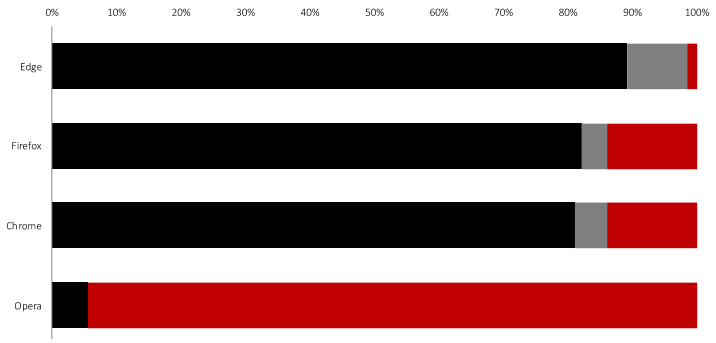
K2 2020 KOMPARATIVNI IZVEŠTAJ O TESTIRANJU

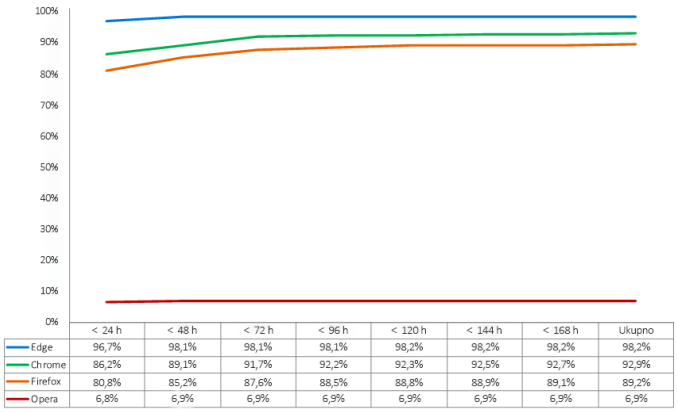
Pregled

Tokom K2 2020. kompanija NSS Labs je obavila nezavisno testiranje zaštite od malvera koju pružaju veb pregledači: 32.267 diskretnih testova (po veb pregledaču) koji koriste 1065 jedinstvenih uzoraka tokom 34 dana. Da bi štitio od malvera, Microsoft Edge koristi SmartScreen filter Microsoft zaštitnika, Google Chrome i Mozilla Firefox koriste Google API za bezbedno pregledanje, a Opera koristi Yandex.

Microsoft Edge je ponudio najbolju zaštitu, blokirao je 98,5% malvera i istovremeno obezbedio najvišu stopu zaštite u zakazano vreme (96,7%). Firefox je pružio drugu po redu najbolju zaštitu, u proseku je blokirao 86,1%, a iza njega sledi Google Chrome sa 86,0%. Pregledač Opera je blokirao 5,6%.



Rezime rezultata

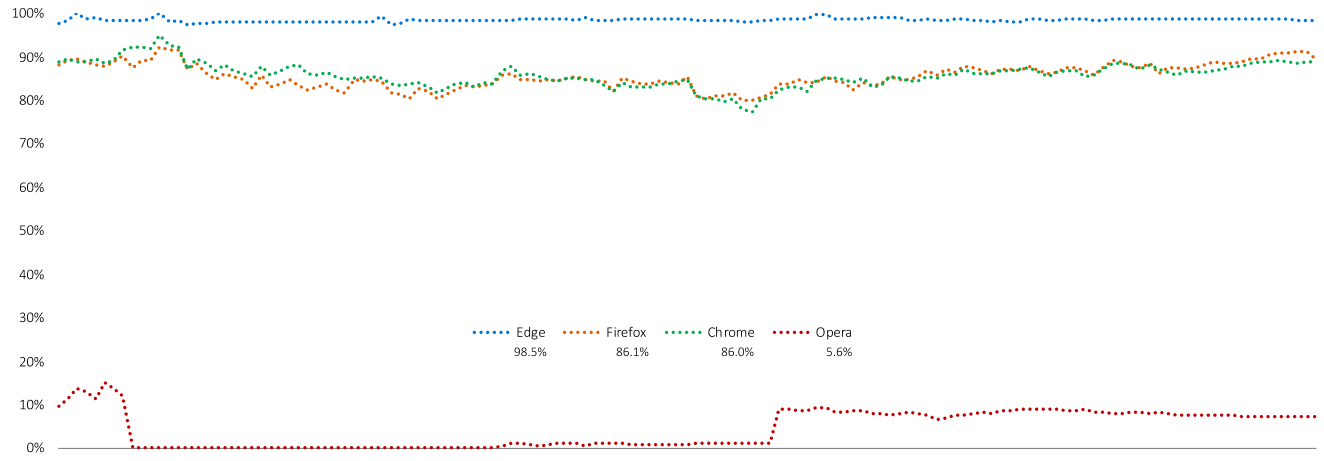


	< 24 h	< 48 h	< 72 h	< 96 h	< 120 h	< 144 h	< 168 h	Ukupno
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Sistemi reputacije skraćuju vreme koje je napadačima potrebno da ostvare ciljeve tako što sprečavaju ili upozoravaju korisnike da su URL adresa, datoteka ili aplikacija opasne. Međutim, korisnici stalno posećuju nove veb sajtove, preuzimaju datoteke i instaliraju aplikacije. Sistemi reputacije ne mogu prosto da blokiraju sve što je novo. Znajući ovo, kampanje malvera napadača se stalno menjaju, a većina svih napada se dešava u prvih nekoliko sati nakon pokretanja kampanje. Zato je precizno i brzo klasifikovanje sadržaja od ključnog značaja za uspešnu zaštitu.

Kompanija NSS Labs je procenila mogućnost pregledača da blokiraju malver čim ga pronađemo na internetu. Nastavili smo da testiramo zlonamerne URL adrese, datoteke i aplikacije na svakih šest sati da bismo utvrdili koliko je vremena potrebno da proizvođač doda zaštitu, ako je uopšte i dodaje.

Zaštita malvera tokom vremena



Tokom celokupnog testiranja neprekidno se dodavao novi malver. URL adrese, datoteke i aplikacije koje više nisu bile dostupne ili više nisu hostovale malver su uklonjene. Svaka tačka podataka se izračunava na osnovu merenja snimljenih u određenom trenutku. Ako je malver blokiran u početku, ocena doslednosti zaštite pregledača se poboljšala tokom vremena. U suprotnom, ako pregledač nije blokirao malver, ocena se smanjila.

Testiranje je zasnovano na Metodologiji testiranja veb pregledača v4.0 (dostupnoj na adresi www.nsslabs.com).

Pozadina

Napadi malvera za društveni inženjering (SEM) koriste dinamičku kombinaciju društvenih mreža, ukradenih naloga e-pošte, lažnih obaveštenja o problemima na računaru i druge obmane koje podstiču korisnike da preuzmu malver. Kibernetički kriminalci koriste ukradene naloge e-pošte da bi iskoristili implicitno poverenje između kontakata i obmanjuju žrtve da poveruju da su veze ka zlonamernim datotekama pouzdane. Ukradeni nalozi na društvenim mrežama koriste se na isti način kao ukradeni nalozi e-pošte. Međutim, u slučaju društvenih mreža, krug postaje širi: prijatelji i čak i prijatelji prijatelja dolaze pod rizik da budu prevareni.

Taktike društvenog inženjeringa mogu koristiti iskačuće poruke, na primer, mogu da savetuju korisnike da treba da instaliraju aplikacije kao što je Adobe Flash Player ili im govore da su njihovi računari zaraženi ili zahtevaju ažuriranje. Kada se malver instalira, žrtve su ranjive na krađu identiteta, ugrožavanje računa u banci i druge potencijalno katastrofalne posledice.

Zaštita veb pregledača od malvera

Da bi štitili od malvera, pregledači koriste sisteme reputacije zasnovane na tehnologiji oblaka koji na internetu pretražuju zlonamerne veb sajtove, a zatim u skladu sa tim kategorizuju sadržaj njegovim dodavanjem na liste blokiranog sadržaja ili bele liste, odnosno davanjem ocene sadržaju (u zavisnosti od pristupa proizvođača).

Ove tehnike kategorizacije mogu da se izvrše ručno ili automatski. Druga funkcionalna komponenta zaštite od malvera uključuje to da veb pregledač od sistema reputacije zasnovanih na tehnologiji oblaka zahteva informacije o reputaciji u vezi sa određenim URL adresama, datotekama ili aplikacijama, a zatim upozorava o malveru ili ga blokira.

Ako rezultati ukazuju na to da je malver prisutan, veb pregledač preusmerava korisnika na poruku upozorenja koja objašnjava da su URL adresa, datoteka ili aplikacija zlonamerne. Neki sistemi reputacije takođe uključuju dodatan obrazovni sadržaj. U suprotnom slučaju, ako se utvrdi da je sadržaj „dobar“, veb pregledač ne radi ništa i korisnik neće znati da je pregledač upravo izvršio bezbednosnu proveru.

Google i Firefox koriste Google API za bezbedno pregledanje za reputaciju URL adresa, kao i za blokiranje ili upozoravanje korisnika o preuzimanju određenih tipova datoteka. Microsoft Edge koristi SmartScreen filter Microsoft zaštitnika, uključujući uslugu reputacije aplikacija kako bi pružio zaštitu od phishinga i pretnji malvera. Opera koristi kombinaciju lista blokiranog sadržaja iz usluga Netcraft,[1] PhishTank[2] i Metamask[3], kao i listu blokiranog malvera iz usluge Yandex.[4]

Pored toga, SmartScreen filter Microsoft zaštitnika je uključen kao funkcija u celom operativnom sistemu u Windows 10 ispravci iz oktobra 2017. Verzija operativnog sistema SmartScreen zaštite predstavlja potporu za sve pregledače, klijente e-pošte, USB i druge aplikacije u sklopu zaštite operativnog sistema od malvera. Stoga korisnici imaju koristi od zaštite URL adresa pregledača, zaštite aplikacija/datoteka pregledača, kao i od zaštite operativnog sistema.

Sastav testa – Uzorci malvera

Podaci u ovom izveštaju prikupljeni su tokom perioda testiranja od 34 dana između 21. aprila 2020. i 25. maja 2020. Celokupno testiranje je izvršeno u NSS objektu za testiranja u Ostinu u Teksasu. Tokom testiranja, NSS inženjeri su rutinski nadgledali mogućnost povezivanja da bi se uverili da testirani pregledači mogu da pristupe malveru, kao i uslugama reputacije u oblaku.

Naglasak je bio na svežini i zato je procenjen veći broj uzoraka od onog koji je na kraju zadržan kao dobijeni skup za testiranje pošto su se novi uzorci stalno dodavali u test, a mrtvi uzorci su se uklanjali.

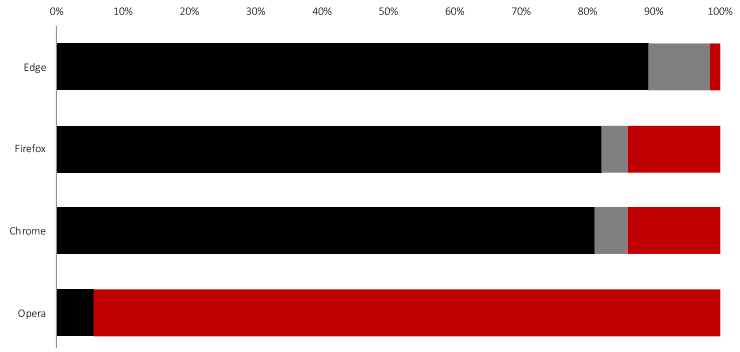
Ukupan broj testiranih zlonamernih uzoraka

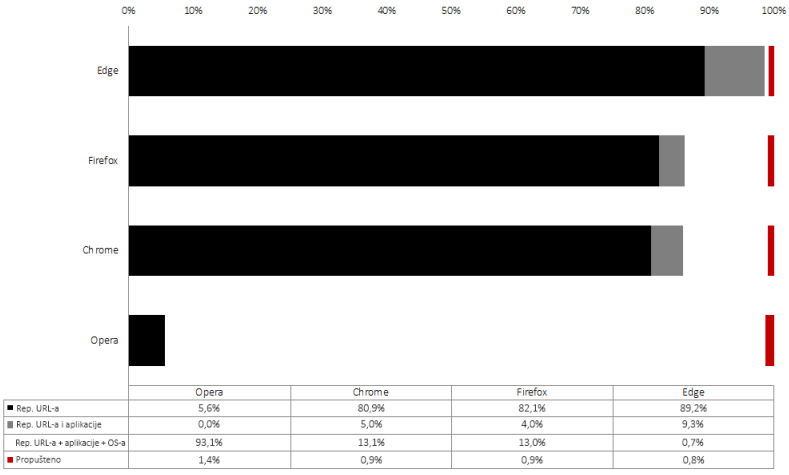
U svakom pregledaču su više puta testirana ukupno 1844 neobrađena uzorka čija valjanost nije proverena, za ukupno 182.676 diskretnih testova obavljenih bez prekida tokom 822 sata (na svakih 6 sati tokom 34 dana). NSS inženjeri su uklonili uzorke koji nisu prošli kriterijum provere valjanosti, uključujući one koji su oštećeni zloupotrebom (nisu deo ovog testa). Na kraju je 1065 jedinstvenih, važećih uzoraka malvera uključeno u 129.068 diskretnih, važećih testova malvera (32.267 po veb pregledaču), što je obezbedilo marginu greške manju od 2 procenta (<2%) uz stepen pouzdanosti od 95%.

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

Stopa blokiranja malvera

Mogućnost upozoravanja potencijalnih žrtvi da će zalutati na zlonamerni veb sajt stavlja veb pregledače u jedinstven položaj za borbu protiv malvera za društveni inženjering. Pošto sajtovi sa malverom imaju kratak vek trajanja, neophodno je da se sajt što pre otkrije, da mu se proveri valjanost, da se klasifikuje i doda u sistem reputacije. Kao takav, dobar sistem reputacije mora da bude precizan i brz da bi se ostvarile velike stope hvatanja. Projektanti pregledača jasno razumeju ovaj odnos i znatno više malvera se blokira u prva 24 sata otkrivanja nego nakon toga.





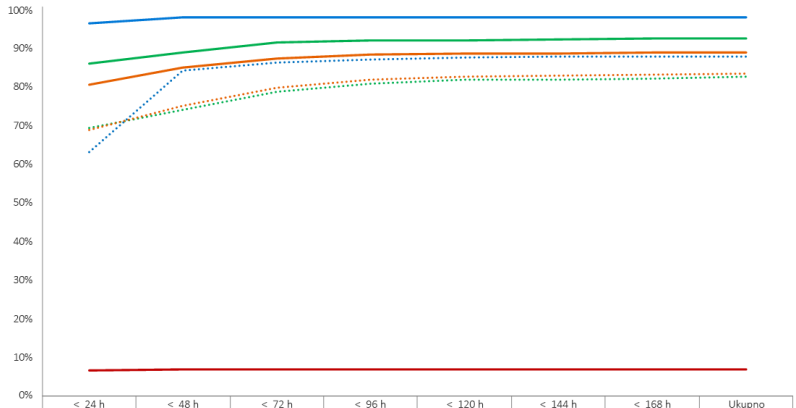
	Opera	Chrome	Firefox	Edge
Rep. URL-a	5,6%	80,9%	82,1%	89,2%
Rep. URL-a i aplikacije	0,0%	5,0%	4,0%	9,3%
Rep. URL-a + aplikacije + OS-a	93,1%	13,1%	13,0%	0,7%
Propušteno	1,4%	0,9%	0,9%	0,8%

Osnovna tehnologija zaštite u okviru pregledača Edge je SmartScreen, koji pruža zaštitu od napada zasnovanu na URL adresama putem integrisane usluge reputacije URL adresa zasnovane na tehnologiji oblaka, kao i putem reputacije aplikacija za blokiranje zlonamernih datoteka. SmartScreen sa reputacijom aplikacija blokirao je 98,5% za Edge. Mozilla Firefox i Google Chrome koriste API za bezbedno pregledanje. Firefox je blokirao 86,1%. Google Chrome je blokirao 86,0%. Pregledač Opera, koji koristi kombinaciju lista blokiranog sadržaja iz nekoliko izvora, blokirao je 5,6%.

Pored toga, SmartScreen filter Microsoft zaštitnika blokirao je dodatnih 93,1% za pregledač Opera, 13,1% za Chrome, 13,0% za Firefox i 0,7% zlonamernih datoteka za Edge kada smo pokušali da ih izvršimo.

Histogram zaštite od malvera

Trenutna zaštita od novog malvera je od kritičnog značaja. Čim se sajtovi koji hostuju malver otkriju, oni se gase, često za relativno kratko vreme. Proizvodi koji ne uspeju da dodaju zaštitu na vreme mogu zakasniti sa otklanjanjem pretnje. Histogram prikazuje koliko je vremena bilo potrebno svakom pregledaču da blokira malver kada je uzorak ubačen u ciklus testiranja. U periodu od sedam dana, kumulativne stope zaštite su se izračunavale svaki dan dok pretnje nisu bile blokirane.



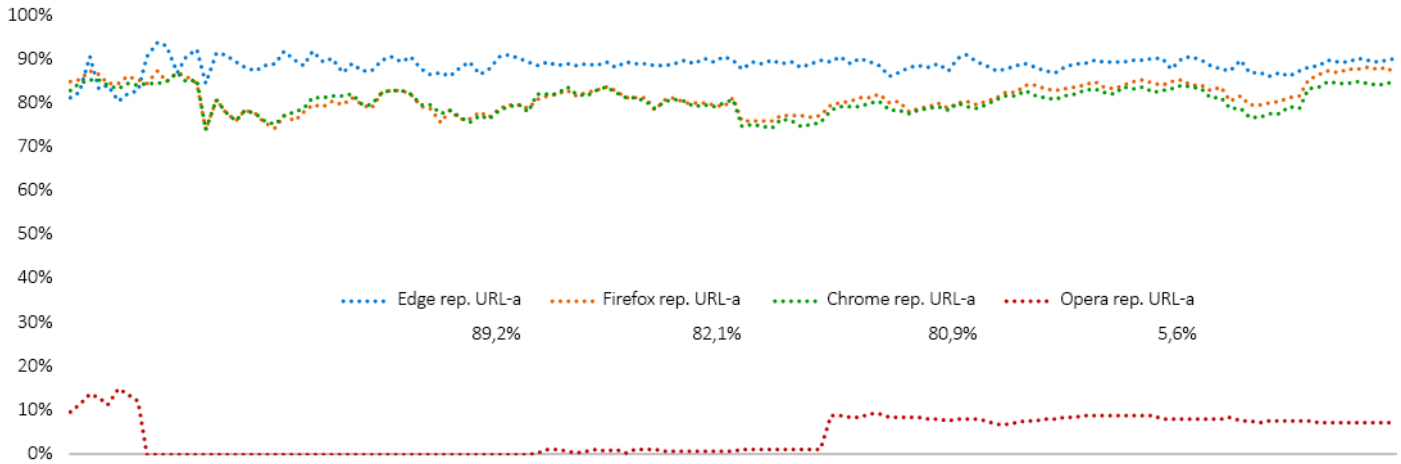
	< 24 h	< 48 h	< 72 h	< 96 h	< 120 h	< 144 h	< 168 h	Ukupno
Edge sa rep. aplikacije	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge sa rep. URL-a	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome sa rep. aplikacije	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome sa rep. URL-a	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Firefox sa rep. aplikacije	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Firefox sa rep. URL-a	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Opera sa rep. URL-a	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Tokom testiranja, Microsoft Edge je pokazao početnu stopu zaštite od malvera od 96,7%. Google Chrome i Mozilla Firefox su ostvarili početnu stopu zaštite od 86,2% i 80,8%, tim redosledom. Početna stopa zaštite pregledača Opera bila je 6,8%. Do kraja sedmog dana testiranja, svi veb pregledači su postigli povećanje zaštite. Microsoft Edge je povećao zaštitu za 4,5% na 98,2%. Google Chrome je povećao za 6,7% na 92,9%, Mozilla Firefox je povećao za 8,4% na 89,2%, a Opera za 0,1% na 6,9%

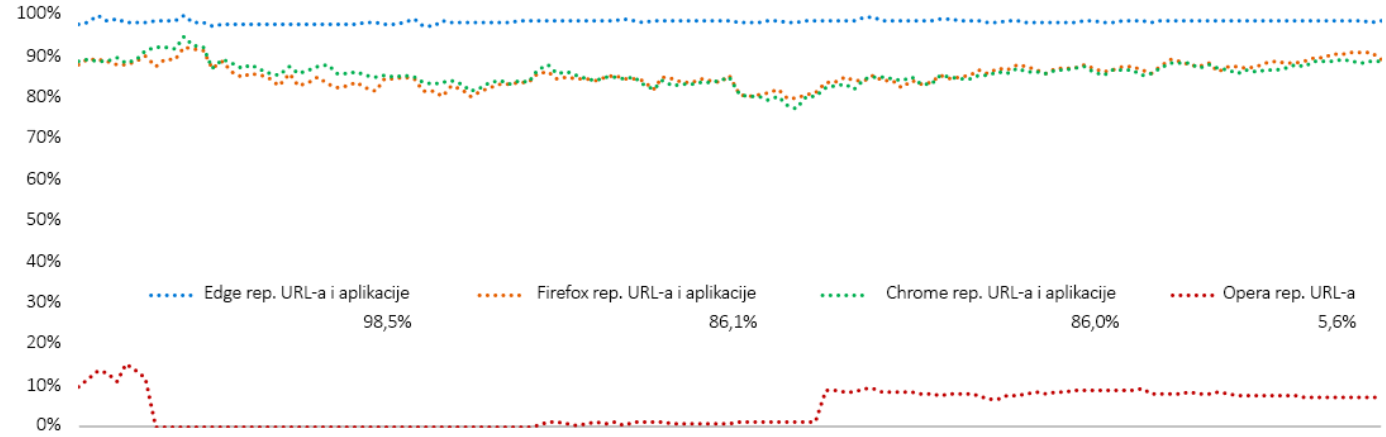
Doslednost zaštite tokom vremena

Tokom celokupnog testiranja neprekidno se dodavao novi malver. URL adrese, datoteke i aplikacije koje više nisu bile dostupne ili više nisu hostovale malver su uklonjene. Svaka tačka podataka se izračunava na osnovu merenja snimljenih u određenom trenutku. Ako je malver blokiran u početku, ocena doslednosti zaštite pregledača se poboljšala tokom vremena. U suprotnom, ako pregledač nije blokirao malver, ocena se smanjila.

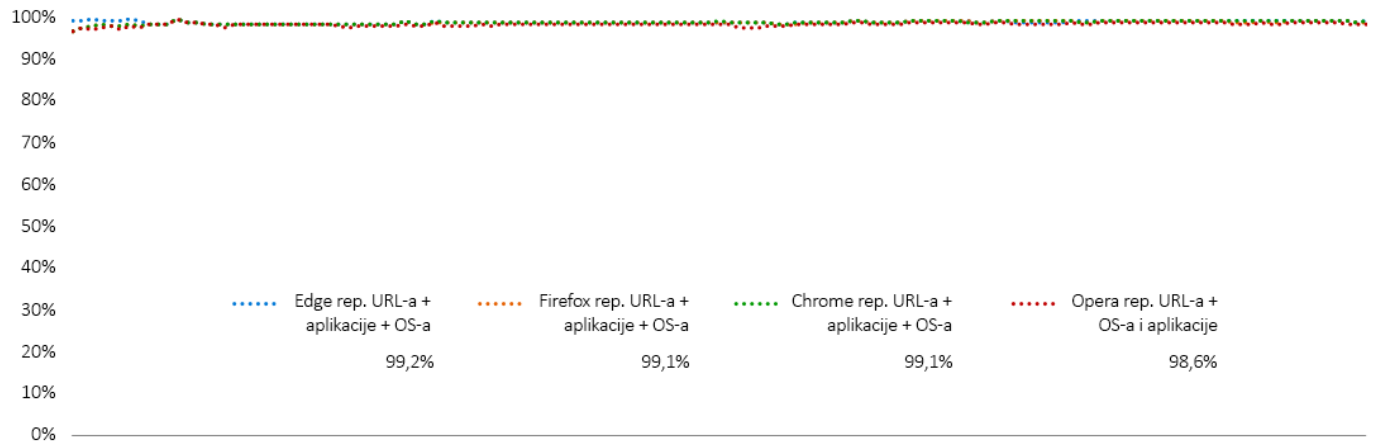
Testiranje je otkrilo tri sloja zaštite: Reputacija URL adresa, reputacija aplikacija u pregledaču i reputacija aplikacija operativnog sistema. Reputacija URL adresa je ponudila prilično dobru zaštitu.



Slojevi u reputaciji aplikacija su povećali zaštitu.



Reputacija operativnog sistema je ponudila dodatnu zaštitu. U idealnom slučaju, veb pregledač će blokirati malver kako on nikada ne bi došao do operativnog sistema. Međutim, testiranje je pokazalo da je reputacija operativnog sistema bila izuzetno efikasna.



Test okruženje

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

Testirani proizvodi

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

Autori

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Metodologija testiranja

NSS Labs Web Browser Security (WBS) metodologija testiranja v4.0 dostupna je na adresi www.nsslabs.com.

Kontakt informacije

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com