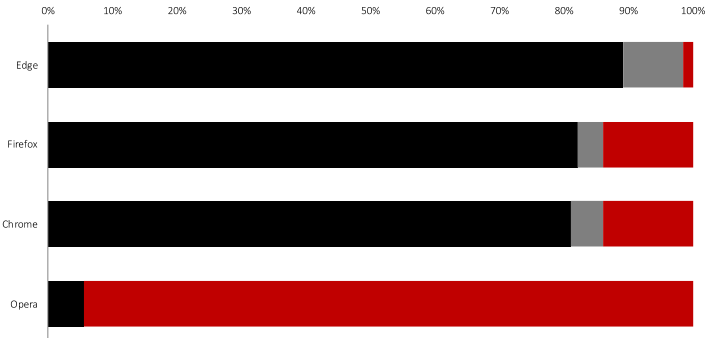
II kw. 2020 RAPORT Z BADANIA PORÓWNAWCZEGO

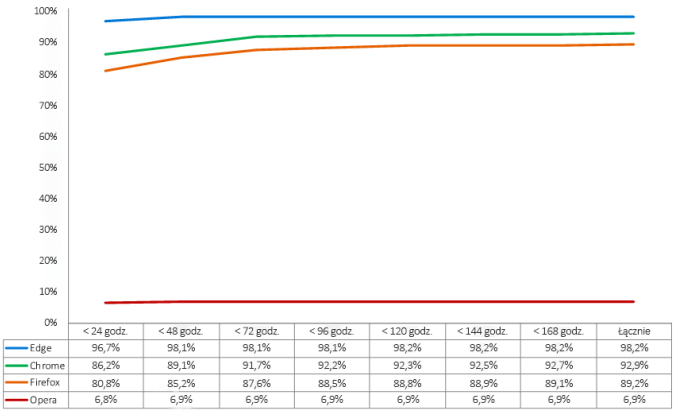
Przegląd

W drugim kwartale 2020 roku firma NSS Labs przeprowadziła niezależny test ochrony przed złośliwym oprogramowaniem oferowanej przez przeglądarki internetowe: 32 267 dyskretnych testów (na przeglądarkę internetową) przy użyciu 1065 unikatowych próbek w ciągu 34 dni. Aby chronić przed złośliwym oprogramowaniem, Microsoft Edge korzysta z funkcji Microsoft Defender SmartScreen, Google Chrome i Mozilla Firefox korzystają z interfejsu API usługi Google Safe Browsing, a Opera korzysta z usług Yandex.

Microsoft Edge zaoferował największą ochronę, blokując 98,5% złośliwego oprogramowania, zapewniając jednocześnie najwyższy wskaźnik ochrony przez zero godzin (96,7%). Firefox zapewnił drugą najwyższą ochronę, blokując średnio 86,1%, a następnie Google Chrome z wynikiem 86,0%. Opera zablokowała 5,6%.



Podsumowanie wyników

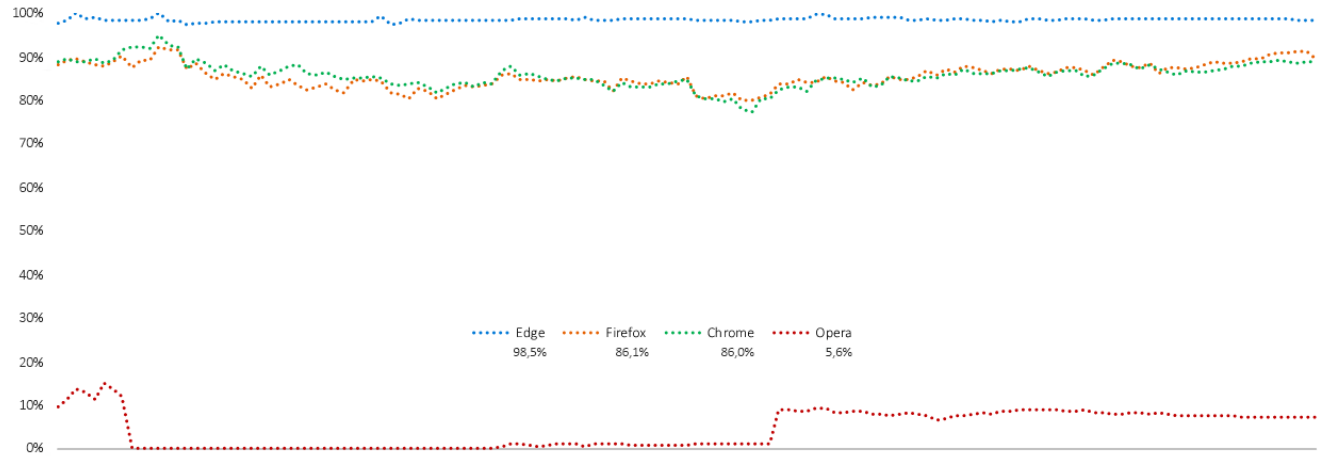


	< 24 godz.	< 48 godz.	< 72 godz.	< 96 godz.	< 120 godz.	< 144 godz.	< 168 godz.	Łącznie
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Systemy reputacji skracają czas, jakim dysponują atakujący na osiągnięcie swoich celów, ostrzegając użytkowników, że adres URL, plik lub aplikacja jest niebezpieczna. Jednak użytkownicy stale odwiedzają nowe witryny internetowe, pobierają pliki i instalują aplikacje. Systemy reputacji nie mogą po prostu blokować wszystkiego, co nowe. Z tego powodu kampanie złośliwego oprogramowania atakujących stale się zmieniają, a większość wszystkich ataków ma miejsce w ciągu pierwszych kilku godzin po rozpoczęciu kampanii. Dlatego szybkie i dokładne klasyfikowanie treści jest kluczem do skutecznej ochrony.

NSS Labs ocenił zdolność przeglądarek do blokowania złośliwego oprogramowania w tej samej chwili, gdy są znajdowane w Internecie. Kontynuowaliśmy testowanie złośliwych adresów URL, plików i aplikacji co sześć godzin, aby określić, ile czasu zajęło dostawcy dodanie ochrony, jeśli w ogóle to zrobił.

Ochrona przed złośliwym oprogramowaniem na przestrzeni czasu



W trakcie całego testu stale dodawano nowe złośliwe oprogramowanie. Adresy URL, pliki i aplikacje, które były już niedostępne lub nie zawierały już złośliwego oprogramowania, zostały usunięte. Każdy punkt danych jest obliczany na podstawie pomiarów zarejestrowanych w określonym momencie. Jeśli złośliwe oprogramowanie zostało wcześnie zablokowane, wynik przeglądarki pod względem spójności ochrony na przestrzeni czasu poprawił się. Alternatywnie, jeśli przeglądarka nie zablokowała złośliwego oprogramowania, wynik spadł.

Testy oparto na metodologii testowania przeglądarek internetowych w wersji 4.0 (dostępnej pod adresem www.nsslabs.com).

Tło

Ataki stosujące złośliwe oprogramowanie oparte na inżynierii społecznej (SEM) wykorzystują dynamiczne połączenie mediów społecznościowych, przejętych kont e-mail, fałszywych powiadomień o problemach z komputerem oraz innych oszustw, aby zachęcić użytkowników do pobrania złośliwego oprogramowania. Cyberprzestępcy używają przejętych kont e-mail, aby wykorzystać bezgraniczne zaufanie między osobami z listy kontaktów i podstępem przekonać swoje ofiary, że linki do złośliwych plików są godne zaufania. Przejęte konta w mediach społecznościowych są używane w taki sam sposób, jak przejęte konta e-mail. W przypadku sieci społecznościowych krąg się jednak poszerza: znajomi, a nawet znajomi znajomych ryzykują, że zostaną oszukani.

Taktyki inżynierii społecznej mogą wykorzystywać wyskakujące komunikaty, na przykład informujące użytkowników, że należy zainstalować aplikacje takie jak Adobe Flash Player lub że ich komputery są zainfekowane lub wymagają aktualizacji. Po zainstalowaniu złośliwego oprogramowania ofiary są narażone na kradzież tożsamości, włamanie na konto bankowe i inne bardzo negatywne konsekwencje.

Ochrona przeglądarek internetowych przed złośliwym oprogramowaniem

Aby chronić się przed złośliwym oprogramowaniem, przeglądarki używają opartych na chmurze systemów reputacji, które przeszukują Internet w poszukiwaniu złośliwych witryn, a następnie odpowiednio kategoryzują zawartość, dodając ją do list zablokowanych lub białych list lub przypisując jej ocenę (w zależności od podejścia dostawcy).

Te techniki kategoryzacji mogą być wykonywane ręcznie lub automatycznie. Drugi funkcjonalny składnik ochrony przed złośliwym oprogramowaniem polega na tym, że przeglądarka internetowa żąda informacji o reputacji z opartych na chmurze systemów reputacji na temat określonych adresów URL, plików lub aplikacji, a następnie ostrzega przed złośliwym oprogramowaniem lub blokuje je.

Jeśli wyniki wskazują, że obecne jest złośliwe oprogramowanie, przeglądarka internetowa przekierowuje użytkownika do komunikatu ostrzegawczego wyjaśniającego, że adres URL, plik lub aplikacja jest złośliwa. Niektóre systemy reputacji zawierają również dodatkowe treści edukacyjne. I odwrotnie, jeśli treść zostanie określona jako „dobra", przeglądarka internetowa nie podejmuje żadnych działań, a użytkownik pozostaje nieświadomy, że przeglądarka właśnie przeprowadziła kontrolę bezpieczeństwa.

Google i Firefox używają interfejsu API usługi Google Safe Browsing zarówno do oceny reputacji adresów URL, jak i do blokowania określonych typów plików lub ostrzegania użytkowników przed ich pobraniem. Microsoft Edge używa funkcji Microsoft Defender SmartScreen, w tym usługi reputacyjnej aplikacji, aby zapewnić ochronę przed zagrożeniami ze strony phishingu i złośliwego oprogramowania. Opera używa kombinacji list blokowanych od Netcraft,[1] PhishTank[2] i Metamask,[3] a także listy blokowanych złośliwego oprogramowania od Yandex.[4]

Ponadto Microsoft Defender SmartScreen stał się jedną z funkcji systemu operacyjnego w aktualizacji systemu Windows 10 z października 2017 r. Wersja ochrony SmartScreen dla systemu operacyjnego stanowi zabezpieczenie dla wszystkich przeglądarek, klientów poczty e-mail, urządzeń USB i innych aplikacji w ramach ochrony systemu operacyjnego przed złośliwym oprogramowaniem. Dlatego użytkownicy korzystają z ochrony adresów URL przeglądarki, ochrony aplikacji/plików przeglądarki, a także ochrony systemu operacyjnego.

Skład testu — Próbki złośliwego oprogramowania

Dane zawarte w tym raporcie obejmują okres testowy trwający 34 dni od 21 kwietnia 2020 r. do 25 maja 2020 r. Wszystkie testy przeprowadzono w ośrodku testowym NSS w Austin w stanie Teksas. Podczas testu inżynierowie NSS rutynowo monitorowali łączność, aby upewnić się, że testowane przeglądarki mogą uzyskać dostęp do złośliwego oprogramowania, a także do usług reputacyjnych w chmurze.

Nacisk położono na świeżość, dlatego oceniono większą liczbę próbek niż ostatecznie zatrzymano w ramach powstałego zestawu testowego, ponieważ do testu ciągle dodawano nowe próbki i usuwano martwe próbki.

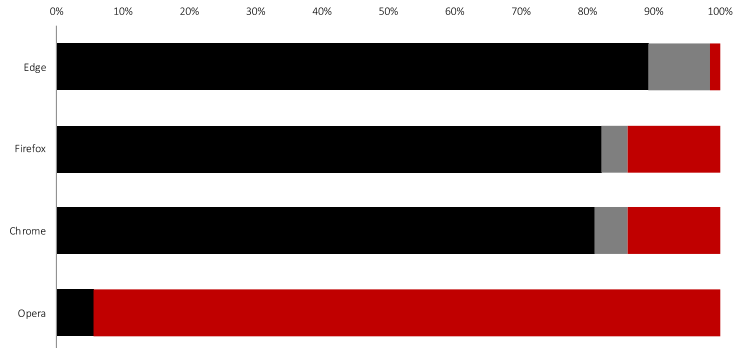
Całkowita liczba przetestowanych szkodliwych próbek

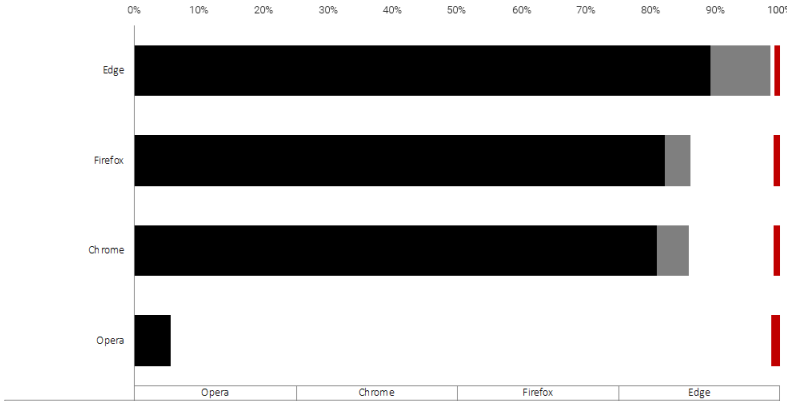
W sumie 1844 pierwotnych, niezatwierdzonych próbek przetestowano wielokrotnie z każdą przeglądarką internetową, co dało w sumie 182 676 dyskretnych testów przeprowadzonych bez przerwy w ciągu 822 godzin (co 6 godzin przez 34 dni). Inżynierowie NSS usunęli próbki, które nie spełniały kryteriów walidacji, w tym te skażone programami wykorzystującymi luki (nie są częścią tego testu). Ostatecznie 1065 unikatowych, prawidłowych próbek złośliwego oprogramowania zostało uwzględnionych w 129 068 dyskretnych, prawidłowych testach złośliwego oprogramowania (32 267 na przeglądarkę internetową), zapewniając margines błędu mniejszy niż 2 procent (<2%) przy poziomie ufności 95%.

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

Współczynnik blokowania złośliwego oprogramowania

Zdolność do ostrzegania potencjalnych ofiar, że zaraz wejdą na złośliwą witrynę, stawia przeglądarki internetowe w wyjątkowej pozycji do zwalczania złośliwego oprogramowania poddanego inżynierii społecznej. Ponieważ witryny zawierające złośliwe oprogramowanie istnieją przez krótki czas, ważne jest, aby jak najszybciej wykryć, zweryfikować, sklasyfikować i dodać witrynę do systemu reputacji. Dobry system reputacji musi być zarówno dokładny, jak i szybki, aby osiągnąć wysokie częstotliwości wykryć. Twórcy przeglądarek bardzo dobrze rozumieją ten związek i znacznie więcej złośliwego oprogramowania jest blokowane w ciągu pierwszych 24 godzin wykrycia niż po tym czasie.





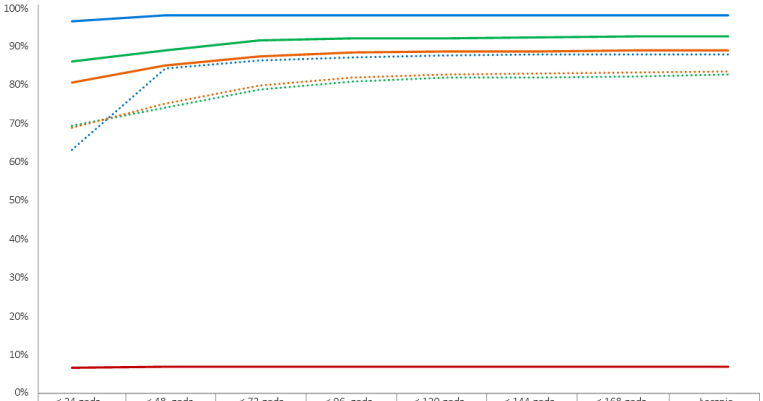
	Opera	Chrome	Firefox	Edge
Spr. reputacji URL	5,6%	80,9%	82,1%	89,2%
Spr. reputacji URL i aplikacji	0,0%	5,0%	4,0%	9,3%
Spr. reputacji URL i aplikacji (internetowych i systemowych)	93,1%	13,1%	13,0%	0,7%
Pominięte	1,4%	0,9%	0,9%	0,8%

Podstawową technologią ochrony w przeglądarce Edge jest funkcja SmartScreen, która zapewnia opartą na adresach URL ochronę przed atakami za pośrednictwem zintegrowanej, opartej na chmurze usługi reputacji adresów URL, a także reputację aplikacji pod kątem blokowania złośliwych plików. Funkcja SmartScreen z reputacją aplikacji zablokowała 98,5% w przypadku przeglądarki Edge. Mozilla Firefox i Google Chrome używają interfejsu API usługi Safe Browsing. Firefox zablokował 86,1%. Google Chrome zablokował 86,0%. Opera, która korzysta z kombinacji list blokowanych z kilku źródeł, zablokowała 5,6%.

Ponadto, kiedy próbowaliśmy uruchomić złośliwe pliki, funkcja Microsoft Defender SmartScreen zablokowała dodatkowe 93,1% w przypadku przeglądarki Opera, 13,1% w przypadku przeglądarki Chrome, 13,0% w przypadku przeglądarki Firefox i 0,7% w przypadku przeglądarki Edge.

Histogram ochrony przed złośliwym oprogramowaniem

Natychmiastowa ochrona przed nowym złośliwym oprogramowaniem ma kluczowe znaczenie. Gdy wykrywane są witryny zawierające złośliwe oprogramowanie, są one usuwane, często w stosunkowo krótkim czasie. Produkty, które nie dodają ochrony w odpowiednim czasie, mogą nie zdążyć z przeciwdziałaniem zagrożeniu. Histogram pokazuje, ile czasu zajęło każdej przeglądarce zablokowanie złośliwego oprogramowania po wprowadzeniu próbki do cyklu testowego. W siedmiodniowym okresie skumulowane wskaźniki ochrony są obliczane każdego dnia do momentu zablokowania zagrożeń.



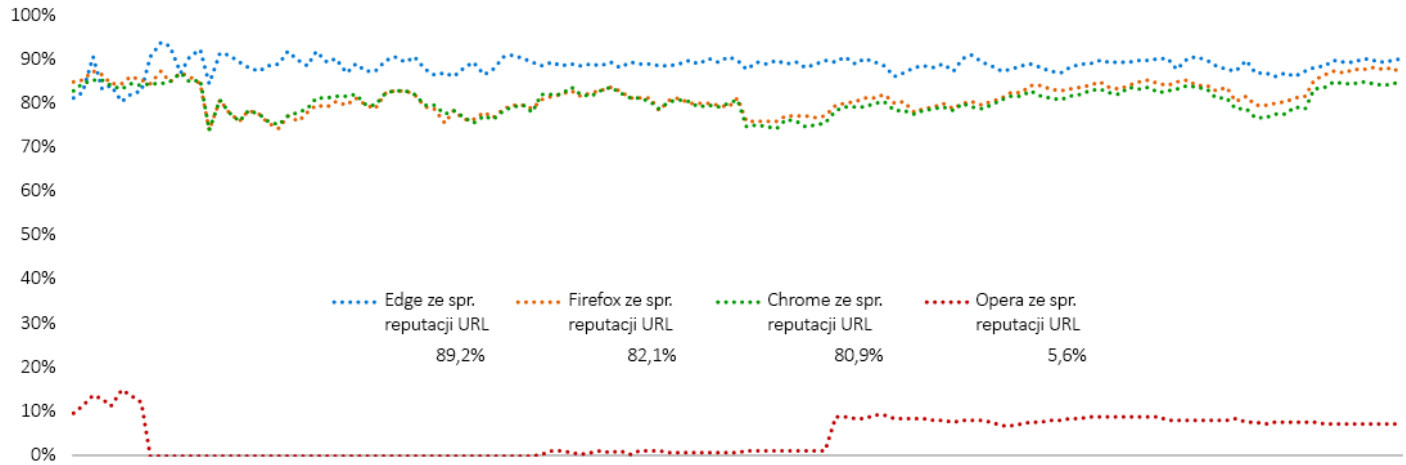
	< 24 godz.	< 48 godz.	< 72 godz.	< 96 godz.	< 120 godz.	< 144 godz.	< 168 godz.	Łącznie
Edge ze spr. reputacji aplikacji	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge ze spr. reputacji URL	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome ze spr. reputacji aplikacji	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome ze spr. reputacji URL	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Firefox ze spr. reputacji aplikacji	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Firefox ze spr. reputacji URL	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Opera ze spr. reputacji URL	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Podczas testu Microsoft Edge wykazał początkowy współczynnik ochrony przed złośliwym oprogramowaniem na poziomie 96,7%. Google Chrome i Mozilla Firefox osiągnęły początkowy współczynnik ochrony odpowiednio 86,2% i 80,8%. Początkowy współczynnik ochrony przeglądarki Opera wyniósł 6,8%. Pod koniec siódmego dnia testów wszystkie przeglądarki internetowe odnotowały wzrost poziomu ochrony. W przypadku Microsoft Edge nastąpił wzrost o 4,5% do 98,2%. Google Chrome — wzrost o 6,7% do 92,9%; Mozilla Firefox — wzrost o 8,4% do 89,2%; Opera — wzrost o 0,1% do 6,9%

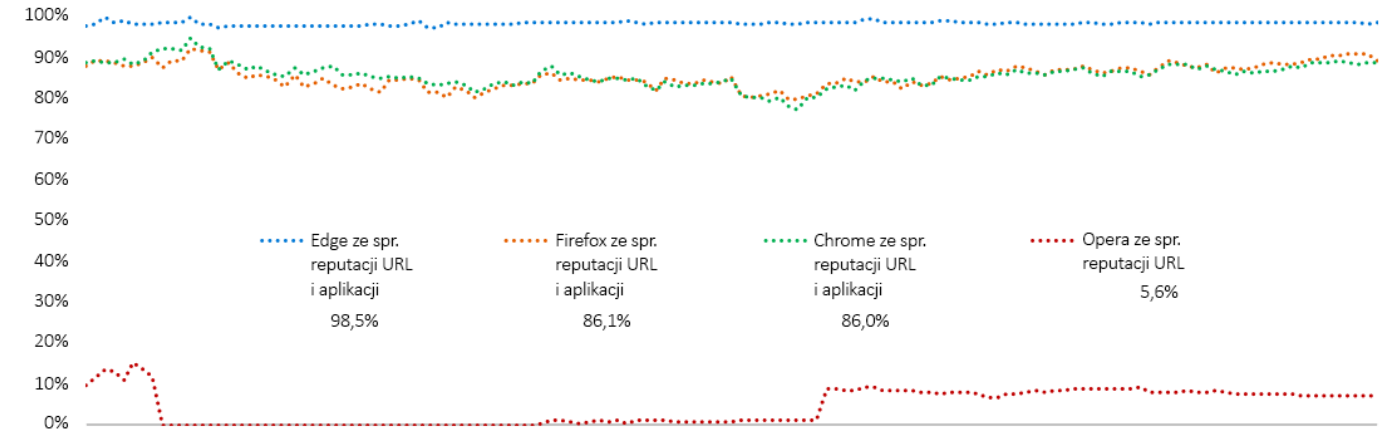
Spójność ochrony na przestrzeni czasu

W trakcie całego testu stale dodawano nowe złośliwe oprogramowanie. Adresy URL, pliki i aplikacje, które były już niedostępne lub nie zawierały już złośliwego oprogramowania, zostały usunięte. Każdy punkt danych jest obliczany na podstawie pomiarów zarejestrowanych w określonym momencie. Jeśli złośliwe oprogramowanie zostało wcześnie zablokowane, wynik przeglądarki pod względem spójności ochrony na przestrzeni czasu poprawił się. Alternatywnie, jeśli przeglądarka nie zablokowała złośliwego oprogramowania, wynik spadł.

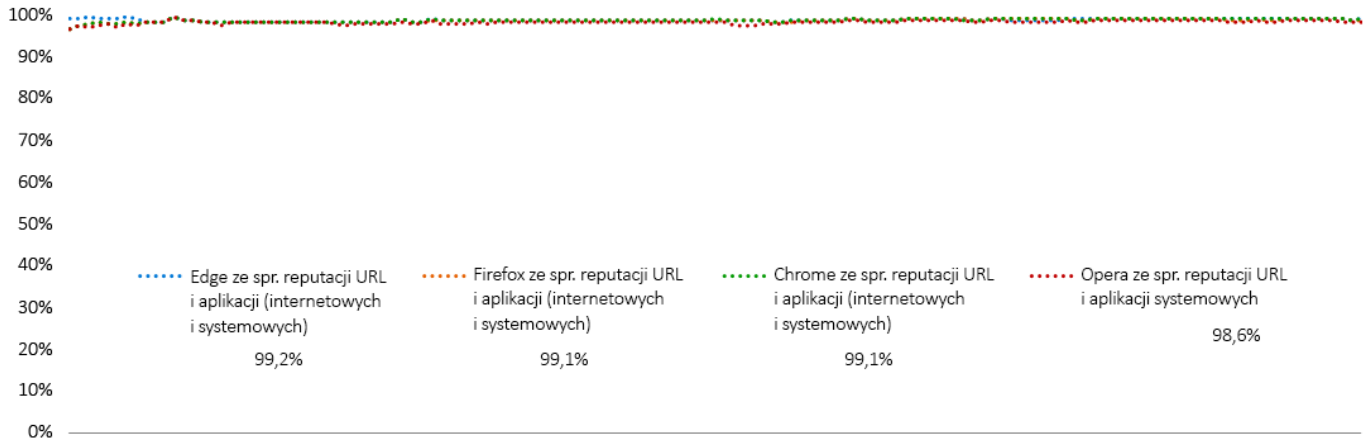
Testy ujawniły trzy warstwy ochrony: Reputacja adresu URL, reputacja aplikacji w przeglądarce i reputacja aplikacji systemu operacyjnego. Reputacja adresu URL oferowała dość dobrą ochronę.



Nakładanie warstw na reputację aplikacji zwiększyło ochronę.



Reputacja systemu operacyjnego oferowała jeszcze dodatkową ochronę. Idealnie byłoby, gdyby przeglądarka internetowa blokowała złośliwe oprogramowanie, aby nigdy nie dotarło do systemu operacyjnego. Jednak testy wykazały, że reputacja systemu operacyjnego była bardzo skuteczna.



Środowisko testowe

- BaitNET™ (NSS Labs Proprietary)
- 64-bitowy system Microsoft Windows 10 Pro (wersja 1909 kompilacja: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (wydanie jądra 4.19.0-kali5-amd64)
- VMware vCenter (wersja 6.7u2 kompilacja 6.7.0.30000)
- VMware vSphere (wersja 6.7.0.20000)
- VMware ESXi (wersja 6.7u3 kompilacja 14320388)
- VMware Tools 10.3.5
- Wireshark w wersji 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (kompilacja 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Testowane produkty

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

Autorzy

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Metodologia testów

Metodologia testów NSS Labs Web Browser Security (WBS) w wersji 4.0 jest dostępna pod adresemwww.nsslabs.com.

Dane kontaktowe

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com