

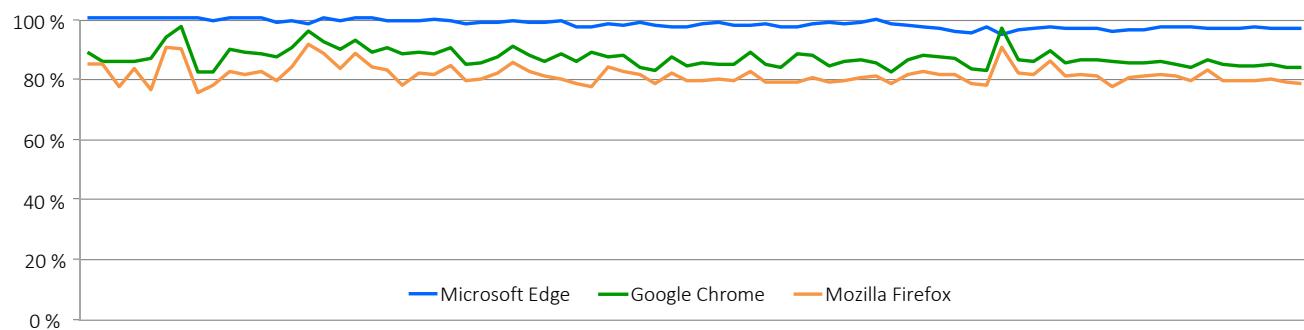
## 2. kvartal 2021. Web-preglednici protiv zlonamjernog softvera

Tijekom drugog kvartala 2021. CyberRatings.org proveo je nezavisno testiranje zaštite od zlonamjernog softvera koju nude web-preglednici. Testiranja su rađena tijekom 20 dana u 80 odvojenih pokretanja testova. Da bi se zaštitio od zlonamjernog softvera, Microsoft Edge koristi Microsoft Defender SmartScreen, dok Google Chrome i Mozilla Firefox koriste Google Safe Browsing API. Microsoft Edge ponudio je najjaču zaštitu, blokirajući 97,4 % zlonamjernog softvera, pri čemu je imao najvišu razinu zaštite od dotad nepoznatih pjetnji (97,7 %). Google Chrome imao je drugu po redu najjaču zaštitu, blokirajući u prosjeku 86,3 %, a nakon njega je bio Mozilla Firefox s 81,8 %.



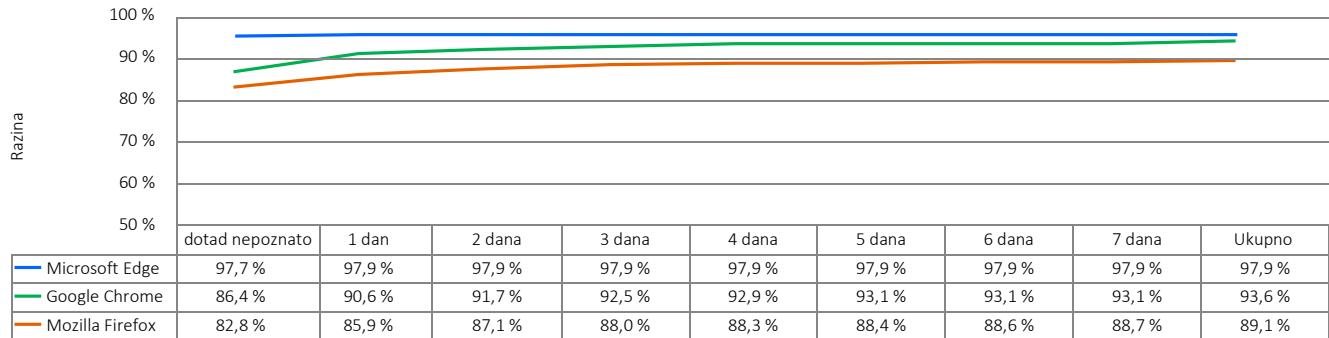
Mogućnost web-preglednika da upozore potencijalne žrtve da će otvoriti zlonamjerno web-mjesto stavlja te programe u jedinstven položaj u borbi protiv zlonamjernog softvera. Web-mjesta koja žele prevariti korisnike (društvenim inženjeringom) da preuzmu zlonamjeren softver kratkog su vijeka, pa je ključno da se takvo mjesto otkrije i čim prije doda u sustav koji prati reputaciju pojedinih web-mjesta. Stoga dobar sustav koji prati reputaciju mora biti točan i brz kako bi ostvario visoku razinu prepoznavanja.

Zaštita od zlonamjernog softvera tijekom vremena



Tijekom testiranja stalno je dodavan novi zlonamjeren softver. Uklanjani su URL-ovi koji više nisu dostupni ili više ne hostiraju zlonamjerne programe. Svaka podatkovna točka izračunata je na temelju mjerenja zabilježenih u određenoj vremenskoj točci. Ako je zlonamjerni softver rano blokiran, poboljšala bi se ocjena preglednika za zaštitu tijekom vremena. Isto tako, ako preglednik nije blokiraо zlonamjeren softver, ocjena bi se smanjila.

Razina blokiranja zlonamjernog softvera tijekom vremena



Prethodna brojka pokazuje koliko je svakom pregledniku trebalo da blokira zlonamjerni softver od trenutka kad je uzorak ubačen u ciklus testiranja. SmartScreen je središnja tehnologija zaštite preglednika Microsoft Edge. On nudi zaštitu od napada utemeljenu na URL-u putem integriranog servisa u oblaku za reputacije URL-ova i reputacije aplikacija radi blokiranja zlonamjernih datoteka. Google Chrome i Mozilla Firefox za reputaciju URL-ova i blokiranje ili upozoravanje korisnika na preuzimanje određenih vrsta datoteka koriste Google Safe Browsing API.

### Napadi zlonamjernim softverom

U napadima zlonamjernim softverom koji se provode društvenim inženeringom (social engineered malware, SEM) koriste se varke kako bi se korisnici naveli da preuzmu zlonamjerni softver: otete adrese e-pošte i računi s društvenih mreža iskorištavaju implicitno povjerenje između kontakata i nasamaruju žrtve, uvjeravajući ih da su veze na zlonamjerne datoteke pouzdane. Među drugim su prevarama skočne poruke koje obaveštavaju korisnike da treba instalirati neke aplikacije (npr. Adobe Flash Player) ili pak upozoravaju da je korisnikovo računalo zaraženo ili da ga treba ažurirati.

Kad se zlonamjerni softver instalira, žrtve su izložene kradji vjerodajnica, kradji identiteta, kompromitiran im je bankovni račun itd.

### Zaštita web-preglednika od zlonamjnog softvera

Radi zaštite od zlonamjnog softvera, reputacijski sustavi u oblaku pretražuju internet u potrazi za zlonamjernim web-mjestima i zatim u skladu s tim kategoriziraju sadržaje. Zatim se web-preglednici kod reputacijskih sustava u oblaku raspituju za određene URL-ove, datoteke ili aplikacije. Ako rezultati govore da je prisutan zlonamjerni softver, web-preglednik preusmjerava korisnika na poruku upozorenja u kojoj se objašnjava da su URL, datoteka ili aplikacija zlonamjerni. Neki reputacijski sustavi obuhvaćaju i dodatne obrazovne sadržaje.

Google Chrome i Mozilla Firefox koriste Google Safe Browsing API za određivanje reputacije URL-ova i aplikacija radi blokiranja zlonamjernih datoteka. Microsoft Edge koristi Microsoft Defender SmartScreen, koji štiti od napada zahvaljujući reputacijskom servisu u oblaku za URL-ove i za reputaciju aplikacija radi blokiranja zlonamjernih datoteka.

### Prosječan broj dnevno dodanih uzoraka zlonamjnog softvera

Prosječno je testnom skupu dnevno dodano 49 novih provjerenih uzoraka zlonamjnog softvera. Taj je broj nekih dana varirao jer se razina zločinačkih aktivnosti mijenja.

### Testno okruženje

- Microsoft Windows 10 Pro, 21H1

### Ukupan broj testiranih uzoraka zlonamjnog softvera

Za svaki je web-preglednik u ukupno 78 testnih ciklusa neprekidnog trajanja više od 468 sati (svakih 6 sati kroz 20 dana) višekratno testirano 18 621 sirovih, neprovjerenih uzoraka. Naši su inženjeri uklonili uzorce koji nisu zadovoljili kriterije provjere valjanosti, uključujući i one koji su sadržavali iskorištavatelje slabih točaka (exploite) jer oni nisu u obuhvatu ovog testiranja. Na kraju je u završni skup od 48 672 odvojenih valjanih testova zlonamjnog softvera uvršteno 950 jedinstvenih i valjanih uzoraka zlonamjnog softvera (16 224 testova po web-pregledniku), čime je ostvarena margina pogreške manja od 3,2 posto (< 3,2 %) uz razinu pouzdanosti od 95 %.

### Kako smo testirali – uzorci zlonamjnog softvera

Podaci u ovom izvješću dobiveni su tijekom razdoblja testiranja u trajanju dvadeset (20) dana – između 11. svibnja i 31. svibnja 2021. Tijekom testiranja inženjeri iz organizacije CyberRatings rutinski su nadzirali mogućnosti povezivanja da bi osigurali da preglednici koji se testiraju mogu pristupiti zlonamjnem softveru, ali i reputacijskim servisima u oblaku.

Naglasak je bio na svježini koju su osigurivali novi uzorci stalno dodavani u testiranje uz uklanjanje „mrtvih“ uzoraka.

### Kako smo formirali rezultate

Mjerili smo sposobnost svakog preglednika da blokira zlonamjerni softver čim se on otkrije na internetu. Inženjeri su ponavljali te testove svakih šest sati da bi utvrdili koliko treba nekom proizvođaču antivirusnog softvera da doda zaštitu od njega.

Stalno su mjerene performanse svakog preglednika te je zabilježena ukupna razina blokiranja svih testiranih uzoraka zlonamjnog softvera. Izračunata je ukupna razina blokiranja svakog preglednika kao broj uspješnih blokiranja podijeljen ukupnim brojem testnih slučajeva. Primjerice, kako su se testiranja radila svakih šest sati, uzorak zlonamjnog softvera koji je bio na mreži 48 sati bio je testiran osam (8) puta. Preglednik koji je blokirao taj zlonamjerni softver u šest rundi testiranja (od maksimalno osam) postigao je razinu blokiranja od 75 %.

### Testirani proizvodi

- Google Chrome: verzija 90.0.4430.212 – 91.0.4472.19
- Microsoft Edge: verzija: 91.0.864.19 – 91.0.864.37
- Mozilla Firefox: verzija 88.0.1 – 88.0.1

# Autori

Thomas Skybakmoen, Vikram Phatak

## Metodologija testiranja

Metodologija testiranja sigurnosti web-preglednika organizacije CyberRatings v1.0 dostupna je na web-mjestu [www.cyberratings.org](http://www.cyberratings.org)

## Podaci za kontakt

CyberRatings.org  
2303 Ranch Road 620 South  
Suite 160, #501  
Austin, TX 78734

[info@cyberratings.org](mailto:info@cyberratings.org)  
[www.cyberratings.org](http://www.cyberratings.org)

© 2021. CyberRatings.org. Sva prava pridržana. Nijedan dio ove publikacije ne smije se reproducirati, kopirati/skenirati, pohraniti na sustav za dohvaćanje, poslati e-poštom ni dijeliti ili prenositi na bilo koji drugi način bez izričitog pisanih pristanka organizacije CyberRatings.org („mi“).

1. Informacije u ovom izvješću možemo mijenjati bez prethodne najave te se odričemo bilo kakve obaveze da ih ažuriramo.
2. Smatramo da su u trenutku objave informacije u ovom izvješću istinite i pouzdane, ali to ne jamčimo. Svaka upotreba i oslanjanje na ovo izvješće isključivo je na vaš rizik. Nismo odgovorni ni za kakve štete, gubitke ili troškove bilo kakve vrste koji bi proizlazili iz pogreške ili propusta u ovom izvješću.
3. NE DAJEMO NIKAKVA IZRAVNA NI PODRAZUMIJEVANA JAMSTVA. OVIME SE ODRIČEMO SVIH PODRAZUMIJEVANIH JAMSTAVA, UKLUČUJUĆI PODRAZUMIJEVANA JAMSTVA KOMERCIJALNOSTI, PRIKLADNOSTI ZA ODREĐENU SVRHU I IZOSTANKA KRŠENJA. NI U KOJEM SLUČAJU NISMO ODGOVORNI NI ZA KAKVU IZRAVNU, POSLJEDIČNU, SLUČAJNU, KAZNENU, PRIMJERNU ILI NEIZRAVNU ŠTETU ILI GUBITAK DOBITI, PRIHODA, PODATAKA, RAČUNALNIH PROGRAMAILI DRUGIH RESURSA, ČAK I AKO JE IZGLEDNA TAKVA MOGUĆNOST.
4. Ovo izvješće ne predstavlja promidžbu, preporuku ni jamstvo ni za koji testirani proizvod (hardverski ili softverski) ili hardver i/ili softver korišten u testiranju proizvoda. Ovo testiranje ne jamči da nema pogrešaka ni nedostataka u proizvodima niti da će proizvodi ispuniti vaša očekivanja, zahtjeve, potrebe ili specifikacije ni da će funkcioništati bez zastoja.
5. Iza ovog izvješća nije promidžba, sponzorstvo, pripadnost ni potvrda bilo koje od organizacija spomenutih u izvješću.
6. Svi žigovi, uslužne oznake i trgovački nazivi korišteni u ovom izvješću pripadaju svojim vlasnicima.