditemukan, divalidasi, diklasifikasikan, dan ditambahkan ke sistem reputasi secepat mungkin. Dengan demikian, sistem reputasi yang baik harus akurat dan cepat untuk mewujudkan laju tangkap yang tinggi. Pengembang browser sangat memahami hubungan ini, dan secara substansial lebih banyak malware yang diblokir dalam 24 jam pertama pendeteksian daripada setelahnya.





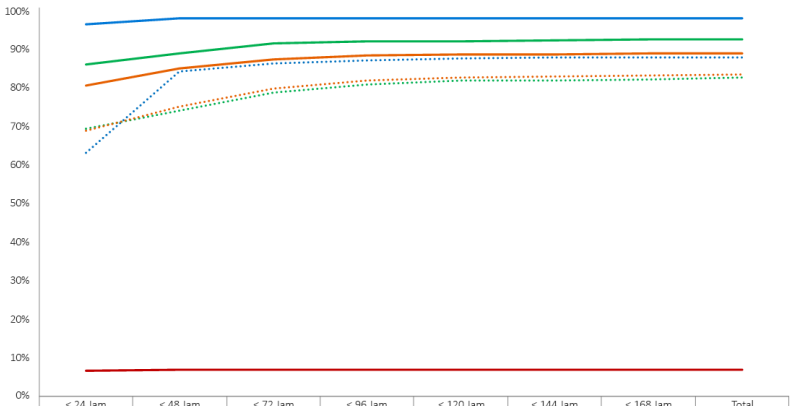
	Opera	Chrome	Firefox	Edge
Rep URL	5,6%	80,9%	82,1%	89,2%
Rep URL + Apl	0,0%	5,0%	4,0%	9,3%
Rep URL + Apl + OS	93,1%	13,1%	13,0%	0,7%
Terlewat	1,4%	0,9%	0,9%	0,8%

Teknologi perlindungan inti dalam Edge adalah SmartScreen, yang memberikan perlindungan berbasis URL dari serangan melalui layanan reputasi URL berbasis awan yang terintegrasi, serta reputasi aplikasi untuk pemblokiran file berbahaya. SmartScreen dengan reputasi aplikasi memblokir 98,5% untuk Edge. Mozilla Firefox dan Google Chrome mengunakan API Penjelajahan Aman Google. Firefox memblokir 86,1%. Google Chrome memblokir 86,0%. Opera yang menggunakan kombinasi daftar blokir dari beberapa sumber memblokir 5,6%.

Selain itu, Microsoft Defender SmartScreen memblokir 93,1% tambahan untuk Opera; 13,1% untuk Chrome; 13,0% untuk Firefox; dan 0,7% file berbahaya untuk Edge saat kami mencoba untuk mengeksekusinya.

Histogram Perlindungan Malware

Perlindungan segera terhadap malware baru sangatlah penting. Saat situs yang menjadi host malware ditemukan, mereka akan dihapus, seringkali dalam waktu yang relatif singkat. Produk yang gagal menambahkan perlindungan pada waktu yang tepat mungkin sudah terlambat untuk melawan ancaman. Histogram menunjukkan berapa lama waktu yang dibutuhkan setiap browser untuk memblokir malware setelah sampel dimasukkan ke siklus pengujian. Dalam waktu tujuh hari, tingkat perlindungan kumulatif dihitung setiap hari sampai ancaman diblokir.



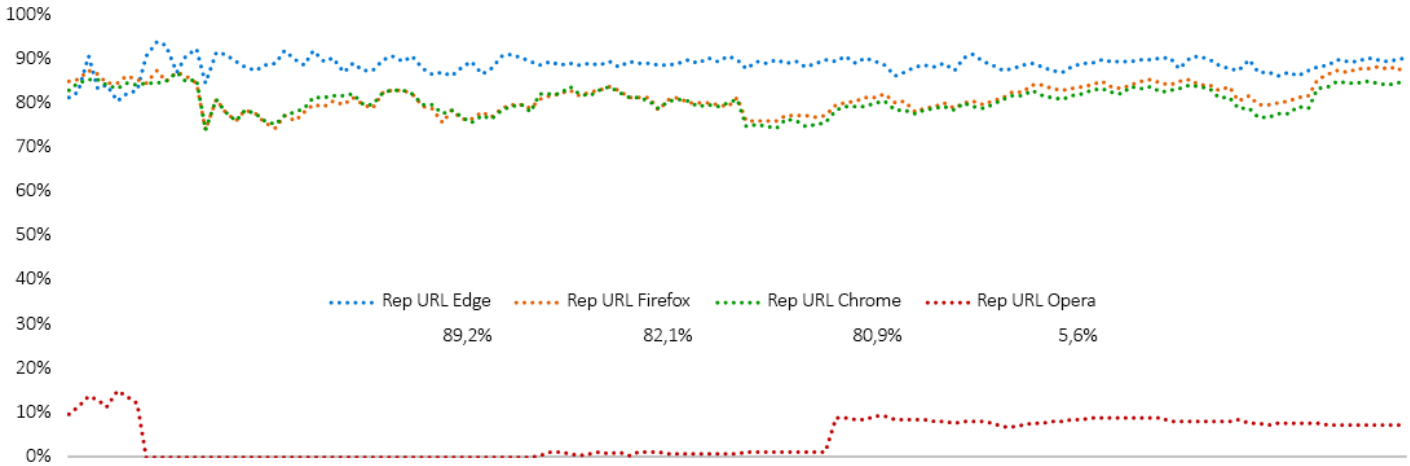
	< 24 Jam	< 48 Jam	< 72 Jam	< 96 Jam	< 120 Jam	< 144 Jam	< 168 Jam	Total
Edge dgn Rep Apl	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge dgn Rep URL	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome dgn Rep Apl	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome dgn Rep URL	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Firefox dgn Rep Apl	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Firefox dgn Rep URL	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Opera dgn Rep URL	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Selama pengujian, Microsoft Edge menunjukkan tingkat perlindungan awal 96,7% terhadap malware. Google Chrome dan Mozilla Firefox mencapai tingkat perlindungan awal masing-masing 86,2% dan 80,8% . Tingkat perlindungan awal Opera adalah 6,8%. Pada akhir hari ketujuh pengujian, semua browser web menunjukkan peningkatan perlindungan. Microsoft Edge meningkat 4,5% menjadi 98,2%. Google Chrome meningkat 6,7% menjadi 92,9%; Mozilla Firefox meningkat 8,4% menjadi 89,2%; Opera meningkat 0,1% menjadi 6,9%

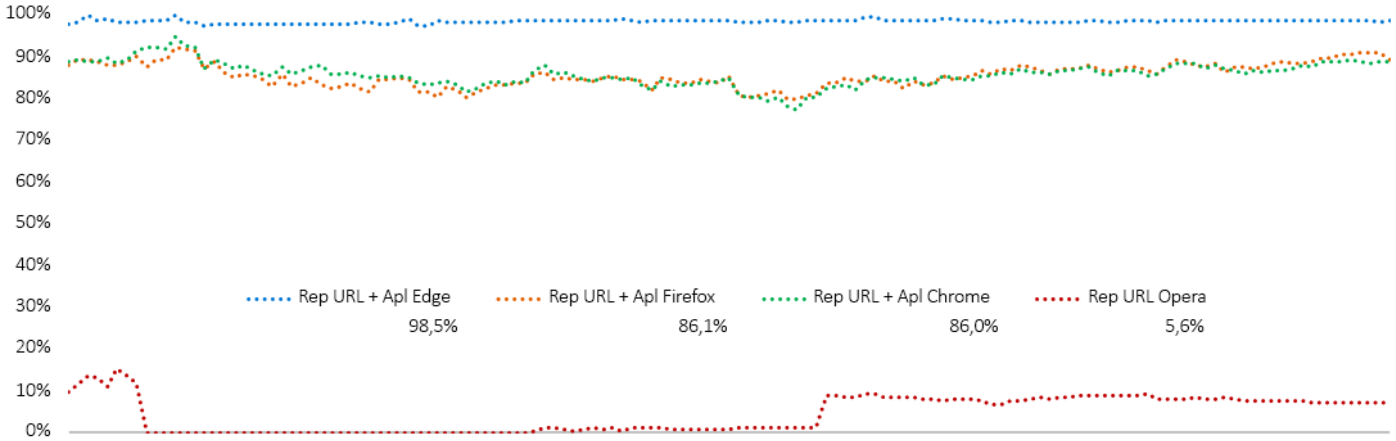
Konsistensi Perlindungan Sepanjang Waktu

Selama pengujian, malware baru terus ditambahkan. URL, file, dan aplikasi yang sudah tidak dapat dijangkau atau menghosting malware telah dihapus. Setiap titik data dihitung dari pengukuran yang direkam pada titik waktu tertentu. Jika malware diblokir sejak awal, skor browser untuk konsistensi perlindungan sepanjang waktu meningkat. Atau, jika browser tidak memblokir malware, skornya menurun.

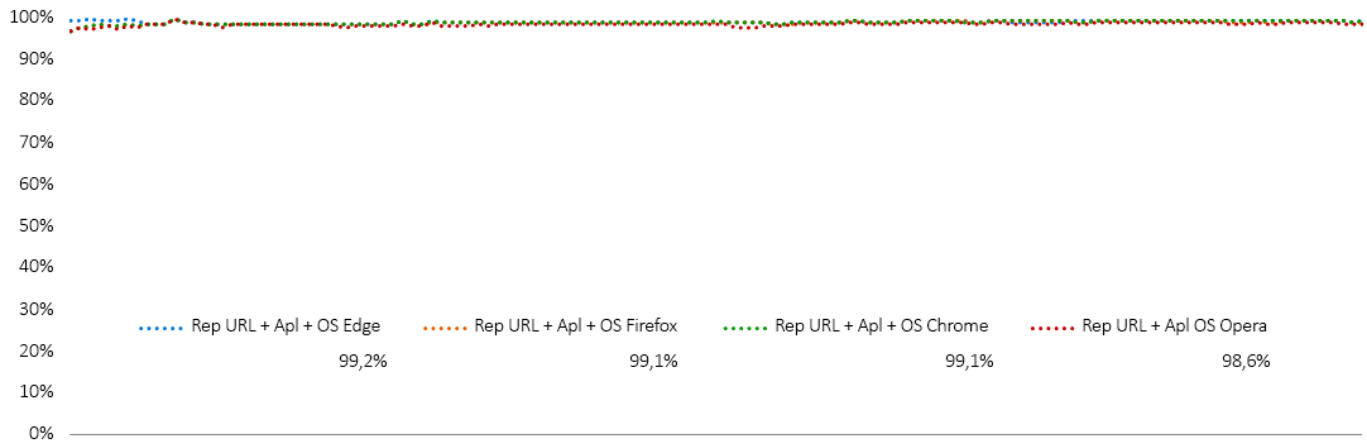
Pengujian memperlihatkan tiga lapis perlindungan: Reputasi URL, reputasi aplikasi pada browser, dan reputasi aplikasi OS. Reputasi URL menawarkan perlindungan yang cukup baik.



Lapisan pada reputasi aplikasi meningkatkan perlindungan.



Reputasi sistem operasi menawarkan perlindungan tambahan. Idealnya browser web akan memblokir malware sehingga tidak pernah mencapai sistem operasi. Namun, pengujian menunjukkan bahwa reputasi sistem operasi sangat efektif.



Lingkungan Pengujian

- BaitNET™ (NSS Labs Proprietary)
- 64-bit Microsoft Windows 10 Pro (versi 1909 Build: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Rilis kernel 4.19.0-kali5-amd64)
- VMware vCenter (Versi 6.7u2 Build 6.7.0.30000)
- VMware vSphere (Versi 6.7.0.20000)
- VMware ESXi (Versi 6.7u3 Build 14320388)
- VMware Tools 10.3.5
- Wireshark versi 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (Build 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Produk yang Diuji

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

Penulis

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Metodologi Tes

Metodologi Pengujian NSS Labs Web Browser Security (WBS) v4.0 tersedia di www.nsslabs.com.

Informasi Kontak

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com