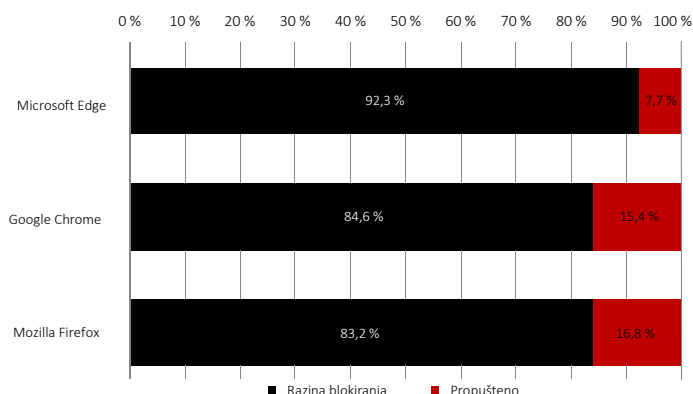


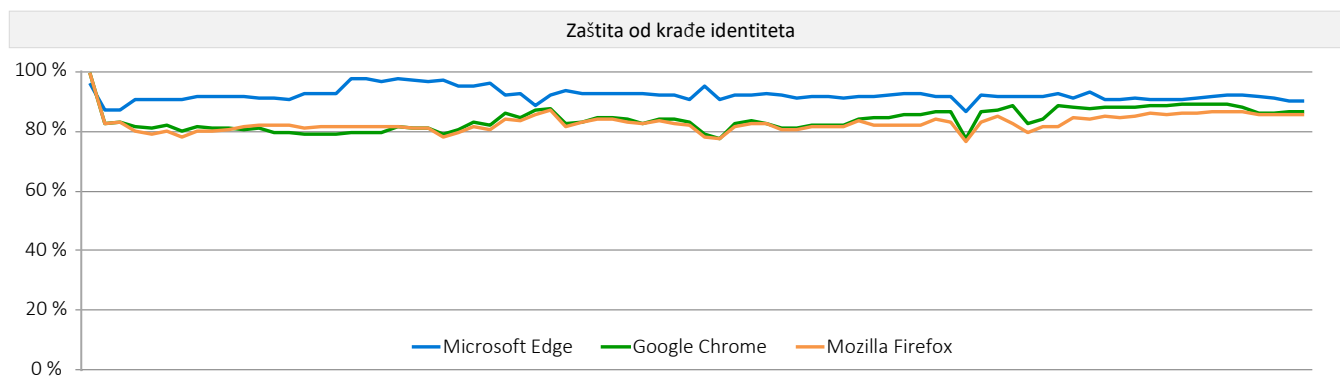
2. kvartal 2021. Web-preglednici protiv krađe identiteta

Pregled

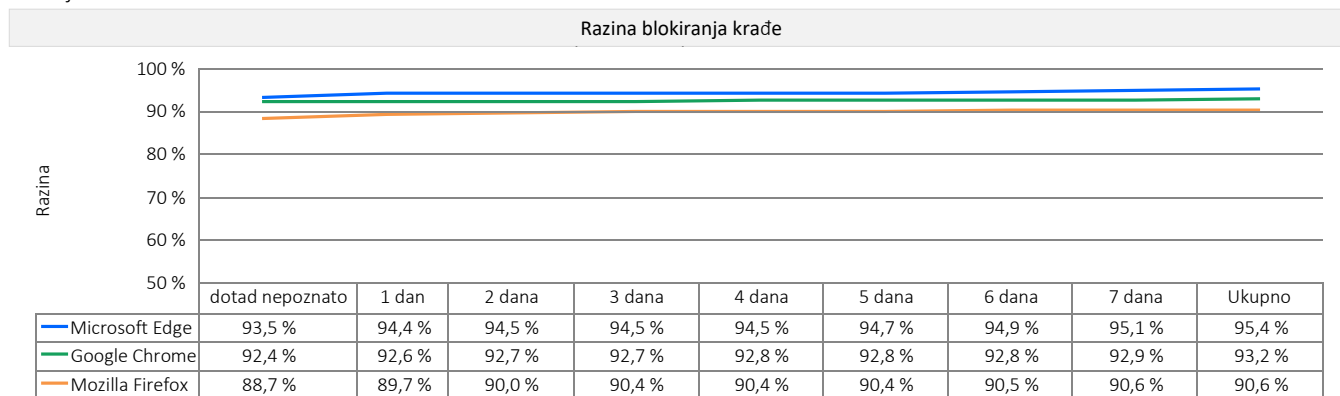
Tijekom drugog kvartala 2021. CyberRatings.org proveo je nezavisno testiranje koliku razinu zaštite od krađe identiteta nude web-preglednici. Testiranja su rađena tijekom 20 dana u 80 odvojenih pokretanja testova. Da bi se zaštitio od krađe identiteta, Microsoft Edge koristi Microsoft Defender SmartScreen, dok Google Chrome i Mozilla Firefox koriste Google Safe Browsing API. Microsoft Edge ponudio je najjaču zaštitu, blokirajući 92,3% URL-ova za krađu identiteta, pri čemu je imao najvišu razinu zaštite od dotad nepoznatih prijetnji (93,5%). Google Chrome imao je drugu po redu najjaču zaštitu, blokirajući u prosjeku 84,6%, a nakon njega je bio Mozilla Firefox s 83,2%.



Sustavi koji bilježe reputaciju URL-ova skraćuju vrijeme koje napadači imaju za postizanje svojih ciljeva tako što sprječavaju/upozoravaju korisnike da je neki URL poznato web-mjesto za krađu identiteta. No, kako korisnici posjećuju raznorazna web-mjesta od kojih su mnoga nova, reputacijski sustavi s URL-ovima ne mogu jednostavno blokirati sve nove URL-ove. Znajući to, kampanje krađe identiteta koje provode napadači stalno se mijenjaju, pa se većina novih napada događa u prvih nekoliko sati nakon pokretanja napada.



Tijekom testiranja svakodnevno su dodavani novi URL-ovi za krađu identiteta, dok su URL-ovi koji više nisu dostupni ili ne služe za napade krađe identiteta uklanjani. Svaka podatkovna točka predstavlja zaštitu u određenoj vremenskoj točki. Ako je URL rano blokirano, poboljšala bi se ocjena preglednika za zaštitu tijekom vremena. Isto tako, ako preglednik nije blokirao URL, ocjena bi se smanjila.



Mjerali smo sposobnost svakog preglednika da blokira zlonamjerne URL-ove čim se oni otkriju na internetu. To se nastavljalo svakih šest sati da bi se utvrdilo koliko treba nekom proizvođaču antivirusnog softvera da doda zaštitu. Prethodna brojka pokazuje koliko je svakom pregledniku trebalo da blokira web-mjesto za krađu identiteta od trenutka kad je prijetnja uvedena u ciklus testiranja.

Sažetak rezultata

Napadi krađe identiteta

Krađa identiteta vrsta je napada društvenim inženjeringom koji pokušava uvjeriti žrtvu da napadaču otkrije povjerljive osobne podatke. Neki su primjeri povjerljivih podataka brojevi kreditnih kartica, OIB te korisnička imena i lozinke bankovnih računa. E-pošta, izravne poruke, SMS-ovi i veze na društvenim mrežama – sve su to vektori za napade krađe identiteta. Odredišna stranica web-mjesta za krađu identiteta često pokušava potajno iskoristiti računalo posjetitelja i instalirati zlonamjeran softver (tzv. usputni exploit).

Napadi krađe identiteta predstavljaju znatan rizik za pojedince i organizacije tako što ugrožavaju ili pribavljaju povjerljive osobne i poslovne podatke. Radna skupina za borbu protiv krađe identiteta APWG (Anti- Phishing Working Group) prijavila je u četvrtom kvartalu 2020. ukupno 396 688 jedinstvenih kampanja krađe identiteta.¹

Zaštita web-preglednika od krađe identiteta

Zaštitu od krađe identiteta pruža aplikacija unutar web-preglednika koja servis u oblaku – a on pregledava internet, traži web-mjesta za krađu identiteta i dodaje ih na popis za blokiranje – pita kakva je reputacija nekog URL-a. Kad web-preglednik pokuša posjetiti neki URL, preglednikova zaštita od krađe identiteta (tj. Safe Browsing, SmartScreen itd.) preusmjerava korisnika na poruku upozorenja koja objašnjava da je taj URL zlonamjeran. Neki reputacijski sustavi obuhvaćaju i dodatne obrazovne sadržaje. Ako se utvrdi da je neko web-mjesto „dobro“, web-preglednik ne poduzima ništa.

Google i Firefox za reputaciju URL-ova i upozoravanje korisnika pri preuzimanju određenih vrsta datoteka koriste Google Safe Browsing API. Microsoft Edge koristi Microsoft Defender SmartScreen, koji nudi zaštitu od napada utemeljenu na URL-u zahvaljujući integriranom servisu u oblaku za provjeru reputacije URL-ova i aplikacija radi blokiranja zlonamjernih datoteka.

Prosječan broj dnevno dodanih zlonamjernih URL-ova

Prosječno je testnom skupu dnevno dodano 50 novih provjerenih URL-ova. Taj je broj nekih dana varirao jer se razina zločinačkih aktivnosti mijenja.

Testno okruženje

- Microsoft Windows 10 Pro, 21H1

Ukupan broj testiranih zlonamjernih URL-ova

Za svaki je web-preglednik u ukupno 80 testnih ciklusa neprekidnog trajanja više od 480 sati (svakih 6 sati kroz 20 dana) višekratno testirano 26 976 sirovih, nepotvrđenih URL-ova. Naši su inženjeri uklonili uzorke 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 61 605 odvojenih valjanih testova krađe identiteta uvršteno 996 jedinstvenih i valjanih uzoraka URL-ova za krađu identiteta (20 535 testova po web-pregledniku), čime je ostvarena margina pogreške manja od 3,1 posto (< 3,1 %) uz razinu pouzdanosti od 95 %.

Kako je provedeno testiranje – URL-ovi za krađu identiteta

Podaci u ovom izvješću dobiveni su tijekom razdoblja testiranja u trajanju dvadeset (20) dana – između 11. svibnja i 31. svibnja 2021. Tijekom testiranja naši su inženjeri rutinski nadzirali mogućnosti povezivanja da bi osigurali da preglednici koji se testiraju mogu pristupiti URL-ovima za krađu identiteta, ali i reputacijskim servisima u oblaku.

Naglasak je bio na svježini koju su osiguravali novi URL-ovi stalno dodavani u testiranje uz uklanjanje „mrtvih“ web-mjesta.

Kako smo formirali rezultate

Mjerali smo sposobnost svakog preglednika da blokira krađu identiteta čim se ona 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 URL-ova. 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, URL koji je bio na mreži 48 sati testiran je osam (8) puta. Preglednik koji ga je blokirao 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

¹ APWG-ovo izvješće o trendovima u aktivnostima krađe identiteta

Autori

Thomas Skybakmoen, Vikram Phatak

Metodologija testiranja

Metodologija testiranja sigurnosti web-preglednika organizacije CyberRatings v1.0 dostupna je na web-mjestu www.cyberratings.org

Podaci za kontakt

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

info@cyberratings.org

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 pisanog 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, UKLJUČUJUĆI 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 PROGRAMA ILI 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 funkcionirati 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.